ISACA®
Trust in, and value from, information systems

GETTING STARTED WITH GEIT:

A Primer for Implementing Governance of Enterprise IT

ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

ISACA has designed and created *Getting Started With GEIT: A Primer for Implementing Governance of Enterprise IT* (the "Work") primarily as an educational resource for security, governance and 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, security, governance and assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

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

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

Website: www.isaca.org

Provide feedback:
www.isaca.org/getting-started-with-GEIT

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

ISBN 978-1-60420-664-7

Getting Started With GEIT: A Primer for Implementing Governance of Enterprise IT

CONTENTS

CHAPTERS

APPENDICES

A Case Studies in Applying GEIT

B Sample Business Case (From *COBIT 5 Implementation*)

C Resources for GEIT Implementation

GETTING STARTED

Introduction

Technology is the lifeblood of organizations in today's business world. Organizations can either fail or succeed on the basis of how they approach and use technology; specifically, technology can present both a business advantage and, in other situations, a potential source of concern and risk.

How do organizations know they are effectively utilizing enterprise technology resources to best realize business goals? Do organizations know the extent to which their business goals are dependent on technology? Is there a better way to achieve enterprise goals? Is there something else that enterprises could use to make them nimbler, more agile or better equipped to respond to market pressures or customer demand? How do they know the technology they have in place is providing value and realizing the expected return on investment?

Governance of enterprise IT (GEIT) is the systematic process of answering these and other related questions. Implementing a GEIT system can bring many benefits to an organization, including lower costs, greater control, more efficient and effective use of resources, and overall better strategic alignment and risk management. According to the Organisation for Economic Co-operation and Development (OECD), stronger governance leads to lower costs of capital and other financial market benefits including increased innovation and entrepreneurship.[1] Enterprises practicing strong governance are rewarded by paying lower interest in the capital markets when they access funds.

Of course, there is an inverse to this. The primary purpose of adopting and using a GEIT system is to deliver value to stakeholders. If that value cannot be delivered or if the delivery (though realized, implemented or delivered) is not well understood by those benefiting from it, then the resources consumed to implement GEIT in the organization will have been wasted. This guide provides the necessary steps to implement GEIT to help the enterprise achieve its goals and demonstrate value delivery.

To successfully implement GEIT, a stepwise approach to and use of a GEIT framework can be helpful. This helps practitioners to gain traction swiftly, implement some quick wins and realize much of the value that comes with GEIT without the need to become framework experts themselves. This guide provides that pathway and leads users through the available GEIT material to quickly gain the value of using GEIT.

Whether the enterprise is already familiar with GEIT concepts and practices or is exploring the possibilities, this guide will help provide an understanding of the steps to implement GEIT and examples of the benefits of GEIT so that buy-in from senior leadership can be obtained and a framework used to guide implementation efforts.

To successfully implement GEIT, a stepwise approach to and use of a GEIT framework can be helpful. This helps practitioners to gain traction swiftly, implement some quick wins and realize much of the value that comes with GEIT without the need to become framework experts themselves.

1 Organisation for Economic Co-operation and Development (OECD), *Corporate Governance, Value Creation and Growth: The Bridge between Finance and Enterprise*, France, 2012

Audience and Purpose

This guide is intended for people who are new to GEIT or have recently been tasked with implementing a GEIT structure.

The guide presents an overview of GEIT and then demonstrates what can be accomplished with the output from a GEIT framework. With a complete and systematic evaluation of goals and an appropriate direction set for technology objectives that is in line with business expectations, a governance structure provides some specific objectives that can be used by management to help execute technology projects and manage technology investments. This execution and management component could be thought of as Management of Enterprise IT or MEIT. In order to best illustrate the importance of properly designing GEIT solutions, it is necessary to show how those solutions are implemented to solve a business problem—i.e., the extent to which they facilitate management. That said, management and governance are different things—governance concerns itself with the goals (i.e., the "why" aspects of accomplishing a particular outcome), while management concerns itself with the execution of the goal (the "how"). Because these two facets are linked, this publication includes the design of a GEIT structure and then shows how that structure is fed through the enterprise to create the expected stakeholder value it was designed to produce.

Knowing how to treat the output of GEIT is critical. Governance produces directives for management, but management must then execute on those directives. The GEIT practitioner must understand what happens downstream from the GEIT structure and must help design the critical measures to be used to monitor how effective the enterprise is achieving the defined goals. Management will employ enterprise resources to deliver on stakeholder expectations and will plan, build, run and monitor operations to ensure the governance objectives were met. This publication includes a comprehensive overview of these steps to provide the GEIT practitioner with a complete understanding of how to use GEIT to satisfy stakeholder requirements.

Note: For the purposes of demonstration and example, this guide will refer frequently to COBIT® 5. However, use of COBIT 5 is not a prerequisite to implementing GEIT within the organization. COBIT 5 is a business framework for the governance and management of IT and is just one of many GEIT frameworks available; many of the steps outlined in this guide can be used with any framework chosen. More in-depth case studies of using COBIT 5 in GEIT implementation are contained in **appendix A**.

1

What Is GEIT?

GEIT is concerned primarily with organizing the IT resources of an enterprise for the purpose of satisfying stakeholders' needs. It is meant to bring alignment among high-level strategic objectives, operational-level activities and work outcomes. As GEIT is essential to ensuring IT alignment and optimization to stakeholder needs, it shares the same purpose as overall corporate and enterprise governance structures and should be considered synergistically.

The formal definition of GEIT overlays three key elements—evaluate, direct and monitor—on the general management of IT resources, ensuring that these governance principles are supported by all IT strategic and operational processes, systems and tools used by an enterprise. These key elements make up the activities of GEIT and serve as the focal point for enterprise leaders.

In the simplest terms, GEIT is making efficient and effective use of resources in support of business needs. The purpose of GEIT is to deliver value to stakeholders. Implementing GEIT in the organization can help to demonstrate and document how the organization engages appropriate functions and uses resources in an efficient and effective way to meet the needs of stakeholders.

Because every industry and organization has specific needs, distinct cultures and different levels of governance in place, a critical first step in implementing a GEIT structure is brainstorming to help answer the question, "What is GEIT here?" from the perspective of the organization planning the initiative and from the context of industry and region in which it operates.

Benefits of Using GEIT

The first step to implementing GEIT is to gain the internal support and organizational will or desire to do so.

Making this happen ties directly to articulating the results and benefits the enterprise intends to achieve. There are several benefits to implementing GEIT that can help gain the support of senior leadership for the effort. The outcomes of a successful GEIT implementation produce both shorter-term, tangible benefits (such as reduced cost) and longer-term benefits (such as enhanced management of IT-related risk, improved relationship between business and IT, and increased business competitiveness).

GEIT ensures greater alignment of IT and its use with business objectives. By implementing GEIT, many organizations experience improvements in the management of IT-related risk as well as improvement in the communication and relationship between the business and IT.

A strong GEIT system can also contribute to lowered financial costs resulting from

both internal and external perspectives—more streamlined use of available resources and lenders' more favorable assessment of the enterprise's risk profile due to increased control.

Absent any problems, few organizations believe they need to be doing anything differently. If there are no apparent issues, it may be difficult to help senior leadership understand why GEIT would be beneficial to the organization. However, the exercise of implementing GEIT can be beneficial because it allows the enterprise to demonstrate to outside parties the level and manner of control and oversight that is occurring within the enterprise. This can be useful in industries that are subject to regulations and can help to demonstrate the value being delivered to stakeholders.

In today's highly interconnected and technology-enabled world, organizations are rapidly realizing that their digital presence and ability to protect critical functions and information are as important to their ability to remain competitive as the product or service they produce. Further, multiple frameworks—security, privacy, compliance, risk, etc.—seek to address and help direct and monitor optimization in support of these bleeding-edge business drivers. The European Research Cluster on the Internet of Things (IERC) notes the challenges that size and heterogeneity place on the governance of the Internet of Things (IoT), given the difficulty in finding common definitions of IoT governance and the many different positions of IoT's various stakeholders.[2]

A GEIT framework is used to align high-level strategic objectives, operational-level activities and work outcomes. It is also a natural mechanism to help align multiple frameworks.

GEIT can help to transition IT's role from a passive one to a more proactive one. Often, IT departments are considered a cost center and follow a "break-fix model," wherein a problem occurs and IT is approached to troubleshoot and remediate a specific issue. In a proactive IT role, the IT function is integral to the definition and achievement of business goals. The IT function is engaged by senior leadership of the enterprise to determine and support enterprise goals. Once the enterprise goals have been determined by an engaged IT function, associated IT-related goals are created that directly support the business needs in a relevant way.

In short, rather than waiting for the business to approach IT to fix a problem where the costs and time line may be prohibitive, IT can position itself to not only support the business in a thoughtful manner but also provide solutions rather than simply reacting to issues as they arise.

An engaged, proactive IT department also lends itself to more innovation by providing guidance on enhanced technology solutions or using IT resources creatively to support new business needs. As resources become aligned optimally with stakeholder needs, they can be reallocated, rebalanced or redirected to support new ideas that might perform better or more directly benefit stakeholders they support.

Moreover, the involvement of IT in the early phases of addressing a need means that IT can assign technology experts to find, select and implement the very best and most advantageous solutions to business challenges. GEIT can help to ensure there is proper balance between these more innovative initiatives and those that are needed to keep business processes up and running. An overview of capturing these benefits is shown in **figure 1**.

In today's highly interconnected and technology-enabled world, organizations are rapidly realizing that their digital presence and ability to protect critical functions and information are as important to their ability to remain competitive as the product or service they produce.

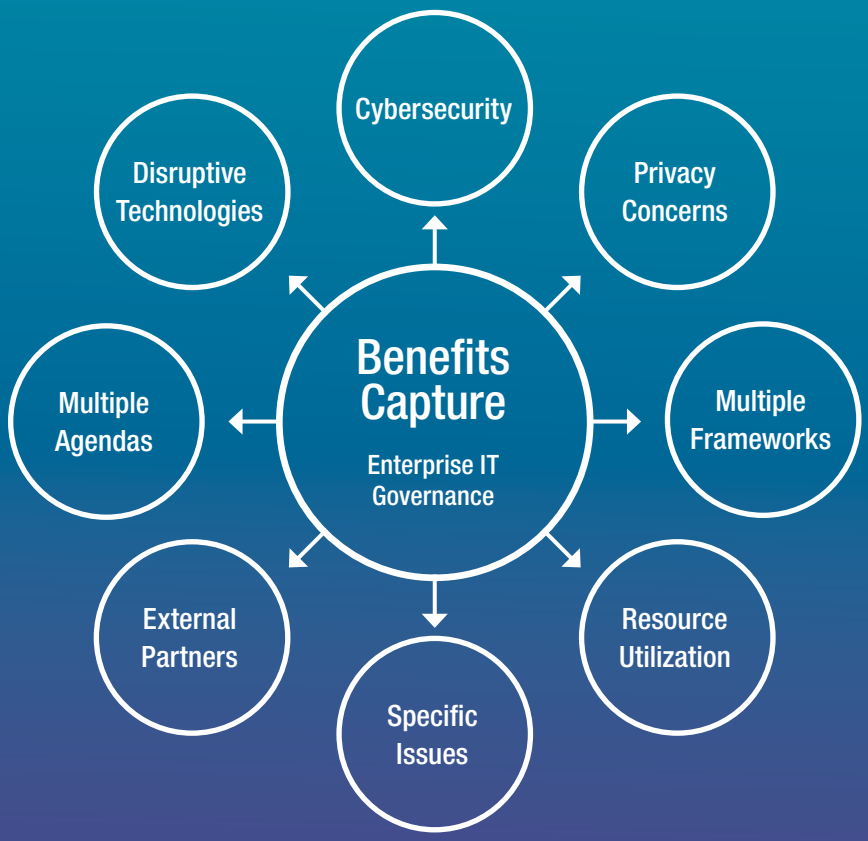
Creating the Business Case

The most direct path to enlisting internal support is through the development of a business case that incorporates the business benefits already described—meaning, codifying a supporting rationale that can be leveraged to seek and obtain the approval and support required for GEIT. The business case can help

2 European Research Cluster on the Internet of Things (IERC), "Internet of Things, IoT Governance, Privacy and Security Issues," January 2015, http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf

FIGURE 1

Capturing GEIT Benefits



communicate the purpose and value of GEIT to the key internal stakeholders (including leadership) and can help to find and obtain an executive sponsor and internal champions for the undertaking.

A business case is essential to the success of a GEIT initiative. The business case can start as a high-level, more strategic document that includes a clear statement of the desired business outcomes. Then, as the initiative progresses through the initial stages of a GEIT implementation, more detail can be added such as tasks, milestones, and roles and responsibilities. It is a dynamic, living document that will be updated as the organization moves through the GEIT implementation process.

The COBIT 5 framework provides an overview of typical business case content, recommending that the business case include, at a minimum, the following:[3]

- The business benefits sought, their alignment with business strategy described and the associated benefit owners (who in the business will be responsible for securing them) identified. This could be based on pain points and trigger events.
- The business changes needed to create the envisioned value. This could be based on health checks and capability gap analyses and should clearly state both what is in scope and what is out of scope.

3 ISACA, *COBIT 5*, USA, 2012

- The investments needed to make the governance and management of enterprise IT changes (based on estimates of projects required)
- The ongoing IT and business costs
- The expected benefits of operating in the changed way
- The risk inherent in the previous bulleted items, including any constraints or dependencies (based on challenges and success factors)
- Roles, responsibilities and accountabilities related to the initiative
- How the investment and value creation will be monitored throughout the economic life cycle and the metrics to be used (based on goals and metrics)

Identifying the possible GEIT options, strengths and weaknesses of each, and associated risk with a recommendation of the most appropriate path can provide context and lend support to the most appropriate GEIT course of action.

Obtaining Buy-in

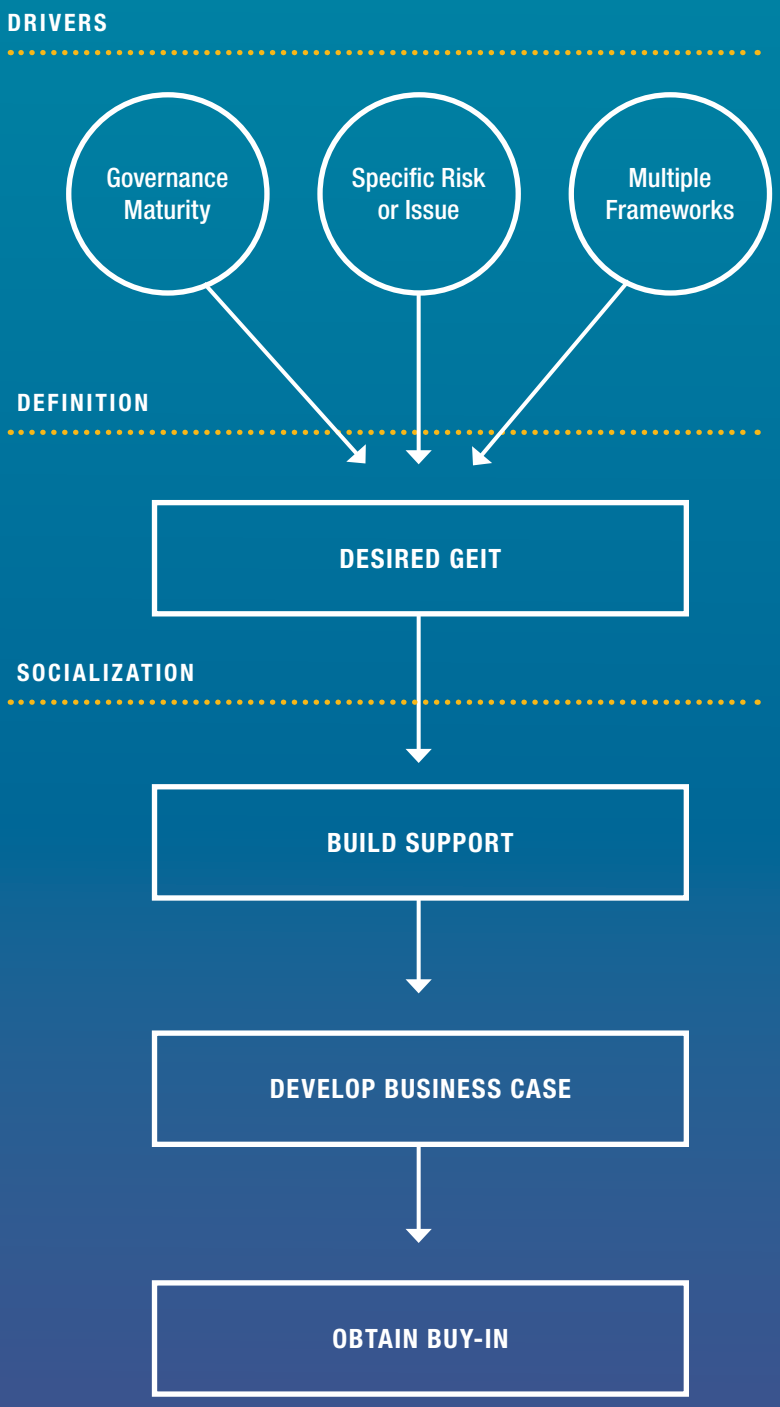
As has been noted, a key step in getting the GEIT initiative underway is generating the organizational will to do so. Specifically, for an enterprise to implement a new GEIT system successfully, commitment must be secured from the highest levels. Only when senior leadership, the board of directors and/or others of highest authority drive the need for GEIT can its implementation succeed. This support directly from the highest levels of the organization can help to ensure the resources necessary to successfully create and implement the plan.

Informing and gaining support from peer organizations is also important; in this context, this could be any organization that holds a stake in decision making relative to technology such as (but by no means limited to): compliance, legal/counsel, purchasing, marketing, research and development, or specific lines of business. These peer organizations help facilitate the GEIT implementation, but if they are not receptive, they can also (intentionally or unintentionally) create roadblocks that can detract from the implementation's success. By engaging peer organizations at the outset, an environment can be created that will reduce any roadblocks in implementing GEIT, including ensuring that critical resources are available when needed to ensure a successful rollout.

Only when senior leadership, the board of directors and/or others of highest authority drive the need for GEIT can its implementation succeed. This support directly from the highest levels of the organization can help to ensure the resources necessary to successfully create and implement the plan.

FIGURE 2

GEIT Initiative Conceptualization



The business case can be used as a starting point for developing the organizational will—specifically, by providing a mechanism to gain support from those in authority, for socializing the benefits and planned changes to peer organizations and stakeholders, and as a road map for all those who may be involved in the implementation process. At the early stages, a high-level overview is typically sufficient to obtain preliminary buy-in, so it may not be necessary to present all the details included in this first meeting. Instead, the focus can be placed on the high-level outcomes: the benefits the enterprise intends to realize and the advantages that a GEIT implementation can offer in the context of the organization.

At this stage it can be most effective to present outcomes in the language of the organization's business or mission. For example, if the organization is a publicly traded for-profit company, it might be useful to highlight positive economic outcomes and shareholder value. If the organization is a government entity, framing the benefits from the perspective of increased transparency, public service and value to the citizenry might make more sense. For a nonprofit, it might be the increased ability to effect change or fulfill specific organizational goals. As every organization is different, the specific parlance, vocabulary and focus will vary from organization to organization. An overview of the process from identifying drivers through obtaining buy-in to conceptualize GEIT is presented in **figure 2**.

Next Steps

Once support from executive and peer levels is in place, the real work begins. As with any major strategic initiative, an implementation plan is needed to capture the desired state, the milestones and all associated activities to ensure the GEIT initiative achieves the desired purpose. COBIT 5 defines seven steps in the implementation of GEIT (**figure 3**). While these steps were designed for the COBIT 5 framework, they can be useful regardless of the framework(s) used to develop the GEIT implementation plan.

These steps include:

1/ Initiate the program
Gaining an understanding of the need to do something (i.e., what triggers the activity of implementing GEIT). As part of the GEIT initiative conceptualization, the organization brainstorms the purpose of the initiative and captures the benefits to the stakeholders.

2/ Define problems and opportunities
Gaining an understanding of the current state of the enterprise

3/ Define a road map
Looking at and documenting the organization's desired state

4/ Plan the program
Gathering the project team and developing an implementation plan that closes the gap between the current state and the desired state

5/ Execute the plan
Putting the plan developed in step 4 into action

6/ Realize benefits
Looking at the plan in place to see if the benefits have been achieved

7/ Review effectiveness
Returning to the plan to see if it is still performing effectively

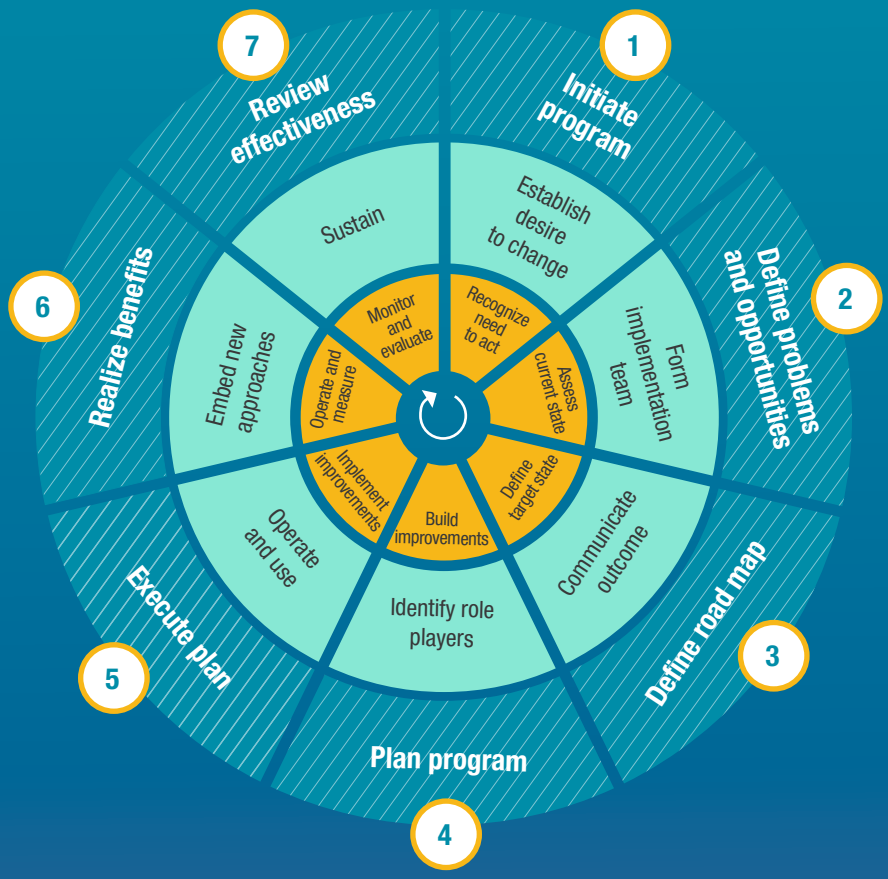
---

ACTION ITEMS:

- ☐ Determine which benefit(s) of GEIT are most appealing to the organization. Document why this is most appealing and what additional benefits may be realized from implementing GEIT in the enterprise.
- ☐ Develop a business case for a GEIT initiative in the enterprise (see **appendix B**). Using the business case as a starting point, create a presentation to present to relevant stakeholders to obtain buy-in for GEIT. For maximum understanding, translate the outcomes to the specific language and perspective to which the organization is most attuned.

FIGURE 3

Stages of GEIT Implementation



1/ What are the drivers?
2/ Where are we now?
3/ Where do we want to be?
4/ What needs to be done?
5/ How do we get there?
6/ Did we get there?
7/ How do we keep the momentum going?

Program management (outer ring)
Change enablement (middle ring)
Continual improvement life cycle (inner ring)

SOURCE: ISACA, *COBIT® 5 Implementation*, USA, 2012, figure 6

2

Initiate the Program: The Rationale for GEIT

Chapter 1 discussed the importance of defining GEIT within a specific environment and identifying and socializing the benefits. Key to the process of obtaining and sustaining buy-in and laying the foundation for future activities is the process of defining why an organization needs to take action in the first place. What is the driving force behind implementing the change?

Critical to this definition are the goals of the enterprise's stakeholders. Stakeholders include, but are not limited to:

- Boards of directors
- Senior/executive management
- Shareholders (if publicly traded)
- Government (depending on the industry)

Stakeholders have strategies to achieve value for the organization. Jack Springman, writing for the *Harvard Business Review*, states that, "Typically there are three dimensions of value—financial (price, volume, margin, ROI, etc.); functional (increasing stakeholder's productivity, providing choice or flexibility, being easy and convenient to do business with, and delivering speedy service) and emotional (providing security to generate trust and stimulating a feel-good factor)."[4]

According to COBIT 5, the needs of the stakeholders drive the strategy for the organization and the objectives of GEIT. The British Standard Institution's standard BS 13500 defines governance as a "system by which the whole organization is directed, controlled and held accountable to achieve its core purpose over the long term."[5] Therefore, meeting with stakeholders early in the process will help to ensure that the scope is correct, the target state defined and the overall initiative successful.

GEIT is primarily implemented in enterprises to meet stakeholders' requirements for new or improved governance structures or systems. These requirements are usually recognized as a result of **pain points** and/or **trigger events**. Understanding what stakeholders need or desire provides additional information that can be used to identify issues or factors

4 Springman, Jack; "Implementing a Stakeholder Strategy," *Harvard Business Review*, 28 July 2011, *https://hbr.org/2011/07/implementing-a-stakeholder-str/*

5 British Standard Institution (BSI), BSI 13500 *Code of practice for delivering effective governance of organizations*, 2013

contributing to the issues that initiated the need for action to be taken.

Identifying Pain Points

Pain points are typically symptoms having negative impact or trend on the business.

They are one of the drivers that motivate the move to, or an improvement in, GEIT. Some typical pain points include, but are not limited to:

- Failed or delayed IT initiatives
- Rising costs
- Perception of low business value for IT investments
- Significant incidents related to IT risk and security events (e.g., data loss)
- Service delivery problems
- Failure to meet regulatory or contractual requirements
- Audit findings for poor IT performance or low service levels
- Hidden and/or rogue IT spending
- Resource waste through duplication or overlap in IT initiatives
- Insufficient IT resources
- IT staff burnout/dissatisfaction
- Frequent failure of IT-enabled changes to meet business needs (late deliveries or budget overruns)
- Multiple and complex IT assurance efforts
- Reluctance of board members or senior managers to engage with IT
- Ineffective IT third-party or vendor relationships

Because of the wide variety of possible factors involved, recognizing and identifying pain points and understanding their dependencies can be a difficult exercise. In some cases, identification of pain points can be simple and direct; for example, it might involve documenting business issues already known to exist or codifying institutional knowledge about adjustments that are widely known by stakeholders to bring about improvements if implemented. However, it can also be more complicated and involved; for example, it could extend to interviewing business units and other teams to determine areas of concern and using those to derive specific outcomes.

Some pain points can make themselves known in ready fashion, but others may not. At times, further analysis into the subject (e.g., cost analysis, inefficiencies) and systematic evaluation may be needed to help determine the specific areas of concern. Therefore, even if pain points seem self-evident on the surface, it is a useful exercise to collect, evaluate and codify them as part of the initial phases of GEIT implementation.

Once a specific pain point is identified, a root cause analysis can be used to determine the cause of the issue. This process looks at the conditions and factors that contributed to the issue and exposes where action must be taken to prevent recurrence or improve the conditions that led to the issue in the first place. This process of examination could include interviews with individuals or groups of stakeholders so their direct experience of pain points can provide raw material for additional analysis. It could also potentially include the examination of specific metrics and performance indicators that are already being collected as a by-product of current operations.

From the pain points identified and their possible damage to—or impact upon—the organization, a business case can be built for the implementation of GEIT by showing how better governance and management of information and related technology can mitigate the damage and help define a desired state for the organization. Keep in mind that the goal here is not yet to reach the desired state—instead, merely to identify the state that the organization wishes to ultimately reach. The business case should include documentation of these pain points and will be used to identify the scope of the GEIT implementation project, its goals and definition of the resources it will require.

Once a specific pain point is identified, a root cause analysis can be used to determine the cause of the issue. This process looks at the conditions and factors that contributed to the issue and exposes where action must be taken to prevent recurrence or improve the conditions that led to the issue in the first place.

Trigger Events

Trigger events are occurrences that prompt the need for a change. One perspective is to think of trigger events (and pain points) as headlines: "XYZ Corporation Welcomes New Chief Security Officer," "ABC Financial Reports Fourth

Quarter Losses," "LMNOP Department Store Reports Security Breach; Millions of Customers Affected," "EFG Bank Adopts Cloud-based Storage." The headline in this case describes the specific event or driver that will cause a change to be brought about.

When a headline occurs, it is reflective of a specific issue (such as adoption of new disruptive technology or a failure to make projected quarterly earnings) that has impacted the organization in some way. Just like the pain points outlined above, examination of these trigger events should be incorporated into GEIT planning. When looking into the issue, the main question to ask is what are the pain points and trigger events?

Trigger events usually signify an improvement opportunity to increase the benefits to the organization. Some examples of trigger events are:

- Merger, acquisition or divestiture
- Shift in the market, economy or competitive position
- Change in business operating model or sourcing arrangements
- New regulatory or compliance requirements
- Significant technology change or paradigm shift
- An enterprisewide governance focus or project
- A change in senior leadership (i.e., a new chief information officer [CIO], chief financial officer [CFO], chief operating officer [COO] or chief executive officer [CEO])
- External audit or consultant assessments
- A new business strategy or priority

GEIT can help an enterprise manage future headline-making events by minimizing negative events, helping to enable change to support new and emerging trends, and documenting for stakeholders and the public that the enterprise continues to deliver value. It can also serve as a vehicle to maximize positive outcomes by helping to increase the impact of positive events and positioning the organization in the way most likely to ensure positive outcomes are repeated.

Deciding to Use a Framework

The practice of good governance provides the direction needed to achieve the desired outcome. When a GEIT program is initiated effectively, the pain points and trigger events, their causes, and the desired end state are clearly understood. The business case and buy-in from executive leadership and peer functions set the foundation such that the desired state can be achieved.

Good governance in practice typically uses a framework to ensure the repeatable, predictable delivery of value to stakeholders. It should be noted that some enterprises can and do operate without the use of a formal system of GEIT—or, more commonly, they have an implicit or informal system of GEIT. The challenge for these organizations is twofold. First, because what they are doing is ad hoc and not formalized, it can be difficult to improve upon it in a systematic fashion and multiple or competing governance structures may arise. Second, if a need arises to extend or reproduce the model (e.g., if the organization acquires a competitor and wishes to extend the model into that new environment), it can be hard to define precisely the elements that have been successful. In other words, it can be difficult to distill down to the core mechanisms that provide the value.

Using a framework formalizes this. By outlining the repeatable, systematic steps to defining the governance approach, organizations can pick for themselves (based on their own needs and circumstances) what works best for them, and they can adapt what they will use to drive improvements and establish oversight. Because the components and structures are enumerated, cataloged and documented, organizations can experiment and adjust as they see fit to find the modes of operation that provide maximum value, the processes that work most efficiently in the context of their business and the elements that are the best cultural fit.

The practice of good governance provides the direction needed to achieve the desired outcome. When a GEIT program is initiated effectively, the pain points and trigger events, their causes, and the desired end state are clearly understood. The business case and buy-in from executive leadership and peer functions set the foundation such that the desired state can be achieved.

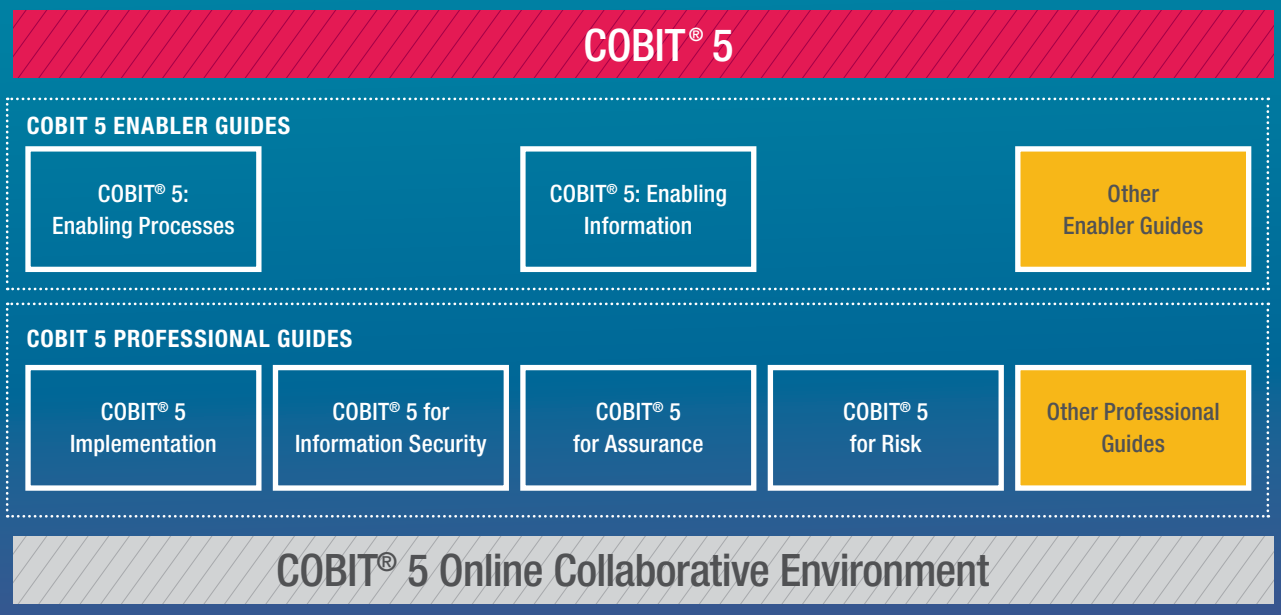
Practical Examples of Using a GEIT Framework

By using pain points or trigger events as the launching point for GEIT initiatives, the business case for GEIT improvement can be related to real-world issues, which will increase buy-in. Some practical examples for implementing a GEIT framework are:

- **Listing in the stock exchange**. A privately owned company is planning to go public and become listed on a stock exchange, which requires increased compliance with regulations. This firm can use an integrated framework to implement GEIT with specific organizational structures and processes in place as per regulatory requirements.
- **Venture funding**. A three-year-old e-commerce start-up company has garnered significant market share and carved a niche in the market with its unique product and service offerings. The founders have decided to pursue venture funding to scale up their operations. As one of the conditions of investment, the investors have advised the founders to implement a governance, risk and compliance (GRC) framework to mitigate risk and ensure systemic growth with appropriate compliance processes and systems in place.
- **Acquisition of a new company**. A firm has recently acquired a software products company. The employees, products and services of the acquired company had ad hoc systems and processes. The acquirer wishes to integrate the new company by implementing its own well-established governance and management processes.
- **Security breach in a financial institution**. A bank has recently encountered a serious security breach perpetrated by hackers that resulted in heavy penalties by regulators and a significant negative impact on the bank's reputation. The board of directors has appointed external consultants, working with an internal steering committee, to implement a robust GRC framework to effectively mitigate risk, build in resiliency and ensure compliance. COBIT 5 is to be used with other relevant frameworks to meet the enterprise objective of providing effective GEIT.

FIGURE 4

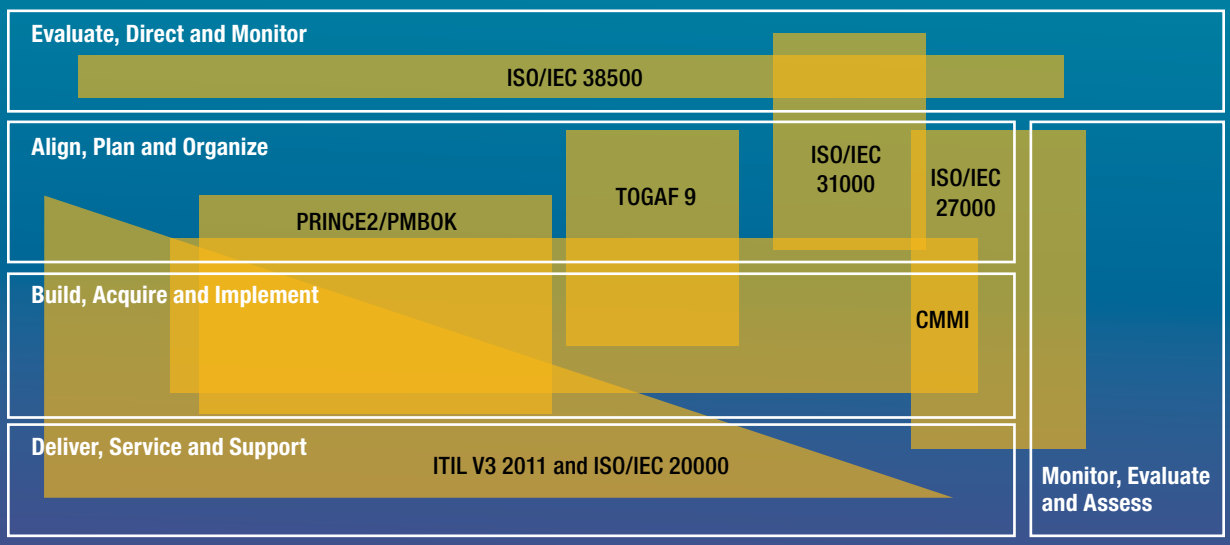
COBIT 5 Family of Publications



SOURCE: ISACA, *COBIT 5,* USA, 2012, figure 1

FIGURE 5

Relative Coverage Between COBIT 5 and Other Standards and Frameworks



SOURCE: ISACA, *COBIT 5,* USA, 2012, figure 25

Existing GEIT Frameworks

Given the many elements and objectives of GEIT, it is not surprising that multiple frameworks exist to address its different components. Some common GEIT frameworks are discussed below.

COBIT 5 is a comprehensive governance and management framework that allows the user to structure and align enterprise resources with the requirements of stakeholders. COBIT 5 provides a generic framework that can be useful for enterprises of all sizes. COBIT 5 also includes supporting publications that focus on specific areas, such as information security, assurance and risk (**figure 4**).

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 38500:2015 *Information technology—Governance of IT for the organization*, provides detailed guidance on IT governance as a subset of corporate governance. The publication can be applied to the governance of an enterprise's current and future use of IT and can be used to help to promote effective and efficient use of IT. **ISO/IEC TS 38501:2015**, *Information technology—Governance of IT—Implementation guide*, provides additional guidance on implementing GEIT within the organization.

In addition, ISO publishes standards that can be used to improve IT processes. Relevant to GEIT implementation are the ISO 2700x family of standards on information security techniques, the ISO/IEC 2000x series on IT service management and the ISO 900x series on quality management.

The **Information Technology Infrastructure Library (ITIL)** provides a set of IT service management practices, including alignment of IT services with the needs of the business. Its focus is on service management and service delivery. It is organized around a service life cycle, which includes service strategy, service design, service transition, service operation and continual service improvement. Guides are available that outline each of these processes in the life cycle.

The Committee of Sponsoring Organizations of the Treadway Committee (COSO)'s ***Internal Control—Integrated Framework*** is a framework focused on designing, implementing, conducting and evaluating the effectiveness of internal control. The framework looks at the interactions of the board of directors, management, external stakeholders and others, and their roles and responsibilities within the enterprise. COSO also issues ***Enterprise Risk Management—Integrated Framework***, which provides a framework for identifying and managing risk that may interfere with the enterprise's ability to achieve its strategic goals.

The Open Group Architecture Framework (TOGAF®) focuses on determining what the enterprise architecture should look like and then maintaining that architecture in a way that is flexible enough to allow the enterprise to readily adapt to change. It provides a methodology and framework for enterprise architecture to ensure consistency in methods, standards and communication.[6]

Selecting a Framework

With a wide variety of frameworks and information available, selecting the framework that works for the organization can seem to be a daunting task. Which is the correct one to choose? In reality, it is not as difficult as it might seem on the surface because many of the frameworks complement each other and can be used together to provide a more robust foundation on which to build a GEIT initiative.

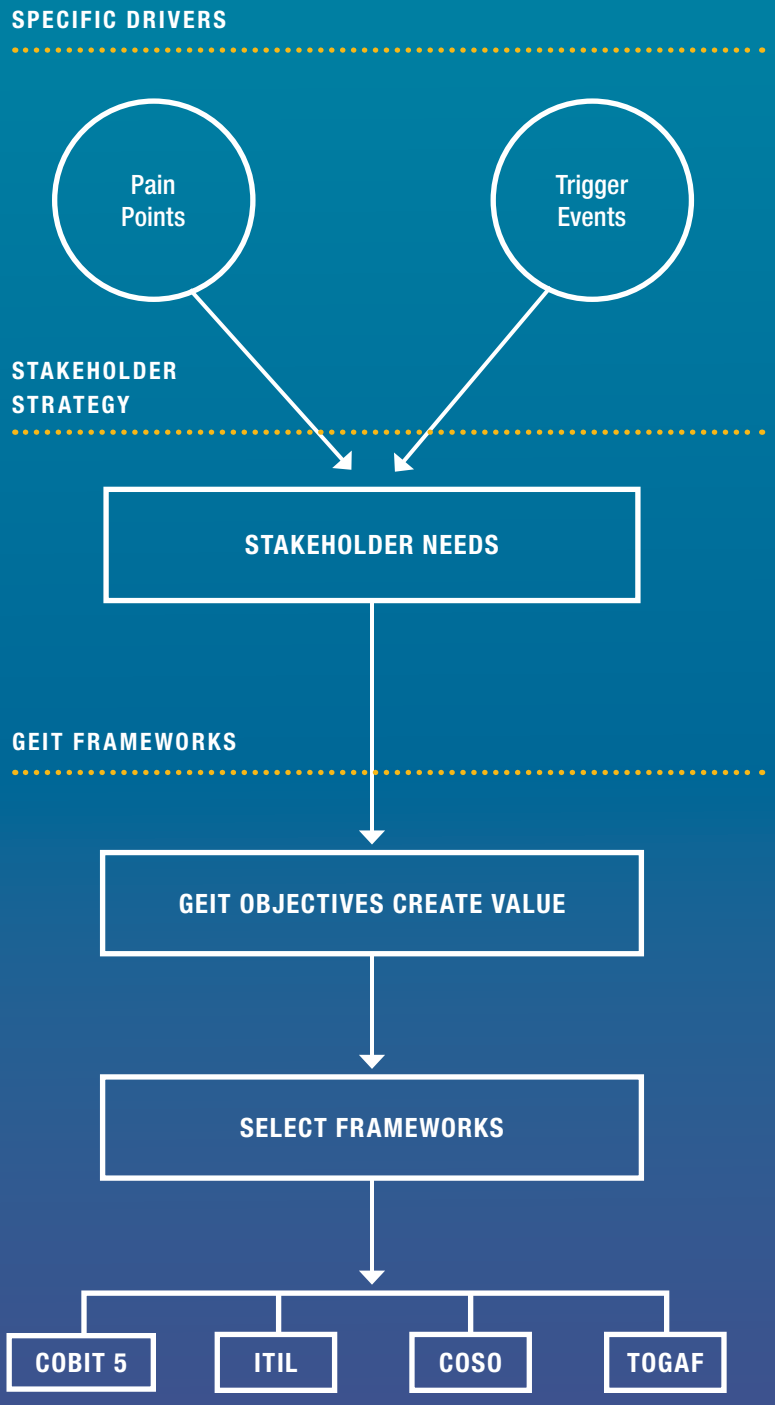
This same approach can be used with governance structures and frameworks that may be uncovered within the environment when evaluating current state.

For example, ISACA's white paper, ***Relating the COSO Internal Control—Integrated Framework and COBIT***, explains the relationship between the two frameworks and how they can effectively be used together. The frameworks are complementary and compatible to support the assessment and improvement of internal control practices and activities within the governance and management arrangements

6 The Open Group, *TOGAF® Version 9.1 Enterprise Edition: An Introduction,* USA, 2011

FIGURE 6

Initiating GEIT



of an enterprise. However, the effective use of both frameworks requires professional judgment and effort by enterprise management and its auditors and advisors to comprehend, adapt and apply the principles and guidance to specific enterprise goals and enterprise capabilities. *Relating the COSO Internal Control—Integrated Framework and COBIT* provides support for such professional judgment.

Figure 5 provides an example of how COBIT 5 fits with other available standards and frameworks.

When selecting the appropriate framework or mix of frameworks, it is important to understand the drivers for developing a GEIT structure and what it must accomplish. These elements can help in selecting the most appropriate framework(s). For example, for a publicly traded company operating in the United States, the trigger event may be compliance with Sarbanes-Oxley regulations. A concern would be demonstrating the effectiveness of internal controls; therefore, the COSO framework would be a good starting point.

Regardless of the framework selected, it must be carefully understood and then modified as needed to fit the enterprise. These changes and modifications will become evident as the project continues to move through the implementation process. The process for analyzing drivers through selecting a framework is presented in **figure 6**.

ACTION ITEMS:

- ☐ Crystallize issues/opportunities at hand and engage appropriate stakeholders. Appendix C contains a list of questions that can be used when interviewing stakeholders.
- ☐ Ensure fluid, bidirectional communication to all impacted areas to socialize the need and enhance benefit understanding.
- ☐ Ensure the purpose statement for the business case includes a discussion of the pain points or trigger events identified in support of implementing GEIT.
- ☐ Gain understanding of current frameworks being used for governance, risk management and compliance.
- ☐ Using identified stakeholder needs, select the framework (or group of frameworks) that can be most appropriate to use in the enterprise.

An example of a real-world issue that generated a need for improved governance and adoption of a framework can be seen in our **Real-World Example**. As this is an actual GEIT implementation, the example will be discussed in each chapter to show progression through the GEIT initiative implementation process.

REAL-WORLD EXAMPLE

Financial Institution: Pain Points of Expansion

A large global financial services institution doing business in the United States expanded its product portfolio. In doing so, the legal department was notified that the institution was subject to additional oversight and regulation. The organization had previously been struggling with problematic internal and external audit findings with significant deficiencies found in its IT and outsourced environments. The legal, compliance and enterprise risk management functions raised the issue to the enterprise risk committee.

3

Creating a Plan for GEIT

Once key stakeholders have been interviewed and an understanding of their needs and the event(s) that have triggered the need to implement GEIT captured, a determination of the organization's current state with respect to GEIT can be developed. This, coupled with where the organization needs to be to satisfy goals and create value, will illustrate the gap between the two states.

These steps in the GEIT implementation process help provide input into the development of a project plan for implementing GEIT. It is also an important precursor activity as it helps to identify the gaps between how well an enterprise is employing GEIT versus the desired state and, based on understanding the risk, benefits and resource requirements, can help prioritize the project team's efforts and governance focus as a whole.

Forming the Project Team

A project team should be established to take temporary ownership of getting the right GEIT elements in place. It will then define the boundaries of the project and develop an appropriate project plan. The team will gather and analyze information that is uncovered during the next steps of GEIT implementation.

A GEIT project team should include members from the appropriate areas of the business and IT. The following characteristics of team members should also be taken into consideration to ensure that the GEIT initiative will be able to achieve its goals:

- Level of knowledge and expertise
- Level of authority
- Experience
- Credibility

At this point it is also essential to ensure that the team has a clear understanding of the stakeholders' needs identified in the previous step, as this will drive the rest of the initiative.

The Current State of the Enterprise

Understanding the current state of IT governance within the enterprise as it relates to the needs and goals identified by critical enterprise stakeholders (discussed in chapter 2) is essential for helping define what needs to be done to implement GEIT. A current-state

assessment enables an understanding of the status and maturity of the processes in place.

In this stage, a thorough analysis of the enterprise's existing resources must be performed to determine what is already in place. Some resources to examine include:

- Process workflows/documents
- Control activities and control frameworks
- Existing controls and matrices
- Policies
- Procedures
- Processes

This stage also provides an opportunity to map IT goals and enterprise goals to see how they currently relate to one another. When reviewing existing resources, it is necessary to identify critical processes, roles and responsibilities, and other factors to determine if there are deficiencies.

One technique that could be useful is a strengths, weaknesses, opportunities and threats (SWOT) analysis. SWOT is a strategic planning method used to evaluate the strengths, weaknesses, opportunities and threats involved in a project or in a business venture. It involves specifying the objective of the business venture or project and identifying the internal and external factors that are favorable and unfavorable to achieving that objective.

Performing a SWOT analysis requires determining the possible elements that fit into each of the four analytical categories for the enterprise. Strengths, weaknesses, opportunities and threats are either internal or external to the enterprise and either hurt or help the enterprise. Strengths are internal to the enterprise and may help achieve enterprise goals. Weaknesses are also internal but hinder or hurt the enterprise's ability to accomplish its goals. Opportunities are external events or circumstances that would help the enterprise if they could be taken advantage of, and threats would likely hurt the enterprise if they occurred.

Good-practice approaches to SWOT analyses include the following:

- Evaluate current methods of identifying and satisfying regulatory needs and changes.
- Evaluate current methods of aligning IT processes and technologies to changes in enterprise goals, regulatory requirements and business needs.
- Evaluate currently used frameworks and identify areas for synergy.

REAL-WORLD EXAMPLE

Financial Institution: Socializing the Challenge

Once the financial institution gained agreement from the enterprise risk committee, a business case was developed by the operational risk management organization and approved. The business case identified all stakeholder areas involved and established the overall mission and time line to achieve for each stakeholder area. The overall goals defined by the enterprise included:

1. A more streamlined approach to satisfying new regulatory requirements
2. Increased alignment of IT processes to overall regulatory requirements and business innovation
3. The establishment of an overarching governance framework to align existing frameworks and to enable achievement of regulatory and business drivers

Each stakeholder area was then charged with developing a cross-functional core team and associated project teams and work streams as needed for each area.

REAL-WORLD EXAMPLE

Financial Institution: Current-state Assessment of GEIT

Because the areas of concern or interest (based on the goals and mission statement established in the business case) centered principally around compliance and IT alignment with business strategy, the core team decided to follow a phased approach and assess the process maturity in these areas within the respective functions: audit and assurance and IT service delivery. A high-level SWOT analysis was performed to gain an understanding of how the enterprise objectives were achieved, how direction was set and how performance was monitored against objectives. From here, a detailed assessment of each area was planned and key stakeholders identified for interview.

	HELPFUL	HARMFUL
INTERNAL	**Strengths** > COBIT 4.1 used by audit/assurance > Culture supportive of change/innovation	**Weakness** > Other audit frameworks utilized in tandem (SOX) > IT areas subscribed to multiple self-assessment processes > Lack of alignment to overall enterprise goals—reactionary
EXTERNAL	**Opportunities** > COBIT 5 for governance and management of IT	**Threats** > Increasing regulation

The Desired State of the Enterprise

The desired state of the enterprise is state in which the enterprise wishes to be at the end of the GEIT initiative—the end target state. Whether it is to better demonstrate compliance with regulatory requirements or decrease operational inefficiencies, the desired state is set by the needs of the stakeholders.

In essence, at the end of the process, the enterprise will want to be able to say to its stakeholders that it has delivered value—and be able to prove that this is the case in a language and format the stakeholders can understand. As with the business case, this means that the specific outcomes should be identified using the same metrics and criteria that the business can best understand; for example, if the culture of the organization is such that economic benefits are paramount, expression of positive outcomes in financial terms (e.g., profitability increase or reduction in expenses associated with overhead) might be most effective. If the organization is one that prioritizes transparency (as in a public sector context), transparency-related enhancements might be the optimal set of outcomes to emphasize.

Once the desired state is identified, a gap analysis is necessary to identify what gaps exist between the current state and the desired state. Typically, this is accomplished by

working backwards from the end target to the current state to determine the steps needed to accomplish the objectives. In other words, what specific actions (at a high level) must be effected to get from the current state to the desired state? The end result of this exercise consists of deliverables, projects and milestones that can be incorporated into a formal project plan for GEIT.

Develop a Road Map and Plan

Identifying the gaps between the enterprise's current state and desired state yields a set of tasks that must be completed to bridge the gaps. These are used to develop the GEIT implementation plan.

The implementation plan outlines the steps that will be taken, the individual(s) responsible, the time line and dependencies, and the resources needed to complete the project. It acts as a project charter and provides authority to the project team members conducting the implementation. This is necessary because resources will be needed from various areas in the enterprise and their managers must be committed to making them available.

Project management becomes key at this stage of the GEIT implementation process. Use of an established project methodology can help ensure reasonable use of resources and control of implementation project deliverables, budget and timing. The specific project management methodology followed is less important than ensuring that the methodology is a comfortable fit for the organization, provides reliable visibility and accountability for tasks, and includes a mechanism to account for unexpected developments midstream. An example of a project methodology framework is PRINCE2 (*www.axelos.com*), which provides a common vocabulary and approach to any type of project. It also provides a process model for managing a project that could be useful when developing the GEIT plan.

The project plan developed in this stage also defines the boundaries and scope of the project and helps to determine when the GEIT initiative is finished. One consideration is to include evaluation periods at milestones in the project that include go or no-go discussions. This can help to determine if the project is on track or achieving its goals.

If a framework is in use, an important consideration is to customize it to the organization. The framework provides a guide and structure for the initiative; however, it is important to figure out what elements are relevant to the current initiative and focus on only those. Not all elements may be necessary, and including them would use resources that could be better used elsewhere.

If a project team has not been assembled prior to this step, it is essential to do so before moving forward. The project sponsor, as described previously, should have the authority to ensure the project will have the resources available to achieve the goals of GEIT. When developing the project plan, it is critical to engage the appropriate personnel and assign them to project tasks to effect change in the enterprise.

Understanding Available and Necessary Resources and Processes

Enterprise resources must be tied to processes in the internal control environment, which provides the enterprise the means to ensure that risk is managed appropriately and resources are used effectively.

Connecting resources to processes will ideally follow the results of a risk assessment. This risk assessment identifies the potential risk areas that face the organization and documents the impact, severity and potential undesirable outcomes for the organization as a result. The scope of the risk assessment could be to enable the organization to select which areas need to be improved based on the data gathered in the SWOT analysis and interviews and help prioritize based on the residual risk that remains after the effectiveness of the control environment are evaluated.

Risk assessments and monitoring should also be performed for the implementation of the GEIT initiative to ensure that program risk—whether it is resource commitments, budgeting or schedule—is addressed to keep the program on track. As the GEIT framework is implemented and as more direct IT management processes are defined, a risk assessment can also be utilized to help

Risk assessments and monitoring should also be performed for the implementation of the GEIT initiative to ensure that program risk—whether it is resource commitments, budgeting or schedule—is addressed to keep the program on track.

FIGURE 7

GEIT Risk Assessment Heat Map

1/ **External Factors:** Trends in business and external factors are not analyzed causing poor governance.

2/ **IT Engagement:** The significance of IT and its role with respect to the business is not determined leading to poor engagement.

3/ **Enterprise Controls:** The implications of the overall enterprise control environment with respect to IT is not determined causing poorly defined IT controls.

4/ **Reward System:** The establishment of a reward system is not established leading to poor adoption of cultural change.

5/ **IT Resources:** IT-enabled investments, service and assets are poorly managed and are not aligned with the value creation causing inefficient spend.

6/ **IT Risk Strategy:** IT risk strategy is not aligned to enterprise risk strategy causing improper handling of risk.

7/ **Value delivery:** Value delivery goals are not defined or communicated causing ineffective monitoring.

KEY	L = Low M = Medium H = High VH = Very High

prioritize the creation or improvement of those processes critical to the success of achieving the IT governance objectives **(figure 7)**.

Done well, the implementation of GEIT uses a risk assessment to inform the GEIT project team what is needed. Risk areas can and will impact the ultimate outcomes that the GEIT initiative is trying to achieve, so the implementation should account for the risk and design in ways to address it.

It is advisable to document only the level of GEIT detail the enterprise needs. In particular, the functional areas, domains, processes and practices should be defined only to the extent that users in the enterprise need these terms to achieve the governance goals at hand, always bearing in mind that a common language is an important aspect of a successful framework implementation.

Selecting Relevant Content From a GEIT Framework

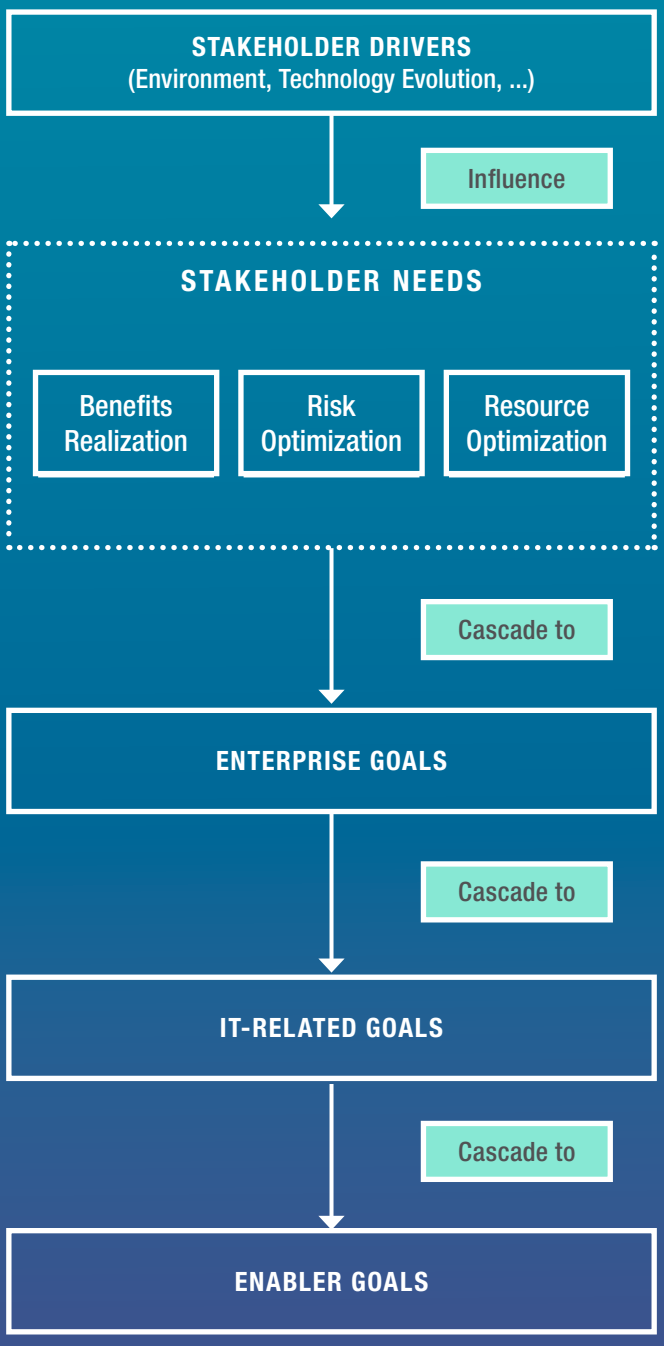
Determining which elements of the framework the enterprise needs is done via a thorough examination of stakeholder requirements, as defined in the business case and outlined in the project plan. These requirements (which comprise the desired state) determine all enterprise goals that follow, and the enterprise goals make clear what other goals, IT and other resources (enablers) are required. For example, the goals cascade of COBIT 5 (**figure 8**) can be used to relate how these goals directly correlate to governance objectives (benefits realization, risk optimization and resource optimization), while simultaneously aligning with the related IT goals that need to be prioritized to meet these needs.

The elements of a framework should be selected after a thorough review of stakeholder needs, keeping in mind the scope and objectives. There are multiple approaches to navigating and selecting relevant processes, practices and activities in order to customize for use. An example of determining effective IT goals to best achieve the governance objectives can be seen using the COBIT 5 goals cascade (**figure 8**).

COBIT 5 provides a top-down approach to the alignment of IT goals to stakeholder

FIGURE 8

COBIT 5 Goals Cascade



SOURCE: ISACA, *COBIT 5,* USA, 2012, figure 4

drivers. Many of the activities and action steps discussed in previous chapters are summarized by the COBIT 5 goals cascade process:

1. Identify stakeholder needs and, based on this information, select relevant governance objectives. COBIT 5 encapsulates governance objectives into three main areas: benefits realization, risk optimization and resource optimization.
2. Based on the governance objectives, select the relevant enterprise goals from the list of 17 enterprise goals detailed in COBIT 5.
3. Based on the selected enterprise goals, select relevant IT-related goals from the list of 17 IT-related goals illustrated in figure 22 of the COBIT 5 framework.
4. Review the relationship level—primary (P) or secondary (S)—assigned to the selected IT-related goals to identify relevant COBIT 5 processes. Goals with primary relationships should be strongly considered; those with secondary relationships can also be considered if deemed relevant to achieving additional benefits.
5. Review the contents of the resulting list of IT goals. Evaluate against the requirements defined from the gap analysis and risk assessment process and further filter based on relevance.
6. Use the related contents (process description, purpose, goals cascade, process goals and related metrics, RACI [responsible, accountable, consulted, informed] charts, practices with input-output document references, and lists of activities and related guidance) to prepare the benchmark of COBIT 5 as applicable to the governance goals defined.
7. Customize these extracted contents of COBIT 5 as relevant to the enterprise's requirements by integrating with other frameworks and internal practices. Also, ensure that this content is aligned with existing policies, procedures, practices and guidelines of the enterprise.

Any form of a goals cascade approach needs to carried out carefully, and the identified processes from this approach must be validated and filtered based on relevance, risk and benefit realization. Users may start from an enterprise goals mapping level (top-down) or an IT-related goals mapping (bottom-up based on strategies, existing projects, etc., that align to governance objectives) and select the relevant IT processes if greater detail is not available in the goal-setting process.

The purpose of validation is to ensure that the processes selected serve to deliver the value required of them. The selection of processes occurs from following enterprise goals down into the base of resources (enablers). Misalignment should not occur, but it can happen. It is prudent to validate the selection of resources and ensure that there is a reasonable likelihood that their employment will cause the satisfaction of stakeholders' needs. Filtering selected resources (processes, in this case) is a part of the validation.

REAL-WORLD EXAMPLE

Financial Institution: Goals Cascade

The overall goals defined by the enterprise include:

1. A more streamlined approach to satisfying new regulatory requirements
2. Increased alignment of IT processes to overall regulatory requirements and business innovation
3. The establishment of an overarching governance framework to align existing frameworks and enable achievement of regulatory and business drivers

The current-state assessment enabled the financial institution to gauge its current strengths and weaknesses in its ability to achieve these goals. Recognizing COBIT 5 as an opportunity in the SWOT analysis helped the institution solidify the decision to migrate from the existing approaches (COBIT 4.1, multiple assessment techniques) to COBIT 5 as a GEIT framework. The COBIT 5 goals cascade and enabler guides helped the financial institution prioritize the efforts across the enterprise. Based on the enterprise goals, the financial institution core team decided that two IT-related goals should be prioritized:

1. Alignment of IT and business strategy
2. IT compliance and support for business compliance with external laws and regulations

Example: Applying COBIT 5 to Implementing GEIT Using the Goals Cascade

Note: This section provides an example of how to develop an implementation plan using COBIT 5 as the guiding framework. While this section focuses on COBIT 5, the concepts discussed can be applied to the use of other frameworks. If the enterprise selects another framework for use, instead of COBIT 5, the documentation associated with that framework should be consulted for assistance in carrying out the tasks described in this section.

Since the overall goals were identified in the business case and appropriate approval was obtained, the next step is to determine which COBIT 5 processes and activities should be prioritized to satisfy enterprise goals. For GEIT implementations that are based on COBIT 5, the *COBIT® 5: Enabling Processes* publication can be very helpful in drafting the implementation plan. It provides a brief introduction to the COBIT 5 concepts and provides the comprehensive description and components of the processes enabler.

An example of following the goals cascade is to start with one particular enterprise goal and follow it down to the related enabler goal(s). The goals cascade starts with enterprise goals as aligned with the balanced scorecard (BSC) dimensions.[7] In this example, figure 22 in the COBIT 5 framework publication is used and enterprise goal number 5, Financial transparency, is selected.

From there, figure 22 is used to find all primary IT-related goals for this enterprise goal. In this case there is only one: IT-related goal number 06, Transparency of IT costs, benefits and risk, corresponding to the financial BSC dimension.

By using figure 23 in the COBIT 5 framework document, it is possible to review IT-related goal number 06 as to corresponding processes that both primarily and secondarily contribute to this goal. A scan down the column reveals all primary COBIT 5 processes that are needed to support this goal: EDM02, EDM03, EDM05, APO06, APO12, APO13 and BAI09.

COBIT 5 includes five domains, each with associated processes and practices relevant to the domain. Each process in the *COBIT 5: Enabling Processes* publication is defined and has a clear statement of its purpose. The process references the IT-related goals it supports and defines metrics to measure the achievement of these goals. Each process also has a goal, and sample metrics are supplied to measure the goal's achievement. The RACI chart assigns levels of involvement to different roles. Practices for each process are described and sources of related guidance are provided.

Based on the goals the organization would like to achieve, COBIT 5 can be used to map the business goals and IT-related goals to determine a process or practice to work toward. The process of moving from needs capture through the GEIT road map to the identification of enabler goals is depicted in **figure 9**.

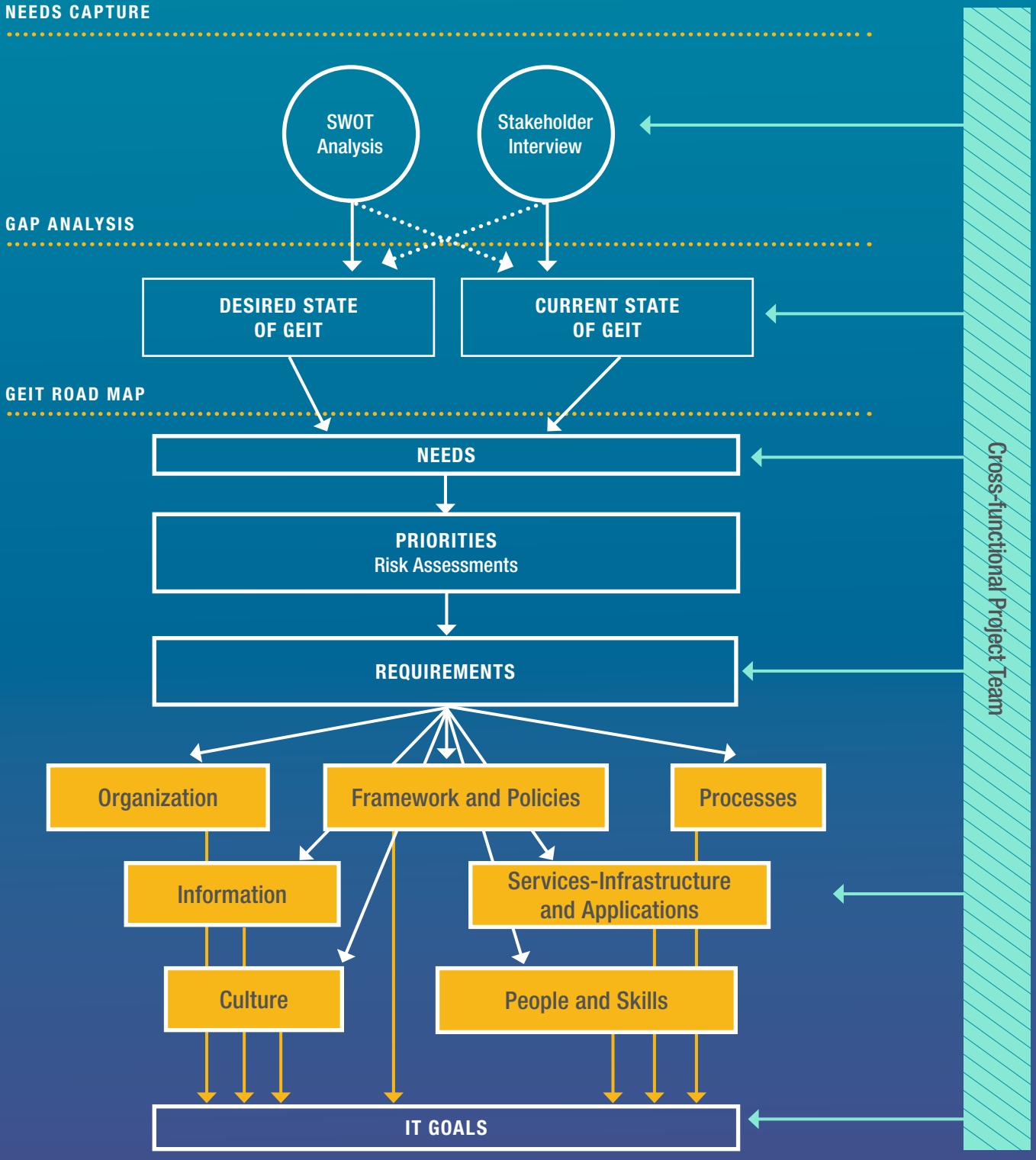
Whatever approach is used, it is important to validate and customize the contents based on relevance. After the processes are selected and the scope of implementation is agreed upon, based on pain points, trigger events or key benefits, the contents extracted from the processes can be customized and used as a benchmark for implementing GEIT within the enterprise.

COBIT 5 includes five domains, each with associated processes and practices relevant to the domain. Each process in the COBIT 5: Enabling Processes *publication is defined and has a clear statement of its purpose.*

7 Kaplan, Robert S.; David P. Norton; *The Balanced Scorecard: Translating Strategy* into Action, Harvard Business Review Press, USA, 1996

FIGURE 9

GEIT Program Planning



REAL-WORLD EXAMPLE

Financial Institution: GEIT Implementation

In migrating from COBIT® 4.1 to COBIT 5, the core team and project teams realize that COBIT 5 activities are equivalent to the COBIT 4.1 control practices and the management practices contained in the COBIT 4.1-related publications specific to value creation and risk management (Val IT and Risk IT). COBIT 5 is based on a revised process reference model with a new governance domain and several new and modified processes that now cover enterprise activities end to end—i.e., business and IT function areas. Because of this, additional practices and processes needed to be defined and existing COBIT 4.1 practices mapped. All COBIT 4.1 control objectives that mapped to the COBIT 5 processes that were prioritized would need to be evaluated across all enabler dimensions. Also any additional frameworks in place (SOX, ITIL) were recognized as also needing to be mapped and evaluated.

In focusing on the Processes enabler, the core team identified the following enabling processes as primary to the achievement of the enterprise goals and their related COBIT 4.1 counterparts:

IT-RELATED GOAL 1:
Alignment of IT and business strategy

COBIT 5 (PRIMARY)		COBIT 4.1 AND VAL IT		
EDM01	APO05	PO1	VG6	IM2
EDM02	APO07	PO3	PM1	IM3
APO01	BA101	ME4	PM2	IM4
APO02	BA102	VG1	PM3	IM5
APO03		VG3	PM4	
		VG5	IM1	

IT-RELATED GOAL 2:
IT compliance and support for business compliance with external laws and regulations

COBIT 5 (PRIMARY)		COBIT 4.1 AND VAL IT	
APO02	BA110	PO2	IM10
APO12	MEA02	PO3	RE1
APO13	MEA03	PO4	RE2
		DS9	RE3
		VG2	

ACTION ITEMS:

- ☐ Assemble the project team. Hold a kickoff meeting to ensure that everyone understands the goals and the purpose of the GEIT initiative.
- ☐ Perform a current-state analysis. Conduct interviews, review existing documentation, perform a SWOT analysis, etc., to identify where the enterprise is currently. See appendix C for tips on conducting interviews.
- ☐ Analyze stakeholder needs to determine the enterprise's desired state. Perform a gap analysis to determine where deficiencies lie. Perform risk assessments as needed to help prioritize and manage project risk.
- ☐ Determine requirements for the supporting structures and processes in order to help identify relevant IT goals.
- ☐ Have the project team create an implementation plan that shows all supporting plans (communication, procurement, etc.) that will be needed to implement GEIT. This can be accomplished in a phased approach and can be partitioned into multiple workstreams to represent the support of the stakeholders involved.
- ☐ Identify specific milestones to demonstrate accomplishment of each implementation phase and report on same. Create project continuation plans or departure points if needed.
- ☐ Deliver the plan to the project sponsor and core team and ask for approval to move forward with the overall GEIT plan.

4

Execute the GEIT Plan

After the plan has been created and approved, it is time to put the GEIT initiative into action. Essential to this step is ensuring that the enterprise is ready for the GEIT implementation, communicating the scope of the plan to the enterprise and confirming that the activities are still tied back to stakeholders' needs. Revisiting the pain points and trigger events will help ensure that both the governance objectives and stakeholder requirements are being met.

Creating the Environment

Even though support is in place for GEIT, the enterprise may still not yet be ready for implementation. For example, there may be competing priorities that need to be resolved before the implementation can proceed, or the resources required to implement may not be readily available. Therefore, the organization must be readied for the implementation to start.

The project plan developed in the prior step should provide an idea of the level of effort and investment required. If the organization is not yet ready to make the investment, plans may need to be deferred until the situation changes and the tactical barriers are removed.

Communication is key to the success of any project, including GEIT implementation. Prior to executing the plan, the enterprise must understand and be on board with the changes that are to come. As discussed in chapter 1, articulating the benefits in terms that the stakeholders recognize helped garner support and buy-in.

At this point in the implementation, continued support from the top down must be reinforced. The vision for the GEIT plan should be communicated clearly and simply so all levels of the enterprise can understand why these changes are being made. This can take the form of a formal presentation to staff at a town hall meeting or involve meetings with key individuals and organizations within the enterprise.

It is also key to encourage feedback and suggestions for improvement and to act on that feedback, so those providing feedback feel they have been heard. This will help to ensure that enthusiasm and buy-in are maintained throughout the execution of the plan.

Effective communication can also help to establish the authority of the project team. It will let the members of the enterprise know that this initiative is supported by and important to senior leadership, which, in turn, can better enable the project team to execute the project plan.

It is also necessary to acquire and position the proper resources in place for the plan to succeed. This can include ensuring that key

personnel are free to work on their assigned tasks or necessary software or physical resources are purchased or designated for use in the project. Just as any project includes a resource allocation phase, so too should the implementation of GEIT be appropriately staffed and resourced prior to execution.

Executing the Plan

With the environment ready, it is now time to make the changes to the organization by executing the tasks and steps outlined in the project plan. This phase of implementation is typically the longest and most involved, but the time frame should be reasonable in order to be manageable and deliver benefits.

Essentially, this step is maintained through good project management skills. If the organization has a project management office (PMO), the project team may wish to leverage the PMO's knowledge and expertise to help the GEIT initiative move into the execution stage.

Of particular importance here is establishing the authority of the project. Two techniques can be useful in achieving that objective: identifying a significant project champion who has the authority to direct resources to participate in the GEIT implementation project and developing a project charter that explicitly states the authority of the project to proceed and use resources.

A few keys elements to effectively manage this stage include:

- Keep the business case and project plan up to date so the plan can continue to operate based on the current situation.
- Build quick wins into the program to keep momentum going from the initial communications. Recognize and reward those involved in achieving the quick wins. Communicate these wins in project communications or more broadly on internal portals or postings.
- Make sure that "success" in this context is clearly defined and communicated.
- Clearly communicate roles and responsibilities for use.
- Be prepared to handle issues related to transition and change (i.e., addressing concerns related to changes in reporting/responsibility/authority or handling new expectations).
- Provide regular updates to stakeholders so they know the program is progressing and remains on track.
- Monitor risk and issues related to executing the project plan and develop means for remediation if needed.
- Approve and manage any changes to the plan.

Ensuring that the project stays in scope can be an issue when implementing GEIT. This could lead to a failure to realize the goals of the implementation plan and to enable the appropriate governance of IT to reduce pain points and trigger events that may have been the initial need.

Contributing factors to this could be trying to do too much too soon, not understanding the scope of the project, creating something from scratch rather than using what already exists and failing to appreciate the organization's capacity to absorb change. Employing the techniques listed previously can help to keep the project in scope and moving forward.

As noted in creating the environment for GEIT, a key component of executing the plan is ensuring communication to key stakeholders. These groups should be asked how often and via what method they would like to receive communication. Some stakeholders may prefer a quick dashboard that is emailed to them weekly, whereas others need only a memo or summary sent to them on a monthly basis or presented at a monthly meeting. This can keep stakeholders enthusiastic about the project and can help in gaining additional assistance and support if an issue should arise. Keep in mind though that having a custom-developed reporting methodology for every possible stakeholder could become time-consuming; therefore, depending on the quantity of stakeholders, a "menu" of possible communication options can help streamline this aspect of the execution in the event that large numbers of stakeholders need to stay informed.

This phase of the project ends when all milestones and tasks listed in the project schedule have been completed.

Of particular importance here is establishing the authority of the project. Two techniques can be useful in achieving that objective: identifying a significant project champion who has the authority to direct resources to participate in the GEIT implementation project and developing a project charter that explicitly states the authority of the project to proceed and use resources.

ACTION ITEMS:

- ☐ Identify any potential barriers to the success of the GEIT initiative. Discuss these barriers with key individuals and develop a plan for resolving these issues prior to executing the project plan.
- ☐ Develop and execute a communication plan for the GEIT initiative that can be delivered to the entire enterprise. This should include how and when information is communicated, including any customization (e.g., to smaller groups for key players or general communication for enterprisewide buy-in).
- ☐ Ensure that efforts are appropriately resourced and resources have been committed to the tasks outlined in the plan.
- ☐ Monitor the progress of the GEIT implementation plan using project management good practices.
- ☐ Develop a communication plan for how and when to update key stakeholders on the progress of the initiative.

5

Continuous Improvement, Evaluation and Wrapping It Up

A completed project plan signals the end of the bulk of the work for a GEIT implementation. However, even after the hard work is done, there are still a few steps to take to ensure that the GEIT initiative has achieved the goals outlined in previous steps. This includes continuous improvement and a review of the GEIT implementation project.

Going From a Project to Business as Usual

At the completion of the project plan, the hope is that the organization is realizing the positive results of all the hard work. New processes and procedures should be in place and achieving their desired goals. But how is success evaluated?

Essentially, overall performance can be monitored against the goals and objectives set in the business case, and investment can be measured in actual costs versus benefits of the initiative. Analysis of processes can also help to see if the enterprise has achieved the efficiencies that were sought at the beginning of the GEIT implementation project.

One way to determine success is to have defined critical success factors (CSFs). CSFs are key issues or actions that must go right if goals are to be attained. Like all metrics, these should be measurable so that it is easy to determine if the action has been successful. Metrics should be SMART:

- Specific—Based on a clearly understood goal; clear and concise
- Measurable—Able to be measured; quantifiable (objective), not subjective
- Attainable—Realistic; based on important goals and values
- Relevant—Directly related to a specific activity or goal
- Time-bound—Grounded in a specific time frame

The objective of this phase is to take these metrics and integrate them into the existing performance measurement system of the enterprise so the process can be monitored regularly. The changes made to move from the enterprise's current state to the desired state should be adopted into regular

REAL-WORLD EXAMPLE

Financial Institution: Communicating Status and Success

As alignment with existing frameworks and identification of key process progressed through the project, the core team identified key milestones to report on in terms of project status and also developed key performance indicators (KPIs) and key risk indicators (KRIs) that would help gauge their ability to achieve milestones that were directly related to the enterprise goals captured. The development of the KPIs and KRIs involved project resources as well as representatives from each stakeholder community. Status and achievements were reported to the project lead, the CIO and the CRO. A subset of the performance and risk indicators was presented to the enterprise risk committee.

KEY PERFORMANCE INDICATORS:

- Line of business satisfaction survey results associated with IT engagement
- Percent of business strategic initiatives supported by IT
- Percent of business initiatives engaging IT during requirements definition
- Percent of issues and action plans consolidated

KEY RISK INDICATORS:

- Significant deficiency change in audit findings
- Speed to market for new business initiatives

practice so they can be maintained and achieve the benefits desired. These changes should become part of the enterprise's culture (i.e., the way things are done).

Essentially, the project plan needs to transition from a one-time process to business as usual.

To aid in this transition, changes to already existing documents and processes—such as job descriptions, KPIs, reward systems and operating procedures—need to be made. The communication program developed in the previous step should also continue to keep the enterprise and key stakeholders aware of the ongoing integration of the changes. Proper roles and responsibilities must be assigned to maintain the changes to the enterprise and an escalation process \has been developed to resolve any outstanding issues when necessary.

Lessons learned are another key output at this stage. It is important to understand what went well and what did not succeed in order to continue to improve GEIT processes and build upon the initial success of the program. Documenting these can also help to prevent the enterprise from repeating a past mistake and illustrate how things could be done differently to achieve success in the future. This can be done at a formal wrap-up meeting where input from key personnel is gathered and recommendations are made for moving forward.

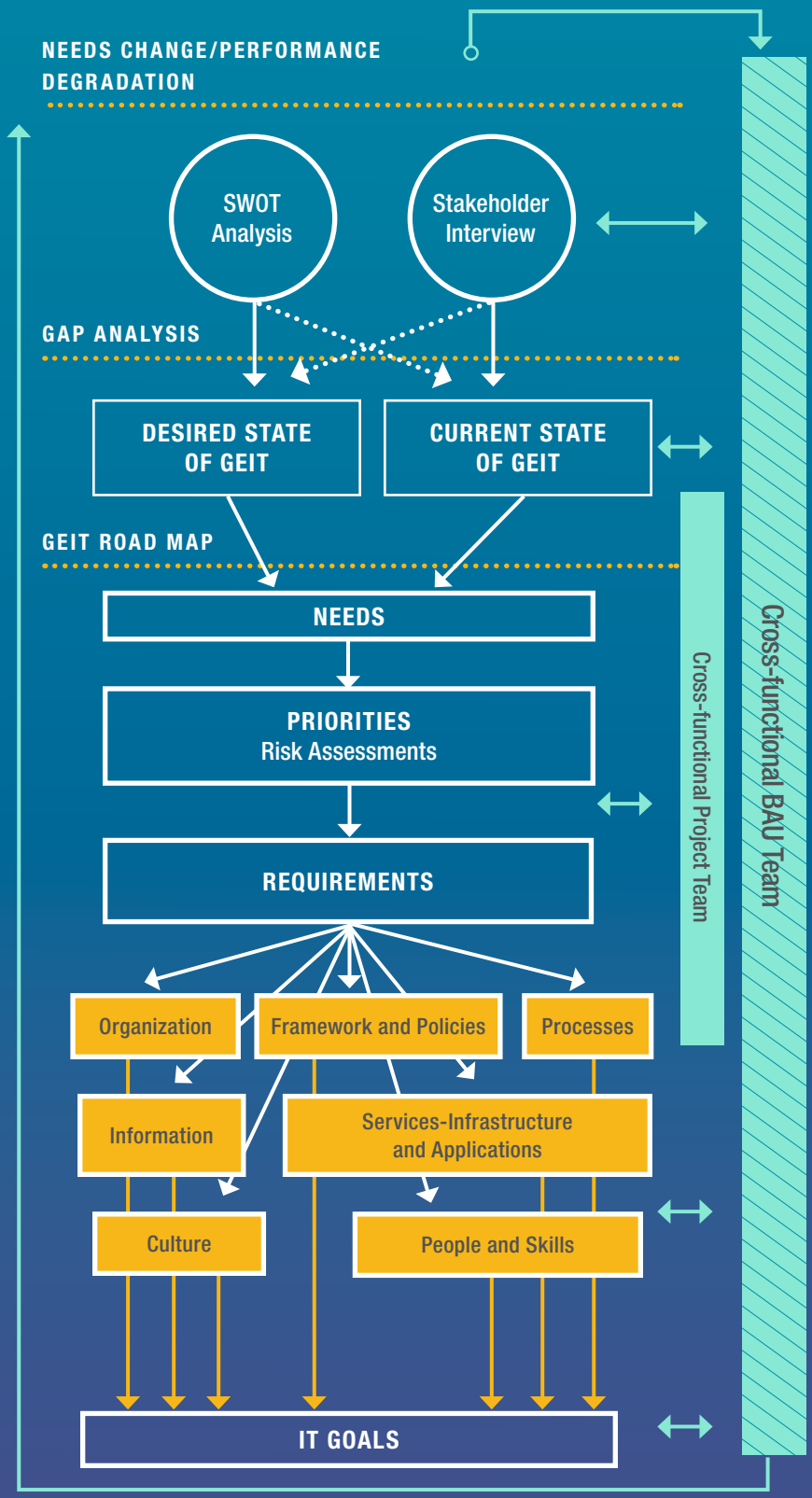
Establishing a Process Improvement Review

GEIT processes have been integrated into the enterprise's business as usual, lessons learned have been gathered and documented, and the GEIT implementation plan has been closed. It may seem that the implementation is completed. However, there is still one final phase to GEIT implementation: reviewing effectiveness.

To support the ongoing effectiveness of GEIT, it is important to establish a review cycle to ensure that the program is still delivering value to stakeholders. At a minimum, this should be done yearly. New requirements may arise that will need to be addressed, stakeholders' needs may change or other changes may occur that can affect the goals of GEIT. New objectives and requirements can trigger a current-/desired-state gap analysis, which continues the GEIT life cycle.

FIGURE 10

GEIT Monitoring and Improvement



The lessons learned should be reviewed to develop ways to improve processes. They contain valuable information for the enterprise that can be used in ongoing initiatives and improvement projects. Ongoing communication of successes and means for improvement can continue to drive and sustain motivation and investment in the GEIT initiative.

At the conclusion of this step, a sustainable plan for improvement and monitoring should be established to drive the ongoing success of GEIT in the enterprise. The process flow for program monitoring and improvement is shown in **figure 10**.

ACTION ITEMS:

- ☐ Schedule a project review meeting upon the completion of the items in the GEIT implementation plan. Evaluate CSFs and other metrics to determine the overall success of the plan. Document what went well, what could have been improved and what the next steps are.
- ☐ Review job descriptions, policies, processes, etc., and make revisions to ensure that GEIT processes and principles are integrated into business as usual.
- ☐ Review lessons learned at the project review meeting and analyze them to see what suggestions for improvement can be applied to a continuous improvement plan for GEIT.
- ☐ Schedule a later date (six months to one year) to review the GEIT program and meet with stakeholders to determine if their needs have changed.

Conclusion

GEIT can benefit enterprises in many ways. The main benefit is effective and efficient use of resources to deliver value.

While the task to align the IT organization with the goals and objectives of the enterprise as a whole can be daunting, following a few basic steps can make the process manageable.

This guide has provided a practical means to implementing GEIT in an organization. This stepwise approach can result in a means for the organization to document its effectiveness and efficiency so that it can continue to demonstrate to stakeholders that their needs are being met.

Once implemented, GEIT provides a method for ensuring alignment of IT with the business as well as a process that can be used to close gaps that may arise from changing stakeholder or regulatory requirements.

A

Case Studies in Applying GEIT

Note: All data provided in these examples are fictitious and used for illustrative purposes only.

Case 1: Illustrative Example Using GEIT for a Business Issue

SCENARIO

The stakeholders of a manufacturing enterprise have stated that one of the enterprise's competitive advantages is that it receives most-favored customer status from suppliers. This means the enterprise is able to secure the highest-quality goods at the most favorable prices.

The stakeholders of this enterprise have stated that this advantage must be maintained and, therefore, suppliers must always be paid in an accurate and timely manner. At present, there is no documentation to support that billings and payments are actually processed in this way. There have been instances in the past where suppliers have revoked the preferred customer status, and stakeholders are concerned about the scope of the enterprise's exposure to this happening again. The enterprise's governing bodies are now tasked with ensuring that this stakeholder requirement is satisfied.

USING GEIT TO SOLVE THE PROBLEM

Senior leaders of the enterprise must now evaluate the stakeholders' requirements and determine how best to satisfy them. Based on their evaluation, they must then direct the enterprise managers to effect a solution. After the solution is in place, it must be monitored to ensure it is providing the desired results.

EVALUATE

The stakeholder requirement is that suppliers be paid in an accurate and timely manner. First, these terms must be clearly and unambiguously defined.

To determine the accuracy of payments, senior leadership analyzed the enterprise's history of payments, the number of suppliers with which the enterprise conducts business, the value of those transactions and the density of payments (i.e., the percentage of payments made to each supplier). These past transactions were reviewed and audited to determine the extent of inaccurate billings and payments and possible issues that arose therefrom. Any specific instances found of a supplier no longer treating the enterprise as a most-favored customer were used to determine the level of accuracy that is necessary to avoid damaging supplier relationships.

The analysis of past transactions also indicated how quickly suppliers must be paid for the enterprise to maintain preferred customer status. This finding was used to define what is meant by "timely" payments.

The results of the transaction analysis are shown in **figure 11**.

The transaction analysis shows that the enterprise appears to have good control over the accuracy of its payments. However, several payments have been late and this has twice caused the loss of preferred customer status. The enterprise will pay higher prices to those suppliers in the coming year to the extent of US $125,000. The analysis further identifies that the root cause of those late payments was twofold: oversight by accounts personnel and incorrect payment flags on supplier accounts.

Now that "accurate" and "timely" have been defined, specific goals can be developed for the enterprise. These goals must be stated in terms that communicate enterprise, IT-related and enabler goals.

DIRECT

Enterprise goal: Ensure suppliers are paid in an accurate and timely manner. This requires having appropriate systems in place, mechanisms to identify the need to make payments, practices in place to process billings and make payments, personnel trained in all related skills, and work practices and instructions documented.

IT-related goals: Understand and immediately correct the underlying cause of incorrect payment flags on supplier accounts. The corrective action may precipitate further goals. Put work plans into place based on additional knowledge gained during the system repair process.

Enabler goals: *Principles, Policies and Frameworks*—Review accounts policies to ensure appropriate training requirements are stipulated.

Processes—Review accounts payable activities and work instructions to ensure that personnel are appropriately aware of how to organize and process payments. Also, dictate that a review process be created to ensure the timeliness of payments, i.e., comparison of billing and payment dates. Complete a review of the accounts payable

FIGURE 11

Results of the Transaction Analysis

PERIOD ANALYZED: 1 March 2014 — 31 March 2014	
Number of billings received	2,400
Monetary value of all billings	US $3.6 million
Total number of suppliers	435
Number of billings with confirmed errors	3
Number of repeat billings due to late payments	17
Number of times preferred status revoked	2
Number of payments processed	2,350
Monetary value of all payments	US $3.5 million
Supplier density: Number of suppliers receiving 80 percent of all payments	87
Number of payments with confirmed errors	2
Monetary value of loss of preferred status (estimated excess payments to be made in following year)	US $125,000

system to ensure that appropriate reporting mechanisms are in place to alert users and administrative personnel when problems arise.

From *COBIT 5: Enabling Processes,* review the following practices:

- DSS01.01 Perform operational procedures.
- DSS01.03 Monitor IT infrastructure.
- DSS02.04 Investigate, diagnose and allocate incidents.
- DSS02.05 Resolve and recover from incidents.
- DSS03.02 Investigate and diagnose problems.
- DSS03.04 Resolve and close problems.
- DSS03.05 Perform proactive problem management.

Organizational Structures—Review reporting relationships to ensure appropriate personnel oversee the accounts payable group.

Culture, Ethics and Behavior—Request the CEO and board of directors to consider quality as a theme for messaging within the enterprise.

Information—Determine whether the existing accounts payable system has sufficient data to permit the creation of reports that compare the timing of billing and payment dates.

Services, Infrastructure and Applications—Ensure that the underlying cause for the supplier payment flag not being set correctly in the relevant application is fixed.

People, Skills and Competencies—Reexamine past training and schedule new training sessions as appropriate to ensure accounts payable personnel fully understand how to perform their duties.

MONITOR

After the new practices were in place for six months, a follow-up review was performed. To demonstrate the delivery of value, the enterprise's governing bodies needed to document that benefits had been realized and risk and resources had been optimized.

Benefits realization: A special audit was conducted six months after the project was completed. This audit performed many of the same tasks as were done in the initial analysis of transactions. The audit report documented that, on a test basis, supplier transactions were paid in an accurate and timely manner. There were no examples of late or inaccurate payments and no incidents of supplier accounts payment flags being misapplied. This is precisely what the stakeholders required.

Risk optimization: The implementation of the changes proposed did not introduce any new risk elements into the enterprise. With no new risk added, the analysis concluded that risk was still optimized.

Resource optimization: The resources consumed to bring about the changes needed were time and effort from existing employees. Although this project put new demands on their time, the project was completed and is no longer requiring effort from those employees. Resource demands increased during the implementation of the changes, but no outside resources were required and no system or hardware requirements were needed. The analysis concluded that resources were still optimized.

CONCLUSION

Stakeholders are satisfied when the benefits they expect are realized, the risk to which they are exposed is optimized and the resources they make available are optimized. The results of the GEIT solution should be reviewed and the delivery of value to stakeholders documented in these terms.

The final analysis demonstrates that the GEIT solution implemented did, in fact, deliver value to the enterprise's stakeholders.

Case 2: Illustrative Example Using GEIT for a Government Enterprise

SCENARIO

The board of directors of a governmental oil and gas enterprise has noted that many compliance issues have emerged recently. As a result, the board members challenged

After the new practices were in place for six months, a follow-up review was performed. To demonstrate the delivery of value, the enterprise's governing bodies needed to document that benefits had been realized and risk and resources had been optimized.

the IT function to provide assurance that it preserves value for IT investments. The board also asked the audit committee to provide recommendations to overcome the issues.

Given the enterprise's government status, it is required to comply with an increasing number of information-security-related regulations as well as reporting requirements to various governmental authorities on IT investments.

Internal audit decided to benchmark the enterprise's IT investment against other competing organizations within the region and identify compliance requirements.

USING GEIT TO SOLVE THE PROBLEM

The internal audit director and the IT director decided to form a team to prepare a report highlighting IT budgets in terms of capital investment and operating expenditure compared to other government enterprises. They will also identify the information security compliance requirements.

APPROACH

Once the cross-functional team was formed, the current-state position related to investments and utilization goals was determined. Information was gathered from internal and external sources and multiple discussions were held with the senior and middle management of other enterprises to help in understanding the current perspective and position and the plan to achieve the targeted future state.

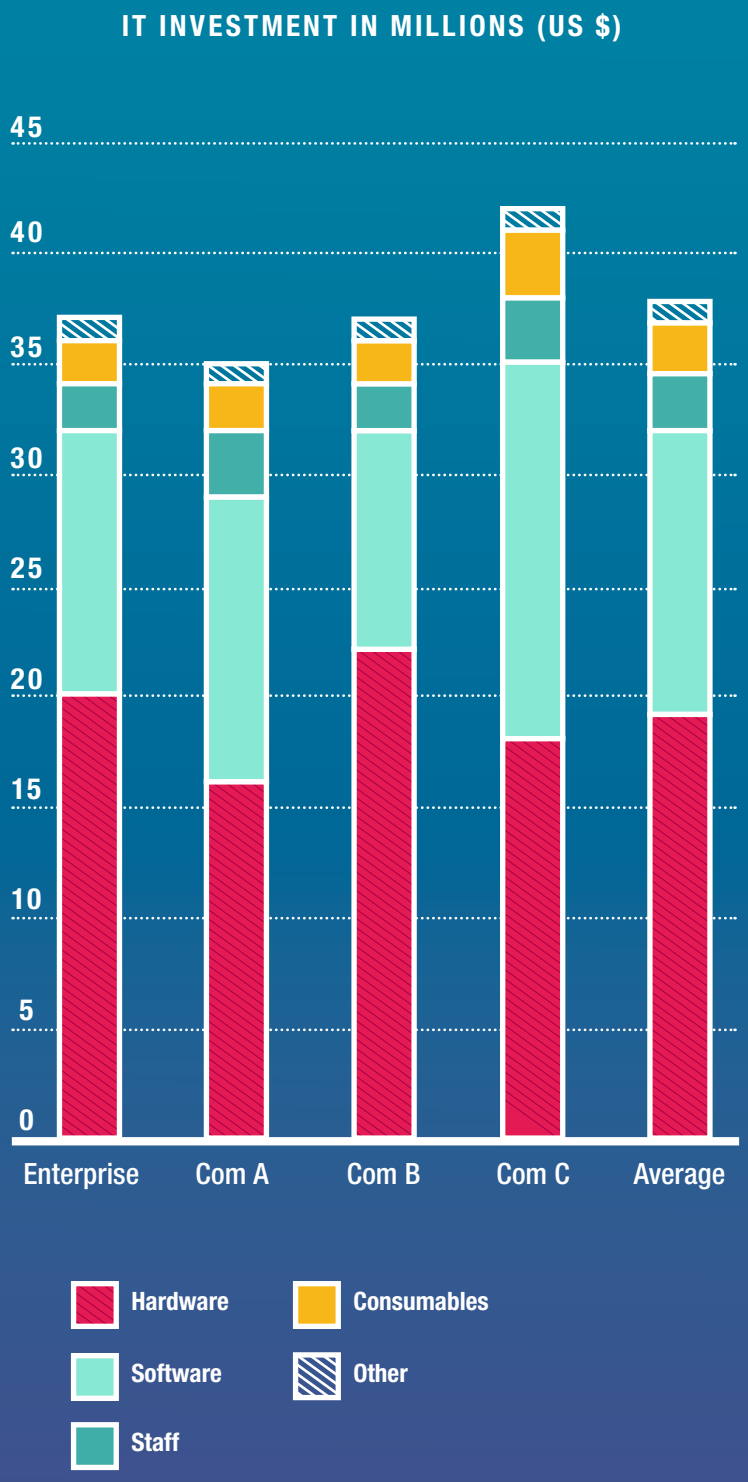
EVALUATE

The stakeholder (board) requirement is for IT investments to be optimally utilized and to meet and exceed the benefit derived from the investments. The board also requires IT to ensure compliance with recently implemented information security regulations.

The information shown in **figure 12** was provided to the board, which instructed IT to confirm its value because the enterprise's IT investment was high compared to some peer enterprises.

FIGURE 12

Comparison to Peer Enterprises



DIRECT

Enterprise goal: Ensure that appropriate value from investments is achieved and compliance with current regulations is attained. This will require alignment of IT goals with business goals, which calls for preparation of an IT balanced scorecard (IT BSC) and a strategic linkage model to ensure IT alignment (**figure 13**).

IT-related goals: Based on the IT BSC, the following IT objectives were identified:

- Optimizing IT cost
- Reporting compliance with external and internal requirements
- Meeting budgets
- Meeting service level agreements (SLAs) and budgets

Enabler goals: *Principles, Policies and Frameworks*—Review policies related to financial management, information security management, resource management and program management.

Processes—Establish the following COBIT 5 processes to ensure all employees are aware of the procedures and the expectation for compliance with these procedures:

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM04 Ensure Resource Optimization
- EDM05 Ensure Stakeholder Transparency
- APO02 Manage Strategy
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO13 Manage Security
- BAI01 Manage Programs and Projects
- BAI09 Manage Assets
- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS05 Manage Security Services
- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

FIGURE 13

IT BSC and Strategic Linkage Model

FINANCIAL	Stakeholders' value of investment—alignment of IT strategy	Compliance with external and internal laws—IT compliance with regulations	Financial transparency (IT investment and cost)
CUSTOMER	Optimization of IT assets and cost	Reporting of regulatory compliance	Customer orientation
INTERNAL	Optimization of IT process cost	IT compliance with policies	Meeting budgets
LEARNING AND GROWTH	Competent and motivated business and IT staff	Employee reward linkage	

Organizational Structures—Ensure that appropriate organizational structures are established to enable proper delegation of authority over internal controls for budget, operations monitoring and compliance with requirements. Establish key goal indicators (KGIs) to ensure that organizational performance is managed.

Culture, Ethics and Behavior—The board of directors should establish, through the CEO, a culture of compliance and ethical service delivery. Employee training and expectations must be established to ensure that efficiency exists in organizational structures so higher value can be achieved from IT investments.

Information—IT uses GRC dashboards to produce appropriate information to take informed decisions.

Services, Infrastructure and Applications—Ensure that appropriate services, infrastructure and applications are available to support decision making, the GRC platform and the budget system.

People, Skills and Competencies—Reexamine past training and schedule new training sessions as appropriate to ensure appropriate skills are available to support organization objectives.

MONITOR

GRC dashboards were established for use in timely monitoring at the management level. Quarterly board review meetings enabled monitoring at the governance level. Comparative KPIs were used to demonstrate value.

Benefits realization: Quarterly review meetings established the fact that IT assets were generating better value. IT investment increased from US $37 million to US $40 million due to inflation and business requirements though the funds were utilized efficiently compared to peers. Before implementing the controls identified in this analysis, utilization stood at 67 percent; after a year operating under the controls, the utilization rate was 78 percent. The compliance rate was increased from 35 percent to 99 percent.

Risk optimization: The implementation of the changes proposed did not introduce any new risk elements into the enterprise. The risk of noncompliance was reduced significantly and the risk of not generating value from IT investments decreased from medium to low. This highlights that risk was optimized appropriately.

Resource optimization: The IT investments were more optimized and the cost of compliance was reduced. This establishes that resources were better optimized.

CONCLUSION

Stakeholders are satisfied when the benefits they expect, such as better use of IT investment and fewer events of noncompliance, are realized. They also appreciate that the risk to which they are exposed in terms of noncompliance and IT assets utilization is optimized and resources are optimized.

The final analysis demonstrates that the GEIT solution implemented did, in fact, deliver value to the enterprise's stakeholders.

B

Sample Business Case

Note: This example[8] is provided as a nonprescriptive generic guide to encourage preparation of a business case to justify investment in a GEIT implementation program. Every enterprise will have its own reasons for improving GEIT and its own approach to preparing business cases, which can range from a detailed approach with an emphasis on quantified benefits to a more high-level and qualitative approach. Enterprises should follow the approved internal business case and investment justification approaches, if they exist, and use this example and the guidance in this publication to help focus on the issues that should be addressed. Further guidance on developing business cases can be found in COBIT 5 process APO05 and in *The Business Case Guide: Using Val IT™ 2.0*.

The sample business is a large multinational enterprise with a mixture of traditional well-established business units as well as new Internet-based businesses adopting the very latest technologies. Many of the business units have been acquired and exist in various countries with different local political, cultural and economic environments. The central group's executive management has been influenced by the latest enterprise governance guidance, including COBIT 5, which management has used centrally for some time. Management wants to make sure that the rapid expansion and adoption of advanced IT in many of the enterprise's businesses will deliver the value expected and also manage significant new risk. The management team has, therefore, mandated an enterprisewide adoption of a uniform GEIT approach that also includes involvement by the audit and risk functions and internal annual reporting by business unit management on the adequacy of controls in all entities.

Although the example is derived from actual situations, it is not a reflection of a specific existing enterprise.

Executive Summary

This business case document outlines the scope of the proposed GEIT program for Acme Corporation based on COBIT 5.

A proper business case is needed to ensure that the Acme Corporation board and each business unit buys in to the initiative, identifies the potential benefits and then monitors the business case to ensure that the expected benefits are realized.

The scope in terms of business entities that make up Acme Corporation is all-inclusive. However, due to limited program resources, some form of prioritization process will be applied across all entities for initial coverage by the GEIT program.

There are many stakeholders that have an interest in the outcomes of the GEIT program, ranging from the Acme Corporation board of directors to local management at each entity, as well as external stakeholders such as shareholders and government agencies.

Consideration needs to be given to some significant challenges, as well as risk, in the

[8]Content in this appendix is based on the following publication: ISACA, *COBIT 5 Implementation*, USA, 2012

implementation of the GEIT program on the required global scale. One of the more challenging aspects is the entrepreneurial nature of many of the Internet businesses, as well as the decentralized or federated business model that exists within Acme Corporation.

The GEIT program will be achieved by focusing on the capability of the Acme processes and other enablers in relation to those that are defined in COBIT 5, relevant to each business unit. The relevant and prioritized processes that will receive focus at each entity will be identified through a facilitated workshop approach by the members of the GEIT program, starting with the business goals of each unit as well as the IT-related business risk scenarios that apply to the specific business unit.

The objectives of the GEIT program are to ensure that adequate governance structures are in place and to increase the level of capability and adequacy of the relevant IT processes, with the expectation that as the capability of an IT process increases, the associated risk will proportionally decrease and efficiencies and quality will increase. In this way, real business benefits can be realized by each business unit.

Once the process of assessing the capability level within each business unit has been established, it is anticipated that self-assessments will continue within each business unit as normal business practice.

The GEIT program will be delivered in two distinct phases. The first is a development phase, where the team will develop and test the approach and tool set that will be used across the Acme Corporation. At the end of phase 1, the results will be presented to group management for final approval. Once final approval has been obtained in the form of an approved business case, the GEIT program will be rolled out across the entity in the agreed-on manner.

It must be noted that it is not the responsibility of the GEIT program to implement the remedial actions identified at each business unit. The GEIT program will merely report progress as supplied by each unit, in a consolidated manner.

The final challenge that will need to be met by the GEIT program is reporting the results in a sustainable manner going forward. This aspect will take time and a significant amount of discussion and development will have to be dedicated to it, which should result in an enhancement to the existing corporate reporting mechanisms and scorecards.

An initial budget for the development phase of the GEIT program has been developed. The budget is detailed in a separate schedule within the business case. A detailed budget will also be completed for phase 2 of the project and submitted for approval by group management. These budgets are separate from and not included in the *Getting Started With GEIT* guide.

Background

GEIT is an integral part of overall enterprise governance and is focused on IT performance and the management of risk attributable to the enterprise's dependencies on IT.

IT is integrated into the operations of the Acme Corporation businesses and for many, specifically the Internet businesses, is at the core of their operations. GEIT, therefore, follows the management structure of the group, a decentralized format. Management of each subsidiary/business unit is responsible for ensuring that proper processes are implemented relevant to GEIT.

Annually, the management of each significant subsidiary company is required to submit a formal written report to the appropriate risk committee, which is a subset of the board of directors, on the extent to which it has implemented the GEIT policy during the financial year. Significant exceptions are to be reported at each scheduled meeting of the appropriate risk committee.

The board of directors, assisted by the risk and audit committees, will ensure that the group's GEIT performance is assessed, monitored, reported and disclosed in a GEIT statement as part of the integrated report. The statement will be based on the reports obtained from the risk, compliance and internal audit teams and the management of each significant subsidiary company, to provide both internal and external stakeholders with relevant and reliable information about the quality of the group's GEIT performance.

Internal audit services will provide assurance to management and the audit committee on the adequacy and effectiveness of GEIT.

IT-related business risk will be reported on and discussed as part of the risk management process in the risk registers presented to the relevant risk committee.

Business Challenges

Due to the pervasive nature of IT and the pace of change of technology, a reliable framework is required to adequately control the full IT environment and avoid control gaps that may expose the enterprise to unacceptable risk.

The intention is not to impede the IT operations of the various operating entities. Instead, it is to improve the risk profile of the entities in a manner that makes business sense and also provides increased quality of service and efficiencies, while explicitly achieving compliance with not only the Acme Corporation group GEIT charter, but also any other legislative, regulatory and/or contractual requirements.

Some examples of the pain points faced are:

- Complicated IT assurance efforts due to the entrepreneurial nature of many of the business units
- Complex IT operating models due to the Internet service-based business models in use
- Geographically dispersed entities, made up of diverse cultures and languages
- The decentralized/federated and largely autonomous business control model employed within the group
- Implementing reasonable levels of IT management, given a highly technical and, at times, volatile IT workforce
- IT's balancing of the enterprise's drive for innovation capabilities and business agility with the need to manage risk and have adequate control
- The setting of risk and tolerance levels for each business unit
- Increasing need to focus on meeting regulatory (privacy) and contractual (payment card industry [PCI]) compliance requirements
- Regular audit findings about poor IT controls and reported IT quality of service problems
- Successful and on-time delivery of new and innovative services in a highly competitive market

Gap Analysis and Goal

There is currently no groupwide approach or framework for GEIT or use of IT good practices and standards. At the local business unit level there are variable levels of adoption of good practice with regard to GEIT. As a result, very little attention has traditionally been paid to the level of IT process capability. Based on experience, the levels are generally low.

The objective of the GEIT program is, therefore, to increase the level of capability and adequacy of IT-related processes and controls appropriate to each business unit, in a prioritized manner.

The outcome should be that significant risk is identified and articulated, and management is in a position to address the risk and report on its status. As the capability level of each business unit increases, so too should the IT-related business risk profile of each entity decrease and quality and efficiency increase proportionally.

Ultimately, business value should increase as a result of effective GEIT.

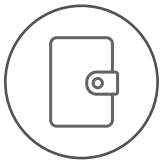
Alternatives Considered

Many IT frameworks exist, each attempting to bring specific aspects of IT under control. The COBIT 5 framework is regarded by many as the world's leading GEIT and control framework. The framework has been implemented by some subsidiaries of the group. It is also specifically mentioned in the King III (chapter 9) report as a potential framework to be implemented for GEIT.

COBIT 5 was chosen by Acme Corporation as the preferred framework for GEIT implementation and should therefore be adopted by all subsidiaries.

COBIT 5 does not necessarily have to be implemented in its entirety; only those areas relevant to the specific subsidiary or business unit need to be implemented, taking into account the following:

1. The development stage of each entity in the business life cycle
2. The business objectives of each entity
3. The importance of IT for the business unit
4. The IT-related business risk faced by each entity



Internal audit services will provide assurance to management and the audit committee on the adequacy and effectiveness of GEIT.

IT-related business risk will be reported on and discussed as part of the risk management process in the risk registers presented to the relevant risk committee.

5. Legal and contractual requirements
6. Any other pertinent reasons

Where other frameworks have already been implemented at a specific subsidiary or business unit, or are still to be implemented in the future, such implementation should be mapped to COBIT 5 for reasons of reporting, audit and clarity of internal control.

Proposed Solution

The GEIT program is being designed in two distinct phases: preplanning and implementation.

PHASE 1. PREPLANNING

Phase 1 of the GEIT program is the development stage. During this stage of the program the following steps should be undertaken:

1. Finalize core team structure between risk management support and group IT.
2. Core team completes the COBIT 5 Foundation Course.
3. Conduct workshop with the core team to define an approach for the group.
4. Create an online community within Acme Corporation to act as a repository for knowledge sharing.
5. Identify all stakeholders and their needs.
6. Clarify and realign, if required, current committee structures, roles and responsibilities, decision rules, and reporting arrangements.
7. Develop and maintain a business case for the GEIT program as a foundation for the successful implementation of the program.
8. Create a communication plan for guiding principles, policies and expected benefits throughout the program.
9. Develop the assessment and reporting tools for use during the life of the program and beyond.
10. Test the approach at one local entity. This activity should be chosen for ease of logistics and to simplify the refinement of the approach and tools.
11. Pilot the refined approach at one of the foreign entities. This is to understand and quantify the difficulties of running the GEIT program assessment phase under more challenging business conditions.
12. Present the final business case and approach, including a rollout plan to Acme Corporation executive management for approval.

PHASE 2. PROGRAM IMPLEMENTATION

The GEIT program is designed to start an ongoing program of continual improvement, based on a facilitated iterative life cycle, by following these steps:

1. Determine the drivers for improving GEIT, from both an Acme Corporation group perspective and the business unit level.
2. Determine the current status of GEIT.
3. Determine the desired state of GEIT (both short- and long-term).
4. Determine what needs to be implemented at the business unit level to enable local business objectives and thereby align with group expectations.
5. Implement the identified and agreed-on improvement projects at the local business unit level.
6. Realize and monitor the benefits.
7. Sustain the new way of working by keeping the momentum going.

Program Scope

The GEIT program will cover the following:

1. All of the group entities; however, the entities will be prioritized for interaction due to limited program resources.
2. The method of prioritization. It will need to be agreed on with Acme Corporation management, but could be done on the following basis:
   a. Size of investment
   b. Earnings/contribution to the group
   c. Risk profile from a group perspective
   d. A combination of these three considerations
3. The list of entities to be covered during the current financial year. This is still to be finalized and agreed on with Acme Corporation management.

Program Methodology and Alignment

The GEIT program will achieve its mandate by using a facilitated, interactive workshop approach with all the entities.

The approach starts with the business objectives and the objective owners, typically the CEO and CFO. This approach should ensure that the program outcomes are closely aligned to the expected business outcomes and priorities.

Once the business objectives have been covered, the focus then shifts to the IT operations, typically under the control of the chief technology officer (CTO) or CIO, where further details of the IT-related business risk and objectives are considered.

The business and IT objectives, as well as the IT-related business risk, are then combined in a tool (based on COBIT 5 guidance) that will provide a set of focus areas within the COBIT 5 processes for consideration by the business unit. In this fashion, the business unit will be able to prioritize its remediation effort to address the areas of IT risk.

Program Deliverables

As mentioned earlier, an overall goal of the GEIT program is to embed the good practices of GEIT into the continuing operations of the various group entities.

Specific outcomes will be produced by the GEIT program to enable Acme Corporation to gauge the delivery of the program's intended outcomes. These will include the following:

1. The GEIT program will facilitate internal knowledge sharing via the intranet platform and leverage existing relationships with vendors to the advantage of the individual business units.
2. Detailed reports on each facilitation interaction with the business units will be created. The reports will include:

   a. The current prioritized business objectives and consequent IT objectives based on COBIT 5

   b. The IT-related risk identified by the business unit in a standardized format and the agreed-on focus areas for attention by the business unit based on COBIT 5 processes and practices and other recommended enablers

   c. The above to be derived from the GEIT program assessment tool
3. Overall progress reports on the intended coverage of the Acme Corporation business units by the GEIT program will be created.
4. Consolidated group reporting will cover:

   a. Progress from business units engaged with their agreed-on implementation projects based on monitoring agreed-on performance metrics

   b. Consolidated IT risk view across the Acme Corporation entities

   c. Specific requirements of the risk committee(s)
5. Financial reporting on the program budget versus actual amount spent will be generated.
6. Benefit monitoring and reporting against business-unit-defined value objectives and metrics will be created.

Program Risk

The following are considered to be potential types of risk to the successful initiation and ongoing success of the Acme Corporation GEIT program. These will be mitigated by focusing on change enablement, and they will be monitored and addressed continually via program reviews and a risk register. These types of risk are:

1. Management commitment and support for the program, at both the group level and the local business unit level
2. Demonstrating actual value delivery and benefits to each local entity through the adoption of the program. The local entities should want to adopt the process for the value it will deliver, rather than doing it because of the policy in place.
3. Local management's active participation in the implementation of the program
4. Identifying key stakeholders at each entity for participation in the program

5. Business insight within the IT management ranks
6. Successful integration with any governance or compliance initiatives that exist within the group
7. The appropriate committee structures to oversee the program. For example, the progress of the GEIT program overall could become an agenda item of the IT executive committee. Local equivalents would also need to be constituted. This could be replicated geographically and at the local holding company level where appropriate.

Stakeholders

The following roles have been identified as stakeholders in the outcome of the GEIT program:

1. Risk committee
2. IT executive committee
3. Governance team
4. Compliance staff
5. Regional management
6. Local entity-level executive management (including IT management)
7. Internal audit services

A final structure with the names of the individuals in each role will be compiled and published after consultation with group management.

The GEIT program needs the identified stakeholders to provide the following:

1. Guidance as to the overall direction of the GEIT program. This includes decisions on significant governance-related topics defined in a group RACI chart according to COBIT 5 guidance, and on setting priorities, agreeing on funding and approving value objectives.
2. Acceptance of the deliverables and monitoring of the expected benefits of the GEIT program

Cost-Benefit

The program should identify the expected benefits and monitor that real business value is being generated from the investment. Local management should motivate and sustain the program. Sound GEIT should result in the following benefits that will be set as specific targets for each business unit, and monitored and then measured during implementation to ensure that the benefits are realized:

1. Maximizing the realization of business opportunities through IT, while mitigating IT-related business risk to acceptable levels, thus ensuring that risk is responsibly weighed against opportunity in all business initiatives
2. Support of the business objectives by key investments and optimum returns on those investments, thus aligning IT initiatives and objectives directly with business strategy
3. Legislative, regulatory and contractual compliance, and internal policy and procedural compliance
4. A consistent approach for measuring and monitoring progress, efficiency and effectiveness
5. Improved quality of service delivery
6. Lowered cost of IT operations and/or increased IT productivity by accomplishing more work consistently in less time and with fewer resources

Central costs will include the time required for group program management, external advisory resources and initial training courses. These central costs have been estimated for phase 1. The cost of individual business unit management and process owners for assessment workshops will be funded locally and an estimate provided. Specific project improvement initiatives for each business unit will be estimated in phase 2 and considered on a case-by-case basis and overall. This will enable the group to maximize efficiency and standardization.

Challenges and Success Factors

Figure 14 summarizes the challenges that could affect the GEIT program during the implementation period of the program and the CSFs that should be addressed to ensure a successful outcome

Central costs will include the time required for group program management, external advisory resources and initial training courses. These central costs have been estimated for phase 1. The cost of individual business unit management and process owners for assessment workshops will be funded locally and an estimate provided. Specific project improvement initiatives for each business unit will be estimated in phase 2 and considered on a case-by-case basis and overall. This will enable the group to maximize efficiency and standardization.

FIGURE 14

Implementation Challenges and CSFs

CHALLENGE	CRITICAL SUCCESS FACTOR — ACTIONS PLANNED
Inability to gain and sustain support for improvement objectives	Mitigate through committee structures within the group (to be agreed on and constituted).
Communication gap between IT and the business	Involve all of the stakeholders.
Cost of improvements outweighing perceived benefits	Focus on benefit identification.
Lack of trust and good relationships between IT and the enterprise	• Foster open and transparent communications about performance, with links to corporate performance management. • Focus on business interfaces and service mentality. • Publish positive outcomes and lessons learned to help establish and maintain credibility. • Ensure the CIO credibility and leadership in building trust and relations. • Formalize governance roles and responsibilities in the business so that accountability for decisions is clear. • Identify and communicate evidence of real issues, risks that need to be avoided and benefits to be gained (in business terms) relating to proposed improvements. • Focus on change and enablement planning.
Lack of understanding of the Acme environment by those responsible for the GEIT program	Apply a consistent assessment methodology.
Various levels of complexity (technical, organizational, operating model)	Treat the entities on a case-by-case basis. Benefit from lessons learned and sharing the knowledge.
Understanding GEIT frameworks, procedures and practices	Train and mentor.
Resistance to change	Ensure that implementation of the life cycle also includes change enablement activities.
Adoption of improvements	Enable local empowerment at the entity level.
Difficult to integrate GEIT with the governance models of outsourcing partners	• Involve suppliers/third parties in GEIT activities. • Incorporate conditions and right to audit in contracts.

CHALLENGE	CRITICAL SUCCESS FACTOR — ACTIONS PLANNED
Failure to realize GEIT implementation commitments	• Manage expectations. • Keep it simple, realistic and practical. • Break down the overall project into small achievable projects, building experience and benefits.
Trying to do too much at once; IT tackling overly complex and/or difficult problems	• Apply program and project management principles. • Use milestones. • Prioritize 80/20 tasks (80 percent of the benefit with 20 percent of the effort) and be careful about sequencing in the correct order; capitalize on quick wins. • Build trust/confidence; have skills and experience to keep it simple and practical. • Reuse what is there as a base.
IT in fire-fighting mode and/or not prioritizing well and unable to focus on GEIT	• Apply good leadership skills. • Gain commitment and drive from top management so people are made available to focus on GEIT. • Address root causes in the operational environment (external intervention, management prioritizing IT). • Apply tighter discipline over/management of business requests. • Obtain external assistance.
Required IT skills and competencies not in place, e.g., understanding of the business, processes, soft skills	Focus on change enablement planning: • Development • Training • Coaching • Mentoring • Feedback into recruitment process • Cross-skilling
Improvements not adopted or applied	Use a case-by-case approach with agreed-on principles for the local entity. It must be practical to implement.
Benefits difficult to show or prove	Identify performance metrics.
Lost interest and momentum	Build group-level commitment, including communication.

SOURCE: ISACA, *COBIT 5 Implementation*, 2012, USA, figure 48

C

Resources for GEIT Implementation

This section contains resources that will help the project team navigate some of the action items described in this guide. These are designed to provide a starting point in the GEIT implementation activities.

Tips for Conducting Interviews

- Designate a specific time period and do not exceed that time without mutual agreement.

  > When a manager is told that a staff member will be needed for 45 minutes, he/she should not discover that the interview lasted 90 minutes.

- Know as much as possible about the business process in advance of the interview. This will reduce the time spent on general explanations of core business functions.

  > Before the interview, obtain and review documentation such as process maps, standard operating procedures, the results of impact assessments and network topologies.

- Prepare questions and provide them to the interviewee in advance so that he or she can bring any supporting documentation, reports or data that may be necessary.

- Conduct interviews with senior leaders to ensure a thorough understanding of the enterprise, including every aspect of each business operation.

  > Senior leaders may include board members, administrators, critical third-party service providers, customers, suppliers and managers.

- Encourage interviewees to be open about challenges they face, risk that concerns them, and any potential missed opportunities or problems associated with their current processes, systems and services/products.

- Avoid setting incorrect expectations regarding confidentiality of interview answers.

  > People may worry about the repercussions of discussing flaws or missed opportunities.

  > Promise confidentiality only if it will actually be maintained.

Acknowledgments

Development Team

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

Peter Tessin
CISA, CRISC, CGEIT, ISACA, USA

Working Group

David Cau
Luxembourg

Okanlawon "Zachy" Olorunojowon
CISA, CGEIT, BC Ministry of Health, Canada

Andre Pitkowski
CGEIT, CRISC, APIT Consultoria De Informatica Ltda, Brazil

Abdul Rafeq
CISA, CGEIT, Wincer Infotech Limited, India

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

Alok Tuteja
Ph.D., CGEIT, CRISC, CISSP, CIA, Mazrui Holdings LLC, UAE

Tichaona Zororo
CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance (Pty) Ltd., South Africa

Subject Matter Experts

Steven Babb
CGEIT, CRISC, Clutch Group, UK

David Cau
Luxembourg

Sushil Chatterji
CGEIT, Edutech Enterprises, Singapore

Matthew Conboy
CISA, CIGNA, USA

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

James Doss
CGEIT, ITIL Expert, PMP, TOGAF 9, EMCCA, SSGB, Itvaluequickstart.com, USA

Jimmy Heschl
CISA, CISM, CGEIT, Red Bull, Austria

Yuichi "Rich" Inaba
CISA, Deloitte Touch Tohmatsu LLC, Japan

John E. Jasinski
CISA, CISM, CGEIT, CRISC, CSX, ITIL Expert, ISO 20000, MOF, SSBB, Scrum Product Owner, Scrum Master, RSA Archer Administration, ServiceNow Certified System Administrator, USA

Larry Marks
CISA, CISM, CGEIT, CRISC, CISSP, PMP, CFE, USA

Okanlawon "Zachy" Olorunojowon
CISA, CGEIT, BC Ministry of Health, Canada

Abdul Rafeq
CISA, CGEIT, Wincer Infotech Limited, India

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

Mark Thomas
CGEIT, CRISC, Escoute, USA

Alok Tuteja
Ph.D., CGEIT, CRISC, CISSP, CIA, Mazrui Holdings LLC, UAE

Board of Directors

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

Theresa Grafenstine
CISA, CGEIT, CRISC, CIA, CGAP, CGMA, CPA, U.S. House of Representatives, USA, Vice-chair

Robert Clyde
CISM, Clyde Consulting LLC, USA, Director

Leonard Ong
CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM, CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA, Merck, Singapore, Director

Andre Pitkowski
CGEIT, CRISC, APIT Consultoria De Informatica Ltda, Brazil, Director

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP, WhiteOps, USA, Director

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

Tichaona Zororo
CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance (Pty) Ltd., South Africa, Director

Zubin Chagpar
CISA, CISM, PMP, Amazon Web Services, UK, Director

Rajaramiyer Venketaramani Raghu
CISA, CRISC, Versatilist Consulting India Pvt. Ltd., India, Director

Jeff Spivey
CRISC, CPP, Security Risk Management, Inc., USA, Director

Robert E Stroud
CGEIT, CRISC, Forrester Research, USA, Past Chair

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past Chair

Greg Grocholski
CISA, SABIC, Saudi Arabia, Past Chair

Matt Loeb
CGEIT, FASAE, CAE, ISACA, USA, Director