ISACA®

Trust in, and value from, information systems

COBIT® 5

Implementation

COBIT® 5

AN ISACA® FRAMEWORK

ISACA®

With 95,000 constituents in 160 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the non-profit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfil their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer

ISACA has designed this publication, *COBIT®5 Implementation* (the 'Work'), primarily as an educational resource for governance of enterprise IT (GEIT), assurance, risk and security 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, readers should apply their own professional judgement to the specific GEIT, assurance, risk and security circumstances presented by the particular systems or information technology environment.

Copyright

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*

Feedback: *www.isaca.org/cobit*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join the COBIT conversation on Twitter: #COBIT
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

COBIT® 5 Implementation
ISBN 978-1-60420-240-3
Printed in the United States of America

Acknowledgements

ISACA wishes to recognise:

COBIT 5 Task Force (2009–2011)
John W. Lainhart, IV, CISA, CISM, CGEIT, IBM Global Business Services, USA, Co-chair
Derek J. Oliver, Ph.D., CISA, CISM, CRISC, CITP, DBA, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd., UK, Co-chair
Pippa G. Andrews, CISA, ACA, CIA, KPMG, Australia
Elisabeth Judit Antonsson, CISM, Nordea Bank, Sweden
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Steven De Haes, Ph.D., University of Antwerp Management School, Belgium
Peter Harrison, CGEIT, FCPA, IBM Australia Ltd., Australia
Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Austria
Robert D. Johnson, CISA, CISM, CGEIT, CRISC, CISSP, Bank of America, USA
Erik H.J.M. Pols, CISA, CISM, Shell International-ITCI, The Netherlands
Vernon Richard Poole, CISM, CGEIT, Sapphire, UK
Abdul Rafeq, CISA, CGEIT, CIA, FCA, A. Rafeq and Associates, India

Development Team
Gert du Preez, CGEIT, PwC, Canada
Gary Hardy, CGEIT, IT Winners, South Africa
Dirk Steuperaert, CISA, CGEIT, CRISC, IT In Balance BVBA, Belgium

Expert Reviewers
Brian Barnier, CGEIT, CRISC, ValueBridge Advisors, USA
Dirk Bruyndonckx, CISA, CISM, CGEIT, CRISC, MCA, KPMG Advisory, Belgium
Christophe Burtin, CISA, ITIL LA 27001, Strategy and Governance, Luxembourg
Ben Farhangui, Atos Worldline, Belgium
James Golden, CISM, CGEIT, CRISC, CISSP, IBM, USA
Jorge Hidalgo, CISA, CISM, CGEIT, ATC, Lic. Sistemas, Argentina
John Manzini, ITIL, Denel Aviation, South Africa
Lucio Augusto Molina Focazzio, CISA, CISM, CRISC, ITIL, Independent Consultant, Colombia
Robert Payne, CGEIT, MBL, MCSSA, PrM, Lode Star Strategy Consulting, South Africa
Martin Rosenberg, Ph.D., Cloud Governance Ltd., UK
Claus Rosenquist, CISA, CISSP, Nets Holding, Denmark
Michael Shortt, CISA, CGEIT, Governance Realm IT, South Africa
Ant Smith, Ph.D., JD Group, South Africa
Greet Volders, CGEIT, Voquals N.V., Belgium
Charl Weitz, CISA, Metropolitan, South Africa
Tichaona Zororo, CISA, CISM, CGEIT, Standard Bank, South Africa

ISACA Board of Directors
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, Inc., USA, Vice President
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vice President
Emil D’Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., (retired), USA, Past International President
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, UK, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Director

Acknowledgements (cont.)

Knowledge Board
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Chairman
Michael A. Berardi Jr., CISA, CGEIT, Bank of America, USA
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapore
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jon Singleton, CISA, FCA, Auditor General of Manitoba (retired), Canada
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France

Framework Committee (2009–2012)
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France, Chairman
Georges Ataya, CISA, CISM, CGEIT, CRISC, CISSP, Solvay Brussels School of Economics and Management, Belgium, Past Vice President
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Sergio Fleginsky, CISA, Akzo Nobel, Uruguay
John W. Lainhart, IV, CISA, CISM, CGEIT, CRISC, IBM Global Business Services, USA
Mario C. Micallef, CGEIT, CPAA, FIA, Malta
Anthony P. Noble, CISA, CCP, Viacom, USA
Derek J. Oliver, Ph.D., CISA, CISM, CRISC, CITP, DBA, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd., UK
Robert G. Parker, CISA, CA, CMC, FCA, Deloitte & Touche LLP (retired), Canada
Rolf M. von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, Forfa, AG, Germany
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia
Robert E. Stroud, CGEIT, CA Inc., USA

ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors
American Institute of Certified Public Accountants
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Institute of Management Accountants Inc.
ISACA chapters
ITGI France
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School

Enterprise GRC Solutions Inc.
Hewlett-Packard
IBM
Symantec Corp.

Table of Contents

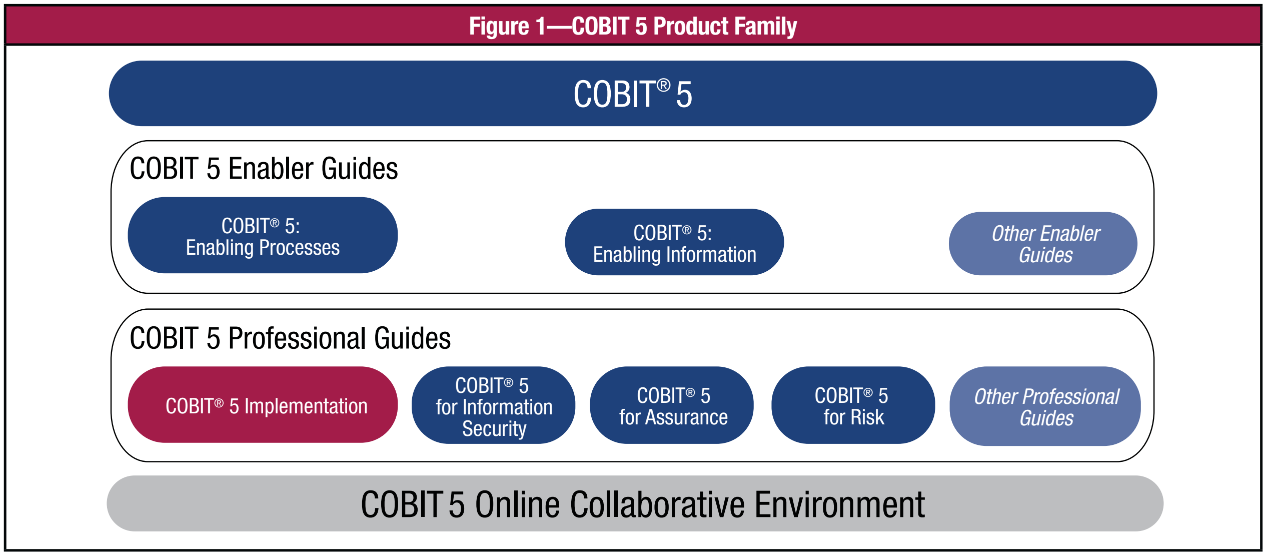
List of Figures

Page intentionally left blank

Chapter 1
Introduction

COBIT 5 Implementation complements COBIT 5 (**figure 1**). The objective of this reference guide is to provide a good practice approach for implementing GEIT based on a continual improvement life cycle that should be tailored to suit the enterprise's specific needs.

Figure 1—COBIT 5 Product Family


COBIT® 5
COBIT 5 Enabler Guides
COBIT® 5: Enabling Processes
COBIT® 5: Enabling Information
Other Enabler Guides
COBIT 5 Professional Guides
COBIT® 5 Implementation
COBIT® 5 for Information Security
COBIT® 5 for Assurance
COBIT® 5 for Risk
Other Professional Guides
COBIT 5 Online Collaborative Environment

The COBIT 5 framework is built on five basic principles, which are covered in detail, and includes extensive guidance on enablers for governance and management of enterprise IT.

The COBIT 5 product family includes the following products:
- COBIT 5 (the framework)
- COBIT 5 enabler guides, in which governance and management enablers are discussed in detail. These include:
  - *COBIT 5: Enabling Processes*
  - COBIT 5: Enabling Information (in development)
  - Other enabler guides (check *www.isaca.org/cobit*)
- COBIT 5 professional guides, which include:
  - *COBIT 5 Implementation*
  - COBIT 5 for Information Security (in development)
  - COBIT 5 for Assurance (in development)
  - COBIT 5 for Risk (in development)
  - Other professional guides (check *www.isaca.org/cobit*)
- A collaborative online environment, which will be available to support the use of COBIT 5

This publication is structured as follows:
- Chapter 2 explains positioning GEIT within an enterprise
- Chapter 3 discusses taking the first steps towards improving GEIT
- Chapter 4 explains implementation challenges and success factors
- Chapter 5 discusses enabling GEIT-related organisational and behavioural change
- Chapter 6 details implementing continual improvement that includes change enablement and programme management
- Chapter 7 discusses using COBIT 5 and its components
- A number of appendices are also included:
  - Appendix A presents COBIT 5 processes and maps pain points to the processes
  - Appendix B provides an example decision matrix
  - Appendix C maps example risk scenarios to COBIT 5 processes
  - Appendix D provides an example business case
  - Appendix E is the COBIT 4.1 maturity attribute table

The improvement of the governance of enterprise IT (GEIT) is widely recognised by top management as an essential part of enterprise governance. At a time when the significance of information and the pervasiveness of information technology (IT) are increasingly part of every aspect of business and public life, the need to drive more value from IT investments and manage an increasing array of IT-related risk has never been greater. Increasing regulation is also driving heightened awareness amongst boards of directors regarding the importance of a well-controlled IT environment and the need to comply with legal, regulatory and contractual obligations.

Effective GEIT will result in improved business performance as well as compliance to external requirements, yet successful implementation remains elusive for many enterprises. Effective GEIT requires a range of enablers with carefully prescribed roles, responsibilities and accountabilities that fit the style and operational norms specific to the enterprise. These include an appropriate culture and behaviour, guiding principles and policies, organisational structures, well-defined and managed governance and management processes, the information required to support decision making, supporting solutions and services, and appropriate governance and management skills.

The improvement of governance of enterprise IT is increasingly recognised by top management as an essential part of enterprise governance.

For many years ISACA has researched this key area of enterprise governance to advance international thinking and provide guidance in evaluating, directing and monitoring an enterprise's use of IT. ISACA has developed the COBIT 5 framework to help enterprises implement sound governance enablers; indeed, implementing good GEIT is almost impossible without engaging an effective governance framework. Best practices and standards are also available to underpin COBIT 5.

Frameworks, best practices and standards are useful only if they are adopted and adapted effectively. There are challenges that must be overcome and issues that must be addressed if GEIT is to be implemented successfully. The board and managers will need to accept more accountability for IT, provide guiding principles and a framework, and instil a different mindset and culture for delivering value from IT.

Objectives and Scope of the Guide

In *COBIT 5 Implementation*, the emphasis is on the enterprisewide view of governance of IT. This guide and COBIT 5 recognise that information and related information technologies are pervasive in enterprises and that it is neither possible nor good practice to separate business and IT-related activities. The governance and management of enterprise IT should therefore be implemented as an integral part of enterprise governance, covering the full end-to-end business and IT functional areas of responsibility.

This guide is also supported by an implementation tool kit containing a variety of resources that will be continually enhanced and available as a download to ISACA members from *www.isaca.org/cobit*. Its contents include:

- Self-assessment, measurement and diagnostic tools
- Presentations
- Related articles and further explanations

One of the common reasons why some GEIT implementations fail is that they are not initiated and then managed properly as programmes to ensure that benefits are realised. GEIT programmes need to be sponsored by executive management, be properly scoped, and define objectives that are attainable so that the enterprise can absorb the pace of change as planned. Programme management is therefore addressed as an integral part of the implementation life cycle.

GEIT implementations need to be managed as programmes sponsored by executive management, be properly scoped, and define objectives that are attainable.

It is also assumed that while a programme and project approach is recommended to effectively drive improvement initiatives, the goal is also to establish a 'normal business practice' and sustainable approach to governing and managing enterprise IT just like any other aspect of enterprise governance. For these reasons, the implementation approach is based on empowering business and IT stakeholders and role players to take ownership of IT-related governance and management decisions and activities by facilitating and enabling change. The implementation programme will be closed when the process for focusing on IT-related priorities and governance improvement is generating a measurable benefit and has become embedded in ongoing business activity.

This guide is not intended to be a prescriptive approach or the complete solution, but rather a guide to avoid pitfalls, leverage the latest good practices and assist in the creation of successful governance and management outcomes over time. Every enterprise will apply its own specific plan or road map, depending, of course, on factors such as its industry and business environment and its culture and objectives. Equally important will be the current starting point. Few enterprises will have no GEIT structures or processes in place, even if they are not recognised as such currently. Therefore, the emphasis needs to be on building on what the enterprise already has in place, especially leveraging existing successful enterprise-level approaches that can be adopted and, if necessary, adapted for IT rather than reinventing something different. Furthermore, any previous improvements using COBIT 4.1 or other standards and best practices need not be reworked, but can, and should be, built on using COBIT 5 and this updated guide as an ongoing part of continual improvement.

It will be beneficial for users of this guide to be familiar with GEIT as a topic and for the implementation team to have the expert knowledge required to be able to successfully implement GEIT using COBIT 5. Undertaking related educational programmes will enable proper understanding of COBIT 5 concepts, how to use the COBIT 5 components and how to apply this implementation method, as well as other related guidance provided by ISACA including process capability assessment and assurance activities based on COBIT 5. ISACA's Certified in the Governance of Enterprise IT (CGEIT) programme also supports the development and recognition of the governance of IT skills and competencies.

COBIT 5 is freely downloadable from *www.isaca.org/cobit*. A link to the ISACA products available to support implementation is available on this page as well.

This guide reflects enhanced understanding and practical experiences of GEIT implementations, lessons learned while applying and using previous versions, and updates that have been made to ISACA's GEIT guidance. Since IT is a fast-changing topic, users of this guide should also maintain an awareness of ISACA's professional publications and other organisations' standards and best practices that may be released from time to time to address new emerging topics.

Page intentionally left blank

Chapter 2
Positioning GEIT

Understanding the Context

GEIT does not occur in a vacuum. Implementation takes place in different conditions and circumstances determined by numerous factors in the internal and external environment such as:

- The community's ethics and culture
- Ruling laws, regulations and policies
- International standards
- Industry practices
- The competitive environment
- The enterprise's:
  - Mission, vision, goals and values
  - Governance policies and practices
  - Culture and management style
  - Models for roles and responsibilities
  - Business plans and strategic intentions
  - Operating model and level of maturity

The implementation of GEIT for each enterprise will, therefore, be different and the context needs to be understood and considered to design the optimal new or improved GEIT environment.

What Is GEIT?

The terms 'governance', 'enterprise governance' and 'GEIT' may have different meanings to different individuals and enterprises depending on (amongst others) the organisational context, e.g., maturity, industry and regulatory environment, or the individual context, e.g., job role, education and experience. To provide a foundation for the rest of this guide, explanations are provided in this section, but it should be recognised that different points of view will exist. The best approach is to build on and enhance the existing approaches to be inclusive of IT rather than developing a new approach just for IT.

'Governance' is derived from the Greek verb *kubernáo* meaning 'to steer'. A governance system enables multiple stakeholders in an enterprise to have an organised say in evaluating conditions and options, setting direction and monitoring performance against enterprise objectives. Setting and maintaining the appropriate governance approach is the responsibility of the board of directors or equivalent body.

COBIT 5 defines governance as:

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

GEIT is not an isolated discipline, but an integral part of enterprise governance. While the need for governance at an enterprise level is driven primarily by delivery of stakeholder value and demand for transparency and effective management of enterprise risk, the significant opportunities, costs and risk associated with IT call for a dedicated, yet integrated, focus on GEIT. GEIT enables the enterprise to take full advantage of IT, maximising benefits, capitalising on opportunities and gaining competitive advantage.

Why Is GEIT so Important?

Globally, enterprises—whether public or private, large or small—increasingly understand that information is a key resource and that IT is a strategic asset and important contributor to success.

IT can be a powerful resource to help enterprises achieve their most important objectives. As an example, IT can represent a core driver of cost savings for large transactions such as mergers, acquisitions and divestitures. IT can enable automation of key processes, such as the supply chain, and can be the cornerstone of new business strategies or business models, thereby increasing competitiveness and enabling innovation, such as the digital delivery of products (e.g., music being sold and delivered online). IT can enable greater customer intimacy, e.g., by collating and mining data in diverse systems and providing a 360-degree view of customers. IT is the foundation of the networked economy that cuts through geographic locations and organisational silos to provide new and innovative ways of creating value. Most enterprises recognise information and the use of IT as critical assets that need to be governed properly.

While IT has the potential for business transformation, it often represents a very significant investment at the same time. In many cases, the true IT cost is not transparent and budgets are spread across business units, functions and geographic locations with no overall oversight. The greatest portion of spending is often for 'keeping the lights on' initiatives (post-implementation maintenance and operational costs) as opposed to transformational or innovation initiatives. When funds are spent on strategic initiatives, they often fail to deliver expected outcomes. Many enterprises still fail to demonstrate concrete, measurable business value for their IT-enabled investments and are focusing on GEIT as a mechanism to address this situation.

The latest survey on GEIT found a range of positive IT and business outcomes as a result of GEIT practices.

Furthermore, the networked economy presents a spectrum of IT-related risk, such as the non-availability of customer-facing business systems, disclosure of customer or proprietary data, or missed business opportunities due to an inflexible IT architecture. The need to manage these and other types of IT-related risk is another driver for better GEIT.

The importance of GEIT can also be attributed to the complex regulatory environment faced by enterprises in many industries and territories today, often extending directly to IT. The focus on financial reporting has driven a significant corresponding focus on the importance of IT-related controls. The use of good practices such as COBIT has been mandated in some countries and industries, one example being the Banking Regulation and Supervision Agency (BRSA) of Turkey, which has mandated that all banks operating in Turkey must adopt COBIT's best practices when managing IT-related processes. The report on Corporate Governance in South Africa—King III—includes, for the first time in a national governance code, a principle to implement GEIT and recommends the adoption of frameworks such as COBIT. A governance framework for IT can enable complex compliance requirements to be achieved in a more effective and efficient way.

The latest survey[1] on GEIT conducted by ISACA and PwC examined the major IT-related initiatives planned by respondents in the next 12 months:
- 46 percent of respondents were planning major IT systems implementations or upgrades
- 45 percent were planning data or information initiatives

These are examples of initiatives which often have complex stakeholder environments (multiple stakeholders from different business and IT units) that reinforce the need for the appropriate GEIT enablers.

Furthermore, the GEIT survey found a range of positive IT and business outcomes as a result of GEIT practices:
- 38 percent of respondents mentioned lower IT costs
- 27 percent experienced an improved return on IT investments
- 42 percent of respondents reported improved management of IT-related risk
- 28 percent mentioned improved business competitiveness

The survey also showed that:
- Approximately 47 percent of respondents can still significantly increase their GEIT maturity.
- While only approximately 5 percent of respondents indicated they do not think GEIT is important, 23 percent responded that they are only starting to assess what needs to be done.
- 29 percent have only some *ad hoc* measures in place.

What Should GEIT Deliver?

Fundamentally, GEIT is concerned with IT value delivery to the business and the mitigation of IT-related risk. This is enabled by the availability and management of adequate resources and the measurement of performance to monitor progress towards the desired goals.

[1] ITGI, *Global Status Report on the Governance of Enterprise IT (GEIT)*, USA, 2011

GEIT focuses on the following objectives:

- **Benefit realisation**—Creating new value for the enterprise through IT, maintaining and increasing value derived from existing IT investments, and eliminating IT initiatives and assets that are not creating sufficient value for the enterprise. The basic principles of IT value are delivery of fit-for-purpose services and solutions, on time and within budget, and generating the financial and non-financial benefits that were intended. The value that IT delivers should be aligned directly with the values on which the business is focussed and measured in a way that transparently shows the impacts and contribution of the IT-enabled investments in the value creation process of the enterprise.
- **Risk optimisation**—Addressing the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. IT-related business risk consists of IT-related events that could potentially impact the business. While value delivery focuses on the creation of value, risk management focuses on the preservation of value. The management of IT-related risk should be integrated within the enterprise risk management approach to ensure a focus on IT by the enterprise and be measured in a way that transparently shows the impacts and contribution of IT-related business risk optimisation in preserving value.
- **Resource optimisation**—Ensuring that the appropriate capabilities are in place to execute the strategic plan and sufficient, appropriate and effective resources are provided. Resource optimisation ensures that an integrated, economical IT infrastructure is provided, new technology is introduced as required by the business, and obsolete systems are updated or replaced. It recognises the importance of people, in addition to hardware and software, and, therefore, focuses on providing training, promoting retention and ensuring competence of key IT personnel.

Strategic alignment and performance measurement are also important and apply overall to all activities to ensure that IT-related objectives are aligned with the enterprise goals.

Leveraging COBIT 5 and Integrating Frameworks, Standards and Good Practices

The board should mandate adoption and adaption of a GEIT framework such as COBIT 5 as an integral part of enterprise governance development. The framework sets the overall approach and then the guidance provided by specific standards and good practices can be used when designing specific policies, processes, practices and procedures. By working within a framework and leveraging good practices, appropriate governance processes and other enablers can be developed and optimised so that GEIT operates effectively as part of normal business practice and there is a supporting culture, demonstrated by top management. Alignment with COBIT should also result in faster and more efficient external audits since COBIT is widely accepted as a basis for IT audit procedures.

The board and executives should mandate adoption of a GEIT framework as an integral part of enterprise governance.

The framework and resulting enablers should be aligned and in harmony with (amongst others) the:

- Enterprise policies, strategies, governance and business plans, and audit approaches
- Enterprise risk management (ERM) framework
- Existing enterprise governance organisation, structures and processes

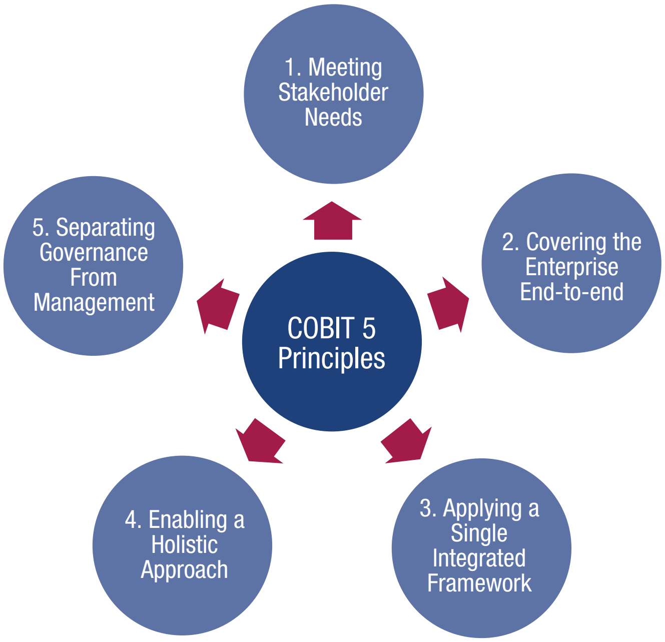
COBIT 5 is intended for enterprises of all types and sizes, including non-profit and public sector, and is designed to deliver business benefits to enterprises, including:

- Increased value creation from use of IT; user satisfaction with IT engagement and services; reduced IT-related risk; and compliance with laws, regulations and contractual requirements
- The development of more business-focussed IT solutions and services
- Increased enterprisewide involvement in IT-related activities

Principles and Enablers

COBIT 5 is based on five principles and seven enablers. The principles that underpin COBIT 5 are identified in **figure 2**.

Figure 2—COBIT Principles


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

The enablers that should be considered to help foster the achievement of the enterprise's framework objectives and deliver value are:

- Principles, policies and frameworks
- Processes
- Organisational structures
- Culture, ethics and behaviour
- Information
- Services, infrastructure and applications
- People, skills and competencies

COBIT 5 includes processes that help guide the creation and maintenance of the governance and management enablers:

- EDM01 *Ensure governance framework setting and maintenance* (culture, ethics and behaviour; principles, policies and frameworks; organisational structures; and processes)
- APO01 *Manage the IT management framework* (culture, ethics and behaviour; principles, policies and frameworks; organisational structures; and processes)
- APO03 *Manage enterprise architecture* (information; services, infrastructure and applications)
- APO07 *Manage human resources* (people, skills and competencies)

The COBIT 5 governance and management processes ensure that enterprises organise their IT-related activities in a repeatable and reliable way. The COBIT 5 process reference model, with five domains and 37 processes that form the structure for the detailed COBIT 5 process guidance, is described in detail in *COBIT® 5: Enabling Processes.*

COBIT 5 is based on an enterprise view and is aligned with enterprise governance best practices, enabling GEIT to be implemented as an integral part of wider enterprise governance. COBIT 5 also provides a basis to effectively integrate other frameworks, standards and practices used such as Information Technology Infrastructure Library (ITIL®), The Open Group Architecture Forum (TOGAF®) and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000. It is also aligned with the GEIT standard, ISO/IEC 38500:2008, which sets out high-level principles for the governance of IT, covering responsibility, strategy, acquisition, performance, compliance and human behaviour that the governing body, such as the board, should evaluate, direct and monitor. COBIT 5 is single overarching framework that serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic common language.

Chapter 3
Taking the First Steps Towards GEIT

Creating the Appropriate Environment

It is important for the appropriate environment to exist when implementing GEIT improvements. This helps ensure that the initiative itself is governed and adequately guided and supported by management. Major IT initiatives often fail due to inadequate management direction, support and oversight. GEIT implementations are no different; they have more chance of success if they are well governed and well managed.

Executive management should specify and design the guiding principles, decision rights and accountability framework for governance of enterprise IT.

Inadequate support and direction from key stakeholders can, for example, result in GEIT initiatives producing new policies and procedures that have no proper ownership. Process improvements are unlikely to become normal business practices without a management structure that assigns roles and responsibilities, commits to their continued operation, and monitors conformance.

An appropriate environment should therefore be created and maintained to ensure that GEIT is implemented as an integral part of an overall governance approach within the enterprise. This should include adequate direction and oversight of the implementation initiative, including guiding principles. The objective is to provide sufficient commitment, direction and control of activities so that there is alignment with enterprise objectives and appropriate implementation support from the board and executive management.

Experience has shown that in some cases, a GEIT initiative identifies significant weaknesses in overall enterprise governance. Success of GEIT is much more difficult within a weak enterprise governance environment, so active support and participation of senior executives are even more critical. The board should be made aware of the need to improve overall governance and the risk of GEIT failing if this is not addressed.

Whether the implementation is a small or major initiative, executive management must be involved in and drive creation of the appropriate governance structures. The initial activities usually include assessment of current practices and the design of improved structures. In some cases it can lead to reorganisation within the business as well as the IT function and its relationship with business units.

Executive management should set and maintain the governance framework—this means specifying the structures, processes and practices for GEIT in line with agreed governance design principles, decision-making models, authority levels and the information required for informed decision making.[2]

Executive management should also allocate clear roles and responsibilities for directing the GEIT improvement programme.

One of the best ways to formalise GEIT, improve executive and board oversight, and set direction of enterprise IT activities is to establish an IT executive strategy committee.

One of the best ways to formalise GEIT and provide a mechanism for executive and board oversight and direction of IT-related activities is to establish an IT executive strategy committee.[3] This committee acts on behalf of the board (to which it is accountable) and is responsible for how IT is used within the enterprise and for making key IT-related decisions affecting the enterprise. It should have a clearly defined mandate, and is best chaired by a business executive (ideally a board member) and staffed by senior business executives representing the major business units, as well as the chief information officer (CIO) and, if required, other senior IT managers. Internal audit and risk functions should provide an advisory role.

Executives need to make decisions based on diverse opinions from business and IT managers, auditors and others. The COBIT 5 framework facilitates this by providing a common language for executives to communicate goals, objectives and expected results.

Figures 3 and **4** illustrate example generic roles for key stakeholders and responsibilities of implementation role players when creating the appropriate environment to sustain governance and ensure successful outcomes. Similar tables are provided for each phase of the implementation life cycle introduced in the next section.

[2] Appendix B contains an example decision matrix.
[3] Often called an IT steering committee, IT council, IT executive committee or IT governance committee.

Figure 3—Roles in Creating the Appropriate Environment

When you are...	Your role in creating the appropriate environment is to...
Board and executives	Set direction for the programme, ensure alignment with enterprisewide governance and risk management, approve key programme roles and define responsibilities, and give visible support and commitment. Sponsor, communicate and promote the agreed-on initiative.
Business management	Provide appropriate stakeholders and champions to drive commitment and to support the programme. Nominate key programme roles and define and assign responsibilities.
IT management	Ensure that the business and executives understand and appreciate the high-level IT-related issues and objectives. Nominate key programme roles and define and assign responsibilities. Nominate a person to drive the programme in agreement with the business.
Internal audit	Agree on the role and reporting arrangements for audit participation. Ensure that an adequate level of audit participation is provided through the duration of the programme.
Risk, compliance and legal	Ensure an adequate level of participation through the duration of the programme.

Figure 4—Creating the Appropriate Environment RACI Chart

	Responsibilities of Implementation Role Players								
Key Activities	Board	IT Executive Committee	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Programme Steering
Set direction for the programme.	A	R	R	C	C	I	C	C	C
Provide programme management resources.	C	A	R	R	C	C	R	R	I
Establish and maintain direction and oversight structures and processes.	C	A	C	I	I	I	I	I	R
Establish and maintain programme.	I	A	R	C	C	I	I	I	R
Align approaches with enterprise approaches.	I	A	R	C	C	I	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Applying a Continual Improvement Life Cycle Approach

Applying a continual improvement life cycle approach provides a method for enterprises to address the complexity and challenges typically encountered during GEIT implementation. There are three interrelated components to the life cycle, as illustrated in **figure 5**: the core GEIT continual improvement life cycle, the enablement of change (addressing the behavioural and cultural aspects of the implementation or improvement), and the management of the programme. In **figure 5**, the initiatives are depicted as continual life cycles to emphasise the fact that these are not one-off activities, but part of an ongoing process of implementation and improvement that in time become 'business as usual', at which time the programme can be retired.

The seven phases of the implementation life cycle are illustrated in **figure 6**. The implementation and improvement programme is typically a continual and iterative one. During the last phase, new objectives and requirements will be identified and a new cycle will be initiated.

High-level health checks, assessments and audits often trigger consideration of a GEIT initiative and these results can be used as input to phase 1.

Figure 5—Components of the Life Cycle

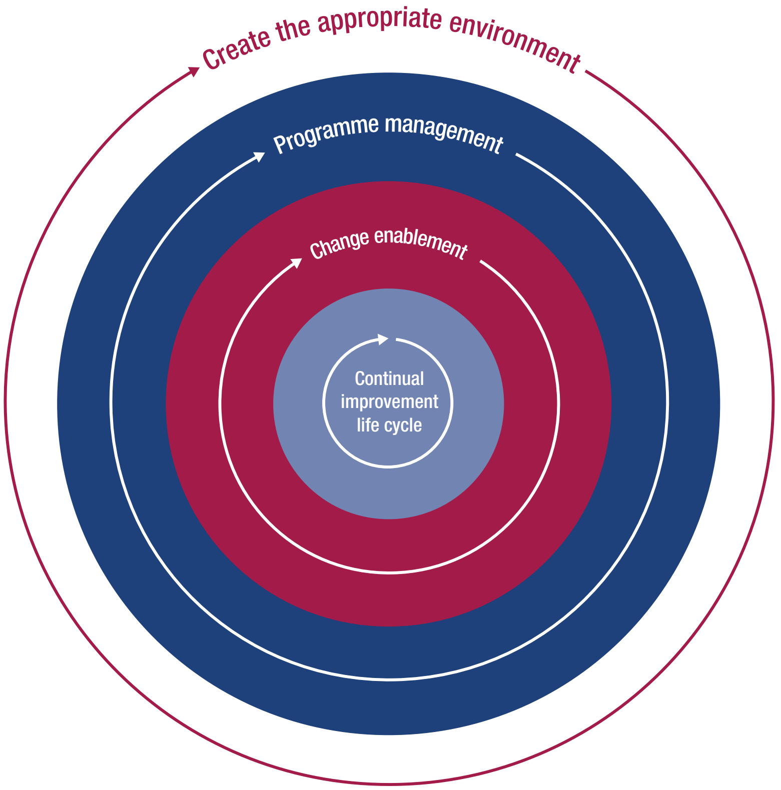
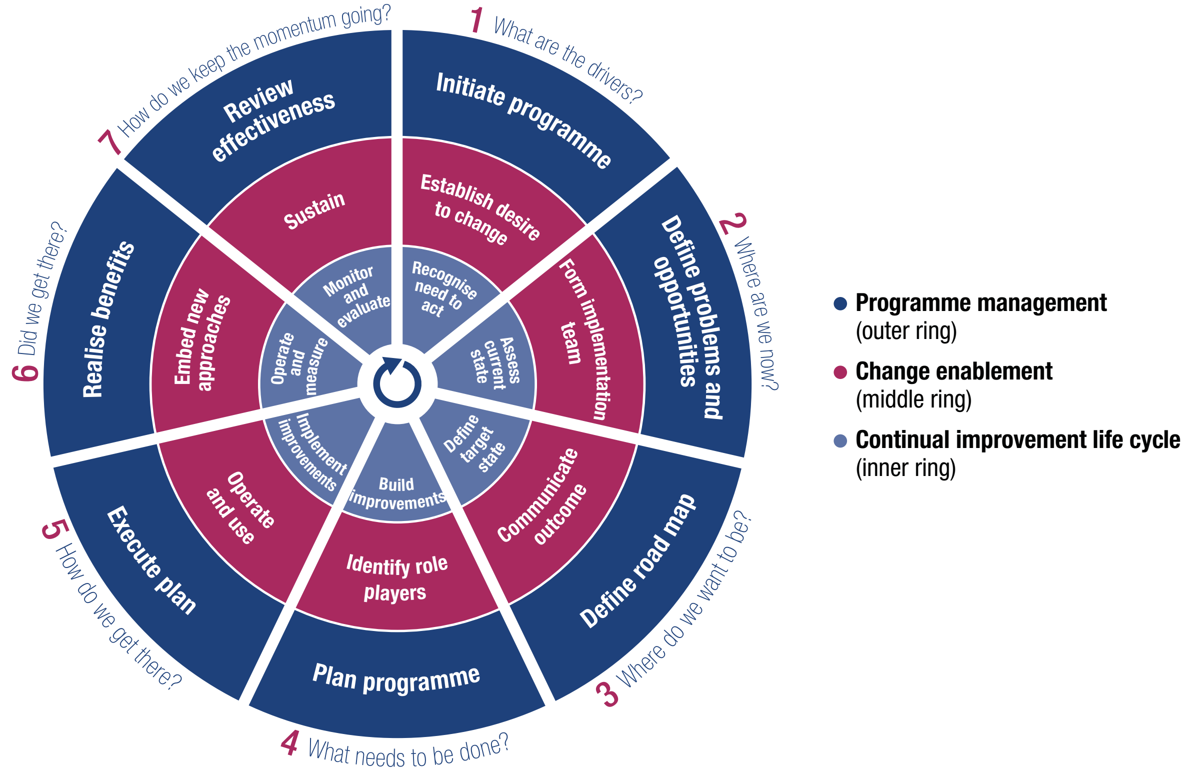

Create the appropriate environment
Programme management
Change enablement
Continual improvement life cycle

Figure 6—Seven Phases of the Implementation Life Cycle



Phase 1—What Are the Drivers?

Phase 1 identifies current change drivers and creates at executive management levels a desire to change that is then expressed in an outline of a business case. A change driver is an internal or external event, condition or key issue that serves as a stimulus for change. Events, trends (industry, market or technical), performance shortfalls, software implementations and even the goals of the enterprise can act as change drivers. Risk associated with implementation of the programme itself will be described in the business case and managed throughout the life cycle. Preparing, maintaining and monitoring a business case are a fundamental and important disciplines for justifying, supporting and then ensuring successful outcomes of any initiative, including the improvement of GEIT. They ensure a continuous focus on the benefits of the programme and their realisation. Appendix D contains an example GEIT business case.

Phase 2—Where Are We Now?

Phase 2 aligns IT-related objectives with enterprise strategies and risk, and prioritises the most important enterprise goals, IT-related goals and processes. COBIT 5 provides a generic mapping of enterprise goals to IT-related goals to IT processes to help with the selection. Given the selected enterprise and IT-related goals, critical processes are identified that need to be of sufficient capability to ensure successful outcomes. Management needs to know its current capability and where deficiencies may exist. This is achieved by a process capability assessment of the as-is status of the selected processes.

Phase 3—Where Do We Want To Be?

Phase 3 sets a target for improvement followed by a gap analysis to identify potential solutions. Some solutions will be quick wins and others more challenging, long-term tasks. Priority should be given to projects that are easier to achieve and likely to give the greatest benefit. Longer-term tasks should be broken down into manageable pieces.

Phase 4—What Needs To Be Done?

Phase 4 plans feasible and practical solutions by defining projects supported by justifiable business cases and developing a change plan for implementation. A well-developed business case will help ensure that the project's benefits are identified and continually monitored.

Phase 5—How Do We Get There?

Phase 5 provides for the implementation of the proposed solutions into day-to-day practices and the establishment of measures and monitoring systems to ensure that business alignment is achieved and performance can be measured. Success requires engagement, awareness and communication, understanding and commitment of top management, and ownership by the affected business and IT process owners.

Phase 6—Did We Get There?

Phase 6 focuses on sustainable transition of the improved governance and management practices into normal business operations and monitoring achievement of the improvements using the performance metrics and expected benefits.

Phase 7—How Do We Keep the Momentum Going?

Phase 7 reviews the overall success of the initiative, identifies further governance or management requirements and reinforces the need for continual improvement. It also prioritises further opportunities to improve GEIT.

Programme and project management is based on good practices and provides for checkpoints at each of the seven phases to ensure that the programme's performance is on track, the business case and risk are updated, and planning for the next phase is adjusted as appropriate. It is assumed that the enterprise's standard approach would be followed. Further guidance on programme and project management can also be found in COBIT 5 process BAI01. Although reporting is not mentioned explicitly in any of the phases, it is a continual thread through all of the phases and iterations.

The time spent per phase will differ greatly depending on (amongst other factors) the specific enterprise environment, its maturity, and the scope of the implementation or improvement initiative. However, the overall time spent on each iteration of the full life cycle ideally should not exceed six months, with improvements applied progressively; otherwise, there is a risk of losing momentum, focus and buy-in from stakeholders. The goal is to get into a rhythm of regular improvements. Larger-scale initiatives should be structured as multiple iterations of the life cycle.

Over time, the life cycle will be followed iteratively while building a sustainable approach. This becomes a normal business practice when the phases in the life cycle are everyday activities and continual improvement occurs naturally.

Getting Started—Identify the Need to Act: Recognising Pain Points and Trigger Events

Many factors may indicate a need for new or revised GEIT practices. It is, however, important to note that these symptoms may not only point to underlying issues that need to be addressed, but could also be indicative of other issues (or a combination of factors). For example, if business has the perception that IT costs are unacceptably high, this may be due to governance and/or management issues (such as the inappropriate criteria being used in the IT investment management process), but it could also be due to a legacy underinvestment in IT that now manifests in significant investments being required.

By using pain points or trigger events as the launching point for GEIT initiatives, the business case for improvement will be related to issues being experienced, which will improve buy-in. A sense of urgency can be created within the enterprise that is necessary to kick off the implementation. In addition, quick wins can be identified and value-add can be demonstrated in areas that are the most visible or recognisable in the enterprise. This provides a platform for introducing further changes and can assist in gaining widespread senior management commitment and support for more pervasive changes.

By using pain points or trigger events as the launching point for governance of enterprise IT initiatives, the business case for GEIT improvement can be related to issues being experienced, which will improve buy-in to the business case.

Typical Pain Points

New or revised GEIT practices can typically solve or be part of a solution to the following symptoms:

- **Business frustration with failed initiatives, rising IT costs and a perception of low business value**—While many enterprises continue to increase their investment in information technology, the value of these investments and overall performance of IT are often questioned or not fully realised. This can be indicative of a GEIT issue where the communication between IT and the business needs to be improved and a common view on the role and value of IT needs to be established. It can also be a consequence of suboptimal portfolio and project formulation, proposal and approval mechanisms.
- **Significant incidents related to IT-related business risk, such as data loss or project failure**—These significant incidents are often the tip of the iceberg and the impacts can be exacerbated if they receive public and/or media attention. Further investigation often leads to the identification of deeper and structural misalignments or even a complete lack of an IT risk-aware culture within the enterprise. Stronger GEIT practices are then required to get a complete view and a solid understanding of IT-related risk and how it should be managed.
- **Outsourcing service delivery problems such as agreed-on service levels not being consistently met**—Issues with service delivery by external service providers may be due to governance issues such as a lack of defined or inadequate tailoring of third-party service management processes (including control and monitoring) with associated responsibilities and accountabilities to fulfil business IT service requirements.
- **Failure to meet regulatory or contractual requirements**—In many enterprises, ineffective or inefficient governance mechanisms prevent complete integration of relevant laws, regulations and contractual terms into organisational systems or lack an approach for managing them. Regulations and compliance requirements are generally increasing globally, often with an impact on IT-enabled activities.
- **IT's limitations of the enterprise's innovation capabilities and business agility**—A common complaint is that IT's role is that of a support function, whereas there is a requirement for innovation capabilities to provide a competitive edge. These are symptoms that may point to a lack of true bidirectional alignment between business and IT, which could be due to communication issues or suboptimal business involvement in IT decision making. It could also be due to business involving IT at too late a stage during strategic planning and business-driven initiatives. This issue typically can be highlighted when economic conditions require rapid enterprise responses such as the introduction of new products or services.
- **Regular audit findings about poor IT performance or reported IT quality of service problems**—This may be indicative of service levels not being in place or not functioning well, or inadequate business involvement in IT decision making.
- **Hidden and rogue IT spending**—A sufficiently transparent and comprehensive view of IT expenditures and investments is often lacking. IT spending can often be 'hidden' in business unit budgets or not classified as IT spending in the accounts, creating an overall biased view of IT costs.
- **Duplication or overlap between initiatives or wasting resources**—This is often due to a lack of a portfolio/holistic view of all IT initiatives and indicates that process and decision structure capabilities around portfolio and performance management are not in place.

- **Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction**—These are significant IT human resource management issues that require effective oversight and good governance to ensure that people management and skills development are addressed effectively. It could also be indicative of (amongst other factors) underlying weaknesses in IT demand management and internal service delivery practices.
- **IT-enabled changes frequently failing to meet business needs and delivered late or over budget**—These pain points could be related to problems with business-IT alignment, definition of business requirements, lack of a benefit realisation process, or suboptimal implementation and project/programme management processes.
- **Multiple and complex IT assurance efforts**—This could be indicative of poor co-ordination between the business and IT regarding the need for and execution of IT-related assurance reviews. An underlying cause could be a low level of business trust in IT, causing the business to initiate its own reviews, or a lack of adequate business accountability for IT assurance reviews, resulting in the business being unaware when they take place.
- **Board members, executives or senior managers who are reluctant to engage with IT, or a lack of committed and satisfied business sponsors for IT**—These pain points often relate to a lack of business understanding and insight into IT, a lack of IT visibility at the appropriate levels, a lack of management structures, or issues with board mandates, often caused by poor communication between the business and IT and the misunderstanding of the business and IT by the business sponsors for IT.
- **Complex IT operating models**—The complexity inherent in, for example, decentralised or federated IT organisations that often have different structures, practices and policies requires a strong focus on GEIT to ensure optimal IT decision making and effective and efficient operations. This pain point often becomes more significant with globalisation because each territory or region may have specific and potentially unique internal and external environmental factors to be addressed.

Trigger Events in the Internal and External Environments

In addition to the symptoms described previously, other events in the enterprise's internal and external environments, such as the following, can signal or trigger a focus on GEIT and drive it high on the enterprise agenda:

- **Merger, acquisition or divestiture**—The strategic and operational consequences relating to IT may be significant following a merger, acquisition or divestiture. During due diligence reviews there will be a need to gain an understanding of IT issues in the environment(s). Also, amongst all of the other integration or restructuring requirements, there will be a need to design the appropriate GEIT mechanisms for the new environment.
- **A shift in the market, economy or competitive position**—For example, an economic downturn could lead enterprises to revise GEIT mechanisms to enable large-scale cost optimisation or performance improvement.
- **Change in business operating model or sourcing arrangements**—For example, a move from a decentralised or federated model towards a more centralised operating model will require changes to GEIT practices to enable more central IT decision making. Another example could be the implementation of shared service centres for areas such as finance, human resources (HR) or procurement. This may have IT impacts such as the consolidation of fragmented IT application or infrastructure domains with associated changes to the IT decision-making structures or processes that govern them. The outsourcing of some IT functions and business processes may similarly lead to a focus on GEIT.
- **New regulatory or compliance requirements**—As an example, expanded corporate governance reporting requirements and financial regulations trigger a need for better GEIT as well as the focus on information privacy caused by the pervasiveness of IT.
- **Significant technology change or paradigm shift**—An example is the migration of some enterprises to a service-oriented architecture (SOA) and cloud computing. This fundamentally changes the way that infrastructure and application functionality is developed and delivered, which also may require changes to the way the associated processes and other enablers are governed and managed.
- **An enterprisewide governance focus or project**—Such projects will likely trigger initiatives in the GEIT area.
- **A new CIO, chief financial officer (CFO), chief executive officer (CEO) or board member**—The appointment of new C-level representatives can often trigger an assessment of current GEIT mechanisms and initiatives to address any weak areas found.
- **External audit or consultant assessments**—An assessment by an independent third party against appropriate practices can typically be the starting point of a GEIT improvement initiative.
- **A new business strategy or priority**—Pursuing a new business strategy will have GEIT implications. For example, a business strategy of being close to customers—i.e., knowing who they are, their requirements, and responding to these requirements in the best possible manner—may require more freedom of IT decision making for a business unit/country as opposed to central decision making at the corporate or holding level.
- **Desire to significantly improve the value to be gained from IT**—A need to improve competitive advantage, be innovative, optimise assets, or create new business opportunities can call attention to GEIT.

The need to act should be recognised and widely solicited and communicated. This communication can be either in the form of a 'wake-up call' (where pain points are being experienced) or an expression of the improvement opportunity to be pursued and benefits that will be realised. Current GEIT pain points or trigger events provide a starting point—the identification of these can typically be done through high-level health checks, diagnostics or capability assessments. These techniques have the added benefit of creating consensus on the issues to be addressed. It can be beneficial to ask a third party to perform a review to obtain an independent and objective high-level view on the current situation, which may increase buy-in to take action.

There is a need to strive for commitment and buy-in of the board and executive management from the beginning. To do this, the GEIT programme and its objectives and benefits need to be clearly expressed in business terms. The correct level of urgency needs to be instilled, and the board and executive management should be aware of the value that well-governed and -managed IT can bring to the enterprise as well as the risk of not taking action. This will also ensure that alignment amongst the GEIT programme and the enterprise objectives and strategy, enterprise objectives for IT, enterprise governance, and ERM initiatives (if existing) is considered from the start. The identification and realisation of some quick wins (visible issues that can be addressed relatively quickly and help establish the credibility of the overall initiative by demonstrating benefits) can be a useful mechanism for obtaining board commitment.

Once the direction has been set at the top, an overall view of change enablement at all levels should be taken. The wider scale and scope of change need to be understood first in hard business terms, but also from a human and behavioural perspective. All of the stakeholders involved in or affected by the change need to be identified and their position relative to the change established. The 2011 GEIT survey[4] showed that change enablement can be one of the biggest challenges to implementing GEIT: 38 percent of respondents mentioned change management as a challenge and 41 percent reported communication issues. A key motivator for change is the identification of incentives for business and IT managers to promote GEIT implementation.

Stakeholder Involvement

There are many stakeholders who need to collaborate to achieve the overall objective of improved IT performance. COBIT 5 is based on stakeholder needs and the approach provided in this guide will help to develop an agreed-on and common understanding of what needs to be achieved to satisfy specific stakeholder concerns in a co-ordinated and harmonised way. The most important stakeholders and their concerns are:

- **Board and executive management**—How do we set and define enterprise direction for the use of IT and monitor the establishment of relevant and required GEIT enablers so that business value is delivered and IT-related risk is mitigated?
- **Executive business management, IT management and process owners**—How do we enable the enterprise to define/align IT-related goals to ensure that business value is delivered from the use of IT and IT-related risk is mitigated?
- **Business management, IT management and process owners**—How do we plan, build, deliver and monitor information and IT solutions and service capabilities as required by the business and directed by the board?
- **Risk, compliance and legal experts**—How do we ensure that we are in compliance with policies, regulations, laws and contracts, and that risk is identified, assessed and mitigated?
- **Internal audit**—How do we provide independent assurance on value delivery and risk mitigation?

Key success factors for implementation are:

- Top management provides the direction and mandate.
- All parties understand the enterprise and IT-related objectives.
- Effective communication and enablement of the necessary organisational and process changes exist.
- Frameworks and good practices are tailored to fit the purpose and design of the enterprise.
- The initial focus is on quick wins and the prioritisation of the most beneficial improvements that are easiest to implement to demonstrate benefit and build confidence for further improvement.

Recognising Stakeholders' Roles and Requirements

Internal Stakeholders

In **figure 6**, an overview of internal stakeholders, their most important high-level responsibilities and accountabilities in the improvement process, and their interest in the outcomes of the implementation programme is provided. These represent generic examples. As such, some adaptation, extension and customisation will be required.

[4] *Op cit* ITGI GEIT Status Report

Figure 7—Overview of Internal GEIT Stakeholders

Internal Stakeholders	Important High-level Accountabilities and Responsibilities	Interest in the Implementation Programme Outcomes
Board and executive management	Set the overall direction, context and objectives for the improvement programme and ensure alignment with the enterprise business strategy, governance and risk management. Provide visible support and commitment for the initiative, including the roles of sponsoring and promoting the initiative. Approve the outcomes of the programme, and ensure that envisioned benefits are attained and corrective measures are taken as appropriate. Ensure that the required resources (financial, human and other) are available to the initiative. Set the direction at the top and lead by example.	The board and executive management are interested in obtaining the maximum business benefits from the implementation programme. They want to ensure that all relevant required issues and areas are addressed, required activities are undertaken, and expected outcomes are successfully delivered.
Business management and business process owners	Provide applicable business resources to the core implementation team. Work with IT to ensure that the outcomes of the improvement programme are aligned to and appropriate for the business environment of the enterprise, and that value is delivered and risk is managed. Visibly support the improvement programme and work with IT to address any issues that are experienced. Ensure that the business is adequately involved during implementation and in the transition to use.	These stakeholders would like the programme to result in better alignment of IT with the overall business environment and their specific areas.
CIO	Provide leadership to the programme and applicable IT resources to the core implementation team. Work with business management and executives to set the appropriate objectives, direction and approach for the programme.	The CIO wants to ensure that all GEIT implementation objectives are obtained. For the CIO, the programme should result in mechanisms that will continually improve the relationship with, and alignment to, the business (including having a shared view on IT performance), lead to better management of IT supply and demand, and improve the management of IT-related business risk.
IT management and IT process owners, e.g., head of operations, chief architect, IT security manager, business continuity management specialist	Provide leadership for applicable work streams of the programme and resources to the implementation team. Give key input into the assessment of current performance and setting of improvement targets for process areas with the respective domains. Provide input on relevant good practices that should be incorporated and provide expert advice. Ensure that the business case and programme plan are realistic and achievable.	These stakeholders are interested in ensuring that the improvement initiative results in better governance of IT overall and in their individual areas, and the business inputs required to do so are obtained in the best possible way.
Compliance, risk management and legal experts	Participate as required throughout the programme and provide compliance, risk management and legal inputs on relevant issues. Ensure alignment with the overall ERM approach (if existing) and confirm that relevant compliance and risk management objectives are met, issues are considered, and benefits are attained. Provide guidance as required during implementation.	These stakeholders want to ensure that the initiative puts in place or improves the mechanisms for ensuring legal and contract compliance as well as effective IT-related business risk management, and these are aligned to any enterprisewide approaches that may exist.
Internal audit	Participate as required throughout the programme and provide audit inputs on relevant issues. Provide advice on current issues being experienced and input on control practices and approaches. Review the feasibility of business cases and implementation plans. Provide guidance as required during implementation. A potential role could also be to verify assessment results independently.	These stakeholders are interested in the outcomes of the implementation programme with regard to control practices and approaches, and how the mechanisms that are put in place or improved will enable current audit findings to be addressed.
Implementation team (combined business and IT team, consisting of individuals from previous stakeholder categories)	Direct, design, control, drive and execute the end-to-end programme from the identification of objectives and requirements to the eventual evaluation of the programme against business case objectives and the identification of new triggers and objectives for further implementation or improvement cycles. Ensure skills transfer during the transition from an implementation environment to the operation, use and maintenance environments.	The team wants to ensure that all envisioned outcomes of the GEIT initiative are obtained and maximised.
Employees	Support GEIT.	These stakeholders are interested in the impact(s) the initiative will have on their day-to-day lives—their jobs, roles and responsibilities, and activities.

External Stakeholders

In addition to the internal stakeholders listed in **figure 7**, there are also several external stakeholders. While these stakeholders do not have any direct accountabilities or responsibilities in the improvement programme, they may have requirements that need to be satisfied. **Figure 8** presents generic examples.

Figure 8—Example External GEIT Stakeholders

External Stakeholders	Interest in the Implementation Programme Outcomes
IT service providers	The enterprise management should ensure that there is alignment and interface between the enterprise's overall GEIT and the governance and management of the services they provide.
Regulators	Regulators are interested in whether the implementation programme outcomes satisfy and/or provide structures and mechanisms to satisfy all applicable regulatory and compliance requirements.
Shareholders (where relevant)	Shareholders may partially base investment decisions on the state of an enterprise's governance and its track record in this area.
Customers	Customers could be affected by the degree to which GEIT objectives are met. An example is IT-related business risk management. If an enterprise is exposed in the security domain, e.g., through loss of customer banking data, the customer will be affected. The customer has an indirect interest in the successful outcomes of the implementation programme.
External auditors	External auditors may be able to place more reliance on IT-related controls as a result of an effective implementation programme and will be interested in regulatory compliance aspects and financial reporting.
Business partners, e.g., suppliers	Business partners that use automated electronic transactions with the enterprise could have an interest in the outcomes of the implementation programme with respect to improved information security, integrity and timeliness. They may also be interested in regulatory compliance and international standards certifications that could be outcomes of the programme.

Independent Assurance and the Role of Auditors

IT managers and stakeholders need to be aware of the role of assurance professionals—they can be internal auditors, external auditors, ISO/IEC standards auditors, or any professional commissioned to provide an assessment on IT services and processes. Increasingly, the board and executive management will seek independent advice and opinions regarding critical IT functions and services. There is also a general increase in the need to demonstrate compliance with national and international regulations.

Page intentionally left blank

Chapter 4
Identifying Implementation Challenges and Success Factors

Experiences from GEIT implementations have shown that there can be several practical issues that need to be overcome for the initiative to be successful and for continual improvement to be sustained. This chapter describes several of these challenges as well as the likely root causes and the factors that should be considered to ensure successful outcomes.

Creating the Appropriate Environment

Phase 1—What Are the Drivers?

Figure 9 lists challenges and their root causes and success factors in phase 1.

Figure 9—Phase 1—What Are the Drivers?

Challenges	**Lack of senior management buy-in, commitment and support** **Difficulty in demonstrating value and benefits**
Root causes	• Lack of understanding (and evidence) of the importance, urgency and value of improved governance to the enterprise • Poor understanding of the scope of GEIT and the differences between governance and management of IT • Implementation driven by a short-term reaction to a problem rather than a proactive, broader justification for improvement • Concern about 'another project likely to fail'—lack of trust in IT management • Poor communication of governance issues and benefits—benefits and time frames not clearly articulated • No senior executive willing to sponsor or be accountable • Poor perception of the credibility of IT function—CIO does not command enough respect • Executive management belief that GEIT is the responsibility of IT management only • Not having the appropriate team (role players) responsible for GEIT or lacking adequate skills to undertake the task • Uninformed usage of available frameworks/lack of training and awareness • Incorrect positioning of GEIT in the context of current enterprise governance • Initiative driven by enthusiastic 'converts' who preach textbook approaches
Success factors	• Make GEIT a board, audit committee and risk committee agenda item for discussion. • Create a committee or leverage an existing committee such as the IT executive strategy committee to provide a mandate and accountability for action. • Avoid making GEIT appear to be a solution 'looking for a problem'—there must be a real need and potential benefit. • Identify leader(s) and sponsor(s) with the authority, understanding and credibility to take ownership of implementation success. • Identify and communicate pain points that can motivate a desire to change the *status quo.* • Use language, approaches and communications appropriate to the audience—avoid jargon and terms they cannot recognise. • Jointly (with the business) define and agree on expected value from IT. • Express benefits in (agreed-on) business terms/metrics. • Obtain, if required, support from, and augment skills with, external auditors or consultants and advisors. • Develop guiding principles that set the tone and scene for the transformation effort. • Produce imperatives based on the transformation effort particular to the enterprise, building in the trust and partnership necessary for success. • Produce a business case tailored for a targeted audience that demonstrates the business benefits of the proposed IT investment. • Prioritise and align the business case based on the strategic focus and current enterprise pain points. • Align the business case with overall enterprise governance objectives. • Gain education and training in GEIT issues and frameworks.
Challenges	**Difficulty in getting the required business participation** **Difficulty in identifying stakeholders and role players**
Root causes	• GEIT not a priority for business executives (not a key performance indicator [KPI]) • IT management's preference to work in isolation—proving the concept before involving the 'customer' • Barriers between IT and the business inhibiting participation • No clear roles and responsibilities for business involvement • Key business individuals and influencers not involved or engaged • Business executives' and process owners' limited understanding of the benefits and value of GEIT

Figure 9—Phase 1—What Are the Drivers? *(cont.)*

Challenges	Difficulty in getting the required business participation Difficulty in identifying stakeholders and role players
Success factors	• Encourage top management and the IT executive strategy committee to set mandates and insist on business roles and responsibilities in GEIT. • Put in place a process for engaging stakeholders. • Clearly explain and sell business benefits. • Explain the risk of non-involvement. • Identify critical services or major IT initiatives to use as pilots/models for business involvement in improved GEIT. • Find the believers—business users who recognise the value of better GEIT. • Promote free thinking and empowerment, but only within well-defined polices and a governance structure. • Ensure that those responsible for, and who need to drive change, are the ones to gain sponsor support. • Create forums for business participation—e.g., IT executive strategy committee—and run workshops to openly discuss current problems and opportunities for improvement. • Involve business representatives in high-level current-state assessments.
Challenge	**Lack of business insight amongst IT management**
Root causes	• IT leadership with an operational technical background—not involved enough in enterprise business issues • IT management isolated within the enterprise—not involved at senior levels • Weak business relationship process • Legacy of perceived poor performance that has driven IT and the CIO into a defensive mode of operation • CIO and IT management in a vulnerable position, unwilling to reveal internal weaknesses
Success factors	• Build credibility by building on successes and performance of respected IT staff. • IT management should ideally be a permanent member of the executive committee to ensure that IT management has adequate business insight and is involved early in new initiatives. • Implement an effective business relationship process. • Invite business participation and involvement. Consider placing business people in IT and *vice versa* to gain experience and improve communications. • If necessary, reorganise IT management roles and implement formal links to other business functions, e.g., finance and HR. • Ensure that the CIO has business experience. Consider appointment of a CIO from the business. • Use consultants to create a stronger business-oriented GEIT strategy. • Create governance mechanisms, such as business relationship managers within IT, to enable greater business insight.
Challenges	**Lack of current enterprise policy and direction** **Weak current enterprise governance**
Root causes	• Commitment and leadership issues, possibly due to organisational immaturity • Autocratic current culture, based on individual commands rather than on enterprise policy • Culture's promotion of free thinking and informal approaches rather than a 'control environment' • Weak enterprise risk management
Success factors	• Raise issues and concerns with board-level executives, including non-executives, of the risk of poor governance, based on real issues related to compliance and enterprise performance. • Raise issues with the audit committee or internal audit. • Obtain input and guidance from external auditors. • Consider how the culture might need to be changed to enable improved governance practices. • Raise the issue with the CEO and board. • Ensure that risk management is applied across the enterprise.

Phase 2—Where Are We Now? and Phase 3—Where Do We Want To Be?

Figure 10 lists the challenges and their root causes and success factors for phases 2 and 3.

Figure 10—Phase 2—Where Are We Now? and Phase 3—Where Do We Want To Be?

Challenges	**Inability to gain and sustain support for improvement objectives** **Communication gap between IT and the business**
Root causes	• Compelling reasons to act not clearly articulated or non-existent • Failure of perceived benefits to sufficiently justify required investment (cost) • Concern about loss of productivity or efficiency due to change • Lack of clear accountabilities for sponsoring and committing to improvement objectives • Lack of appropriate structures with business involvement from strategy to tactical and operational levels • Inappropriate way of communicating (not keeping it simple, not using brief and business language, not suited to politics and culture) or not adapting style to different audiences • Business case for improvements not well developed or articulated • Insufficient focus on change enablement and obtaining buy-in at all required levels
Success factors	• Develop agreed-on understanding of the value of improved GEIT. • Have the appropriate structures, e.g., IT steering committee, audit committee, to facilitate communication and agreement of objectives and establish meeting schedules to exchange strategy status, clarify misunderstandings and share information. • Implement an effective business relationship process. • Develop and execute a change enablement strategy and communication plan explaining the need to reach a higher level of maturity. • Use the correct language and common terminology with style adapted to audience subgroups (make it interesting, use visuals). • Develop the initial GEIT business case into a detailed business case for specific improvements, with clear articulation of risk. Focus on added value for the business (expressed in business terms) as well as costs. • Educate and train in COBIT 5 and this implementation method.
Challenge	**Cost of improvements outweighing perceived benefits**
Root causes	• Tendency to focus solely on controls and performance improvements and not on efficiency improvements and innovation • Improvement programme inadequately phased and preventive of clear association between improvement benefits and cost • Prioritisation of complex, expensive solutions rather than lower-cost, easier solutions • Significant IT budget and manpower already committed to maintenance of existing infrastructure and so a limited appetite to direct funds or staff time left to deal with GEIT
Success factors	• Identify areas in infrastructure, processes and HR, e.g., standardisation, higher maturity levels and fewer incidents, where efficiencies and direct cost savings can be made by better governance. • Prioritise based on benefit and ease of implementation, especially quick wins.
Challenge	**Lack of trust and good relationships between IT and the enterprise**
Root causes	• Legacy issues underpinned by poor IT track record on project and service delivery • Lack of IT understanding of business issues and *vice versa* • Scope and expectations not properly articulated and managed • Unclear governance roles, responsibilities and accountabilities in business, causing abdication of key decisions • Lack of supporting information and metrics illustrating the need to improve • Reluctance to be proven wrong, general resistance to change
Success factors	• Foster open and transparent communication 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 that the CIO has credibility and leadership in building trust and relations. • Formalise governance roles and responsibilities in the business so that accountability for decisions is clear. • Identify and communicate evidence of real issues, risk that needs to be avoided and benefits to be gained (in business terms) relating to proposed improvements. • Focus on change enablement planning.

Phase 4—What Needs To Be Done?

Figure 11 lists the challenges and their root causes and success factors for phase 4.

Figure 11—Phase 4—What Needs To Be Done?

Challenge	**Failure to understand the environment**
Root causes	• Not enough consideration of culture changes, stakeholder perceptions and organisational changes required • Not enough consideration of existing governance strengths and practices within IT and the wider enterprise
Success factors	• Perform a stakeholder assessment and focus on developing a change enablement plan. • Build on and use existing strengths and good practices within IT and the wider enterprise. Avoid 'reinventing wheels' just for IT. • Understand the different constituencies, their objectives and mindsets.
Challenge	**Various levels of complexity (technical, organisational, operating model)**
Root causes	• Poor understanding of GEIT practices • Attempting to implement too much at once • Prioritising critical and difficult improvements with little practical experience • Complex and/or multiple operating models
Success factors	• Educate and train in COBIT 5 and this implementation method. • Break down into smaller projects, building a step at a time, and prioritise quick wins. • Collect the needs for improvement from different constituencies, correlate and prioritise them, and map them to the change enablement programme. • Focus on business priorities to phase implementation.
Challenge	**Difficulty in understanding COBIT 5 and associated frameworks, procedures and practices**
Root causes	• Inadequate skills and knowledge • Copying best practices, not adapting them • Focussing only on procedures, not on other enablers such as roles and responsibilities and skills applied
Success factors	• Educate and train in COBIT 5, other related standards and best practices, and this implementation method. • If required, obtain qualified and experienced external guidance and support. • Adapt and tailor best practices to suit the enterprise environment. • Consider and deal with required skills, roles and responsibilities, process ownership, goals and objectives, and other enablers when designing processes.
Challenge	**Resistance to change**
Root causes	Resistance is a natural behavioural response when the *status quo* is threatened, but it may also indicate an underlying concern such as: • Misunderstanding of what is required and why it is useful • Perception that workload and cost will increase • Reluctance to admit shortcomings • Not-invented-here syndrome, underpinned by forcing generic governance frameworks onto the enterprise • Entrenched thinking/threat to role or power base
Success factors	• Focus awareness communications on specific pain points and drivers. • Raise awareness by educating business and IT managers and stakeholders. • Use an experienced change agent with business and IT skills. • Follow up at regular milestones to ensure that implementation benefits are realised by involved parties. • Go for quick wins and low-hanging fruit as eye-openers of the values provided. • Make generic frameworks such as COBIT 5 relevant to the context of the enterprise. • Focus on change enablement planning such as: – Development – Training – Coaching – Mentoring – Skills transfer • Organise road shows, and find champions to promote the benefits.

Figure 11—Phase 4—What Needs To Be Done *(cont.)*	
Challenge	**Failure to adopt improvements**
Root causes	• External experts designing solutions in isolation, or imposing solutions without adequate explanation • Internal GEIT team operating in isolation and acting as an informal proxy for real process owners, causing misunderstandings and resistance to change • Inadequate support and direction from key stakeholders, resulting in GEIT projects producing new policies and procedures that have no valid ownership
Success factors	• Engage process owners and other stakeholders during design. • Use pilots and demos where appropriate to educate and obtain buy-in and support. • Start with quick wins, demonstrate benefits and build from there. • Look for champions who want to improve, rather than forcing people who resist. • Encourage a management structure that assigns roles and responsibilities, commits to their continued operation, and monitors compliance. • Enforce knowledge transfer from the external experts to process owners. • Delegate responsibility and empower the process owners.
Challenge	**Difficulty in integrating internal governance approach with the governance models of outsourcing partners**
Root causes	• Fear of revealing inadequate practices • Failure to define and/or share GEIT requirements with the outsource provider • Unclear division of roles and responsibilities • Differences in approach and expectations
Success factors	• Involve suppliers/third parties in implementation and operational activities where appropriate. • Incorporate conditions and right to audit in contracts. • Look for ways to integrate frameworks and approaches. • Address roles, responsibilities and governance structures with third parties up front, not as an afterthought. • Match evidence (via audit and document review) of service provider processes, people and technology with required GEIT practices and levels.

Phase 5—How Do We Get There?

Figure 12 lists the challenges and their root causes and success factors for phase 5.

Figure 12—Phase 5—How Do We Get There?	
Challenge	**Failure to realise implementation commitments**
Root causes	• Overly optimistic goals, underestimation of effort required • IT in fire-fighting mode and focussed on operational issues • Lack of dedicated resources or capacity • Priorities incorrectly allocated • Scope misaligned with requirements or misinterpreted by implementers • Programme management principles, e.g., business case, not well applied • Insufficient insight into business environment, e.g., operating model
Success factors	• Manage expectations. • Follow guiding principles. • Keep it simple, realistic and practical. • Break down the overall project into small achievable projects, building experience and benefits. • Ensure that the implementation scope underpins the requirements and all stakeholders have the same understanding of what the scope will deliver. • Focus on implementations that enable business value. • Ensure that dedicated resources are allocated. • Apply programme management and governance principles. • Leverage existing mechanisms and ways of working. • Ensure adequate insight into the business environment.

Figure 12—Phase 5—How Do We Get There? *(cont.)*

Challenge	**Trying to do too much at once; tackling overly complex and/or difficult problems**
Root causes	• Lack of understanding of scope and effort (also for human aspects, creating common language) • Not understanding capacity to absorb change (too many other initiatives) • Lack of formal programme planning and management; not building a foundation and maturing the effort from there • Undue pressure to implement • Not capitalising on quick wins • Reinventing the wheel and not using what is there as a base • Lack of insight into organisational landscape • Lack of skills
Success factors	• Apply programme and project management principles. • Use milestones. • Prioritise 80/20 tasks (80 percent of the benefit with 20 percent of the effort) and be careful about sequencing in the correct order. Capitalise on quick wins. • Build trust/confidence. Have the skills and experience to keep it simple and practical. • Reuse what is there as a base.
Challenge	**IT and/or business in fire-fighting mode and/or not prioritising well and unable to focus on governance**
Root causes	• Lack of resources or skills • Lack of internal processes, internal inefficiencies • Lack of strong IT leadership • Too many workarounds
Success factors	• 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 prioritising IT). • Apply tighter discipline over/management of business requests. • Use external resources where appropriate. • Obtain external assistance.
Challenge	**Lack of required skills and competencies, e.g., understanding governance, management, business, processes, soft skills**
Root causes	• Insufficient understanding of COBIT and IT management best practices • Business and management skills often not included in training • IT staff not interested in non-technical areas • Business staff not interested in IT
Success factors	• Focus on change enablement planning: – Development – Training – Coaching – Mentoring – Feedback into recruitment process – Cross-skilling

Phase 6—Did We Get There? and Phase 7—How Do We Keep the Momentum Going?

Figure 13 lists the challenges and the root causes and success factors for phases 6 and 7.

Figure 13—Phase 6—Did We Get There? and Phase 7—How Do We Keep the Momentum Going?

Challenge	**Failure to adopt or apply improvements**
Root causes	• Solutions too complex or impractical • Solutions developed in isolation by consultants or an expert team • Best practices copied, but not tailored to suit the enterprise operation • Solutions not ‘owned’ by process owners/team • Organisation lacking clear roles and responsibilities • Management not mandating and supporting change • Resistance to change • Poor understanding of how to apply the new processes or tools that have been developed • Skills and profile not matched with the requirements of the role
Success factors	• Focus on quick wins and manageable projects. • Make small improvements to test the approach and make sure it works. • Involve the process owners and other stakeholders in development of the improvement. • Make sure roles and responsibilities are clear and accepted, changing roles and job descriptions if required. • Drive the improvement from management down throughout the enterprise. • Apply adequate training where required. • Develop processes before attempting to automate. • Reorganise, if required, to enable better ownership of processes. • Match roles (specifically those that are key for successful adoption) to individual capabilities and characteristics. • Provide effective education and training.
Challenge	**Difficulty in showing or proving benefits**
Root causes	• Goals and metrics not established or working effectively • Benefits tracking not applied after implementation • Loss of focus on benefits and value to be gained • Poor communication of successes
Success factors	• Set clear, measurable and realistic goals (outcome expected from the improvement). • Set practical performance metrics (to monitor whether the improvement is driving achievement of goals). • Produce scorecards showing how performance is being measured. • Communicate in business impact terms the results and benefits that are being gained. • Implement quick wins and deliver solutions in short time scales
Challenge	**Lost interest and momentum**
Root causes	• Continual improvement not part of the culture • Management not driving sustainable results • Resources focussed on fire-fighting and service delivery, not on improvement • Personnel not motivated, cannot see the personal benefit in adopting and driving change
Success factors	• Ensure that management regularly communicates and reinforces the need for robust and reliable services, solutions and good governance. Communicate to all stakeholders the successful improvements already achieved. • Revisit stakeholders and get their support to ‘fuel’ momentum. • If resources are scarce, take opportunities to implement improvements ‘on the job’ as part of a project of daily routine. • Focus on regular and manageable improvement tasks. • Obtain external assistance, but remain engaged. • Align personal reward systems with process and organisation performance improvement targets and metrics.

Page intentionally left blank

Chapter 5
Enabling Change

The Need for Change Enablement

Successful implementation or improvement depends on implementing the appropriate change (the good practices) in the correct way. In many enterprises, there is a significant focus on the first aspect, but not enough emphasis on managing the human, behavioural and cultural aspects of the change and motivating stakeholders to buy into the change. Change enablement is one of the biggest challenges to GEIT implementation.

It should not be assumed that the various stakeholders involved in, or affected by, new or revised governance arrangements will necessarily readily accept and adopt the change. The possibility of ignorance and/or resistance to change needs to be addressed through a structured and proactive approach. Also, optimal awareness of the programme should be achieved through a communication plan that defines what will be communicated, in what way and by whom throughout the various phases of the programme.

When reviewing a major recent IT transformation initiative, the US Department of Veterans Affairs (VA) noted, 'The primary challenge the VA will face in achieving this transformation will be gaining the acceptance and support of all VA personnel, including leadership, middle managers and field staff'.[5] The VA has stated that its effort cannot succeed if it only addresses technological transformation; it recognises that the human factor that is needed to achieve acceptance, change the enterprise and change the way business is conducted is critical to success.

In many enterprises, there is not enough emphasis on managing the human, behavioural and cultural aspects of the change and motivating stakeholders to buy into the change.

COBIT 5 defines change enablement as:

> *A systematic process of ensuring that all stakeholders are prepared and committed to the changes involved in moving from a current state to a desired future state.*

All key stakeholders should be involved. At a high level, change enablement typically entails:
- Assessing the impact of the change on the enterprise, its people and other stakeholders
- Establishing the future state (vision) in human/behavioural terms and the associated measures that describe it
- Building 'change response plans' to manage change impacts proactively and maximise engagement throughout the process. These plans may include training, communication, organisation design (job content, organisational structure), process redesign and updated performance management systems.
- Continually measuring the change progress towards the desired future state

In terms of a typical GEIT implementation, the objective of change enablement is having enterprise stakeholders from the business and IT leading by example and encouraging staff at all levels to work according to the desired new way. Examples of desired behaviour include:
- Following agreed-on processes
- Participating in defined GEIT structures such as a change approval or advisory board
- Enforcing defined guiding principles, policies, standards, processes or practices such as a policy regarding new investments or security

This can be best achieved by gaining the commitment of the stakeholders (diligence and due care, leadership, and in communicating and responding to the workforce) and selling the benefits. If necessary, it may be required to enforce compliance. In other words, human, behavioural and cultural barriers must be overcome so that there is a common interest to properly adopt, instil a will to adopt and ensure the ability to adopt a new way. It may be useful to draw on change enablement skills within the enterprise or, if necessary, from external consultants to facilitate the change in behaviour.

[5] Walters, Jonathan; 'Transforming Information Technology at the Department of Veterans Affairs', IBM Center for the Business of Government, USA, 2009

Change Enablement of GEIT Implementation

Various approaches to enabling change have been defined over the years and they provide valuable input that could be utilised during the implementation life cycle. One of the most widely accepted approaches to change enablement has been developed by John Kotter:[6]

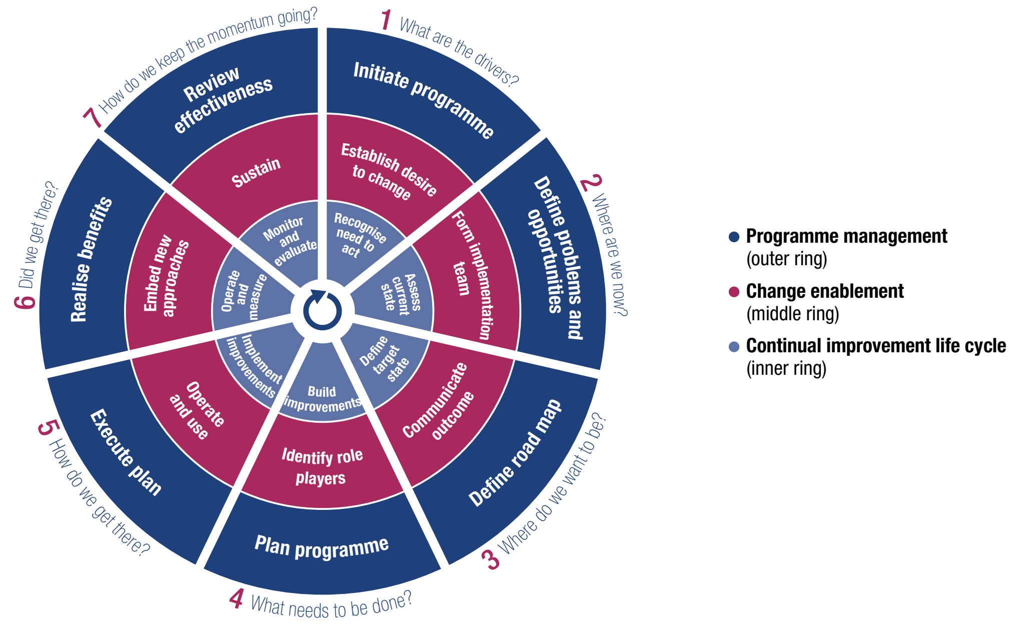
1. Establish a sense of urgency.
2. Form a powerful guiding coalition.
3. Create a clear vision that is expressed simply.
4. Communicate the vision.
5. Empower others to act on the vision.
6. Plan for and create short-term wins.
7. Consolidate improvements and produce more change.
8. Institutionalise new approaches.

Human, behavioural and cultural barriers must be overcome so that there is a common interest to properly adopt, instil a will to adopt and ensure the ability to adopt a new way.

The Kotter approach has been chosen as an example and adapted for the specific requirements of a GEIT implementation or improvement. This is illustrated by the change enablement life cycle in **figure 14**.

The following subsections create a high-level, but holistic, overview by discussing briefly each phase of the change enablement life cycle as applied to a typical GEIT implementation.

Figure 14—Seven Phases of the Implementation Life Cycle



Phases in the Change Enablement Life Cycle Create the Appropriate Environment

The overall enterprise environment should be analysed to determine the most appropriate change enablement approach. This will include aspects such as the management style, culture (ways of working), formal and informal relationships, and attitudes. It is also important to understand other IT or enterprise initiatives that are ongoing or planned, to ensure that dependencies and impacts are considered.

It should be ensured from the start that the required change enablement skills, competencies and experience are available and utilised, for example, by involving resources from the HR function or by obtaining external assistance.

As an outcome of this phase, the appropriate balance of directive and inclusive change enablement activities required to deliver sustainable benefits can be designed.

[6] Kotter, John; *Leading Change*, Harvard Business School Press, USA, 1996

Phase 1—Establish the Desire to Change

The purpose of this phase is to understand the breadth and depth of the envisioned change, the various stakeholders that are affected, the nature of the impact on and involvement required from each stakeholder group, as well as the current readiness and ability to adopt the change.

Current pain points and trigger events can provide a good foundation for establishing the desire to change. The 'wake-up call', an initial communication on the programme, can be related to real-world issues that the enterprise may be experiencing. Also, initial benefits can be linked to areas that are highly visible to the enterprise, creating a platform for further changes and more widespread commitment and buy-in.

While communication is a common thread throughout the implementation or improvement initiative, the initial communication or wake-up call is one of the most important and should demonstrate the commitment of senior management. Therefore, it should ideally be communicated by the executive committee or CEO.

Phase 2—Form an Effective Implementation Team

Dimensions to consider in assembling an effective core implementation team include involving the appropriate areas from business and IT as well as the knowledge and expertise, experience, credibility, and authority of team members. Obtaining an independent, objective view, as provided by external parties such as consultants and a change agent, could also be highly beneficial by aiding the implementation process or addressing skill gaps that may exist within the enterprise. Therefore, another dimension to consider is the appropriate mix of internal and external resources.

The essence of the team should be a commitment to:

- A clear vision of success and ambitious goals
- Engaging the best in all team members, all the time
- Clarity and transparency of team processes, accountabilities and communications
- Integrity, mutual support and commitment to each other's success
- Mutual accountability and collective responsibility
- Ongoing measurement of its own performance and the way it behaves as a team
- Living out of its comfort zone, always looking for ways to improve, uncovering new possibilities and embracing change

It is important to identify potential change agents within different parts of the business that the core team can work with to support the vision and cascade changes down.

Phase 3—Communicate Desired Vision

A high-level change enablement plan should be developed in conjunction with the overall programme plan. A key component of the change enablement plan is the communication strategy, which should address who the core audience groups are, their behavioural profiles and information requirements, communication channels, and principles.

The desired vision for the implementation or improvement programme should be communicated in the language of those affected by it. The communication should include the rationale for and benefits of the change as well as the impacts of not making the change (purpose), the vision (picture), the road map to achieving the vision (plan) and the involvement required of the various stakeholders (part).[7] Senior management should deliver key messages (such as the desired vision). It should be noted in the communication that both behavioural/cultural and logical aspects should be addressed, and that the emphasis is on two-way communication. Reactions, suggestions and other feedback should be acted upon and captured.

Phase 4—Empower Role Players and Identify Quick Wins

As core improvements are designed and built, change response plans are developed to empower various role players. The scope of these may include:

- Organisational design changes such as job content or team structures
- Operational changes such as process flows or logistics
- People management changes such as required training and/or changes to performance management and reward systems

Any quick wins that can be realised are important from a change enablement perspective. These could be related to the pain points and trigger events discussed in chapter 3. Visible and unambiguous quick wins can build momentum and credibility for the programme and help to address any scepticism that may exist.

It is imperative to use a participative approach in the design and building of the core improvements. By engaging those affected by the change in the actual design, e.g., through workshops and review sessions, buy-in can be increased.

[7] The 'four Ps' (purpose, picture, plan and part) is from: Bridges, William; *Managing Transitions: Making the Most of Change*, Addison-Wesley, USA, 1999

Phase 5—Enable Operation and Use

As initiatives are implemented within the core implementation life cycle, the change response plans also are implemented. Quick wins that have been realised are built on, and the behavioural and cultural aspects of the broader transition are addressed (issues such as dealing with fears of loss of responsibility, new expectations and unknown tasks).

It is important to balance group and individual interventions to increase buy-in and engagement and to ensure that all stakeholders obtain a holistic view of the change.

Solutions will be rolled out, and during this process, mentoring and coaching will be critical to ensure uptake in the user environment. The change requirements and objectives that had been set during the start of the initiative should be revisited to ensure that they were adequately addressed.

Success measures should be defined and should include both hard business measures and perception measures that track how people feel about a change.

Phase 6—Embed New Approaches

As concrete results are achieved, new ways of working should become part of the enterprise's culture and be rooted in its norms and values (the way we do things around here) by, for example, implementing policies, standards and procedures. The implemented changes should be tracked, and the effectiveness of the change response plans should be assessed and corrective measures taken as appropriate. This might include enforcing compliance where still required.

The communication strategy should be maintained to sustain ongoing awareness.

Changes are sustained by stakeholders leading by example, through conscious reinforcement and an ongoing communication campaign.

Phase 7—Sustain

Changes are sustained through conscious reinforcement and an ongoing communication campaign, and they are maintained and demonstrated by continued top management commitment.

Corrective action plans are implemented, lessons learned are captured and knowledge is shared with the broader enterprise.

Chapter 6
Implementation Life Cycle Tasks, Roles and Responsibilities

Introduction

Continual improvement of GEIT is accomplished using the seven-phase implementation life cycle. Each phase is described with:

- A chart summarising the responsibilities of each group of role players in the phase. Note that these roles are generic and not every role necessarily must exist as a specific function.
- A table for each phase containing:
  - Phase objective
  - Phase description
  - Continual improvement tasks
  - Change enablement tasks
  - Programme management tasks
  - Examples of the inputs likely to be required
  - Suggested ISACA and other framework items to be utilised
  - The outputs that need to be produced
- A RACI chart describing who is responsible, accountable, consulted and informed for key activities selected from the continual improvement (CI), change enablement (CE) and programme management (PM) tasks, with corresponding cross-references. The activities covered in the RACI chart are the most important ones, e.g., activities that produce deliverables or outputs to the next phase, have a milestone attached to them, or are critical to the success of the overall initiative. Not all activities are included, in the interest of keeping this guidance concise.

This guidance is not intended to be prescriptive, but rather a generic phase and task plan that should be adapted to suit a specific implementation.

Phase 1—What Are the Drivers?

Figures 15, 16, 17 and **18** describe phase 1.

Figure 15—Continual Improvement Life Cycle Phase 1

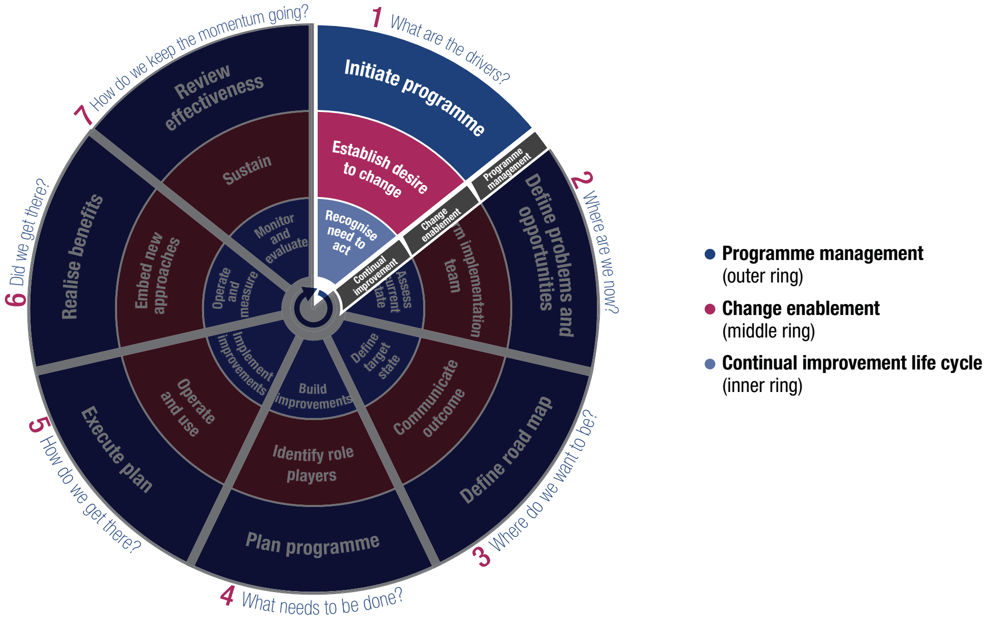


Figure 16—Roles in Phase 1

When you are...	Your role in this phase is to...
Board and executive	Provide guidance regarding stakeholder needs, business strategy, priorities, objectives and guiding principles with respect to governance and management of enterprise IT. Approve the high-level approach.
Business management	Together with IT, ensure that stakeholder needs and business objectives have been stated with sufficient clarity to enable translation into business goals for IT, and provide input to understanding of risk and priorities.
IT management	Gather requirements and objectives from all stakeholders, gaining consensus on approach and scope. Provide expert advice and guidance regarding IT matters.
Internal audit	Provide advice and challenge proposed activities and actions, ensuring that objective and balanced decisions are made. Provide input on current issues. Provide advice regarding controls and risk management practices and approaches.
Risk, compliance and legal	Provide advice and guidance regarding risk, compliance and legal matters. Ensure that the management-proposed approach is likely to meet risk, compliance and legal requirements.

Figure 17—Phase 1 Description

Phase 1	What Are the Drivers?
Phase objective	Obtain an understanding of the programme background and objectives and current governance approach. Define the initial programme concept business case. Obtain the buy-in and commitment of all key stakeholders.
Phase description	This phase articulates the compelling reasons to act within the organisational context. In this context the programme background, objectives and current governance culture are defined. The initial programme concept business case is defined. The buy-in and commitment of all key stakeholders is obtained.
Continual improvement (CI) tasks	Recognise the need to act: 1. Identify current governance context, business IT and IT pain points, events and symptoms triggering the need to act. 2. Identify the business and governance drivers and compliance requirements for improving GEIT and assess current stakeholder needs. 3. Identify business priorities and business strategy dependent on IT, including any current significant projects. 4. Align with enterprise policies, strategies, guiding principles and any ongoing governance initiatives. 5. Raise executive awareness of IT's importance to the enterprise and the value of GEIT. 6. Define GEIT policy, objectives, guiding principles and high-level improvement targets. 7. Ensure that the executives and board understand and approve the high-level approach and accept the risk of not taking any action on significant issues.
Change enablement (CE) tasks	Establish the desire to change: 1. Ensure integration with enterprise-level change enablement approaches or programmes, if any exist. 2. Analyse the general organisational environment in which the change needs to be enabled, including organisation structure, management style(s), culture, ways of working, formal and informal relationships, and attitudes. 3. Determine other ongoing or planned enterprise initiatives to determine change dependencies or impacts. 4. Understand the breadth and depth of the change. 5. Identify stakeholders involved in the initiative from different areas of the enterprise (e.g., business, IT, audit, risk management) as well as different levels (e.g., executives, middle management) and consider their needs. 6. Determine the level of support and involvement required from each stakeholder group or individual, their influence and the impact of the change initiative on them. 7. Determine the readiness and ability to implement the change for each stakeholder group or individual. 8. Establish a wake-up call, using the pain points and trigger events as a starting point, and communicated by the IT executive strategy or steering committee (or an equivalent governance structure) to create awareness of the programme, its drivers and its objectives amongst all stakeholders. 9. Eliminate any false signs of security or complacency by, for example, highlighting compliance or exception figures. 10. Instil the appropriate level of urgency, depending on the priority and impact of the change.
Programme management (PM) tasks	Initiate the programme: 1. Provide high-level strategic direction and set high-level programme objectives in agreement with the IT executive strategy committee or equivalent (if one exists). 2. Define and assign high-level roles and responsibilities within the programme, starting with the executive sponsor to the programme manager and all important stakeholders. 3. Develop an outline business case indicating the success factors to be used to enable performance monitoring and reporting of the success of the governance improvement. 4. Obtain executive sponsorship.
Input	• Enterprise policies, strategies, governance and business plans, and audit reports • Other major enterprise initiatives with which there may be dependencies or impacts • IT steering committee performance reports, help desk statistics, IT customer surveys or other inputs that indicate current IT pain points • Any useful and relevant industry overviews, case studies and success stories, *www.isaca.org/cobitcasestudies* • Specific customer requirements, marketing and servicing strategy, market position, enterprise vision and mission statements

Figure 17—Phase 1 Description *(cont.)*	
Phase 1	**What Are the Drivers?**
ISACA materials and other frameworks	• COBIT 5 (enterprise goals, enablers) • *COBIT 5: Enabling Processes* (EDM01; APO01; MEA01), *www.isaca.org/cobit* • *COBIT 5 Implementation* (appendices A. Mapping Pain Points to COBIT 5 Processes, B. Example Decision Matrix and D. Example Business Case) • ISACA supporting products as currently defined at *www.isaca.org* • *The Business Case Guide: Using Val IT 2.0*
Output	• Business case outline • High-level roles and responsibilities • Identified stakeholder map, including support and involvement required, influence and impact, and agreed-on understanding of the efforts required to manage human change • Programme wake-up call (all stakeholders) • Programme kick-off communication (key stakeholders)

Figure 18—Phase 1 RACI Chart

	Responsibilities of Implementation Role Players								
Key Activities	**Board**	**IT Executive Committee**	**CIO**	**Business Executive**	**IT Managers**	**IT Process Owners**	**IT Audit**	**Risk and Compliance**	**Programme Steering**
Identify issues triggering need to act (CI1).	C/I	A	R	R	C	C	C	C	R
Identify business priorities and strategies affecting IT (CI3).	C	A	R	R	C	C	C	C	R
Gain management agreement to act and obtain executive sponsorship (CI7).	C	A/R	R	C	I	I	I	I	R
Instil the appropriate level of urgency to change (CE10).	I	A	R	R	C	C	C	C	R
Produce convincing outline business case (PM3).	I	A	R	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Phase 2—Where Are We Now?

Figures 19, 20, 21 and **22** describe phase 2.

Figure 19—Continual Improvement Life Cycle Phase 2

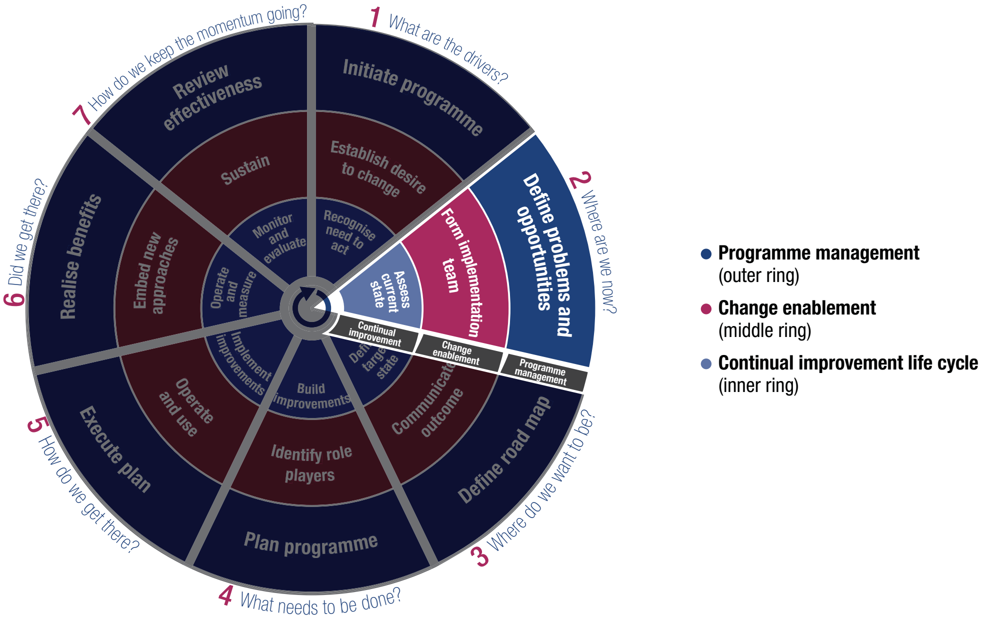


Figure 20—Roles in Phase 2

When you are...	Your role in this phase is to...
Board and executive	Verify and interpret the results/conclusions of assessments.
Business management	Assist IT with reasonableness of current assessments by providing the customer view.
IT management	Ensure open and fair assessment of IT activities. Guide assessment of current practice. Obtain consensus.
Internal audit	Provide advice, provide input to and assist with current-state assessments. If required, independently verify assessment results.
Risk, compliance and legal	Review assessment to ensure that risk, compliance and legal issues have been considered adequately.

Figure 21—Phase 2 Description

Phase 2	Where Are We Now?
Phase objective	Ensure that the programme team knows and understands the enterprise goals and how the business and IT function need to deliver value from IT in support of the enterprise goals, including any current significant projects. Identify the critical processes or other enablers that will be addressed in the improvement plan. Identify the appropriate management practices for each selected process. Obtain an understanding of the enterprise's present and future attitude towards risk and IT risk position and determine how it will impact the programme. Determine the current capability of the selected processes. Understand the enterprise's capacity and capability for change.
Phase description	This phase identifies the enterprise and IT-related goals, i.e., how IT contributes to the enterprise goals identified via solutions and services. The focus is on identifying and analysing how IT creates value for the enterprise in enabling business transformation in an agile way, in making the current business processes more efficient, in making the enterprise more effective, and in meeting governance-related requirements such as managing risk, ensuring security, and complying with legal and regulatory requirements. Based on the enterprise risk profile and its risk history and appetite, and actual benefit/value enablement risk, define benefit/value enablement risk, programme/project delivery and service delivery/IT operations risk to the enterprise and IT-related goals. Appendix C contains a table mapping generic risk scenarios to COBIT 5 processes that can be used to support this analysis. The understanding of business and governance drivers and a risk assessment are used to focus on the processes critical to ensuring that IT goals are met. Then, it is necessary to establish how mature, well managed and executed these processes are, based on process descriptions, policies, standards, procedures and technical specifications, to determine whether they are likely to support the business and IT requirements. This is achieved by assessing the capability for each process. The presence of specific pain points in an enterprise could also contribute to the selection of IT processes on which to focus. Appendix A of this document provides example mappings of common pain points (as discussed in chapter 4) to COBIT 5 processes. There is also an illustration of all 37 processes within the process reference model.
Continual improvement (CI) tasks	Assess current state: Understand how IT needs to support the current enterprise goals (the COBIT 5 goals cascade material in the COBIT 5 framework and *COBIT 5: Enabling Processes* provides generic examples and relationships that can be used): 1. Identify key enterprise and supporting IT-related goals. 2. Establish the significance and nature of IT's contribution (solutions and services) required to support business objectives. 3. Identify key governance issues and weaknesses related to the current and required future solutions and services, the enterprise architecture needed to support the IT-related goals, and any constraints or limitations. 4. Identify and select the processes critical to support IT-related goals and, if appropriate, key management practices for each selected process. 5. Assess benefit/value enablement risk, programme/project delivery and service delivery/IT operations risk related to critical IT processes. 6. Identify and select IT processes critical to ensure that risk is avoided. 7. Understand the risk acceptance position as defined by management. Assess actual performance (refer to chapter 7. Using the COBIT 5 Components): 8. Define the method for executing the assessment. 9. Document understanding of how the current process actually addresses the management practices selected earlier. 10. Analyse the current level of capability. 11. Define the current process capability rating.

Figure 21—Phase 2 Description *(cont.)*

Phase 2	Where Are We Now?
Change enablement (CE) tasks	Form a powerful implementation team: 1. Assemble a core team from the business and IT with the appropriate knowledge, expertise, profile, experience, credibility and authority to drive the initiative. Identify the most desirable person (effective leader and credible to the stakeholders) to lead this team. Consider the use of external parties, such as consultants, as part of the team to provide an independent and objective view or to address any skill gaps that may exist. 2. Identify and manage any potential vested interests that may exist within the team to create the required level of trust. 3. Create the appropriate environment for optimal teamwork. This includes ensuring that the necessary time and involvement can be given. 4. Hold a workshop to create consensus (shared vision) within the team and adopt a mandate for the change initiative. 5. Identify change agents that the core team can work with using the principle of cascading sponsorship (having sponsors at various hierarchical levels supporting the vision, spreading the word on quick wins, cascading changes down, working with any blockers and cynics that may exist) to ensure widespread stakeholder buy-in during each phase of the life cycle. 6. Document strengths identified during the current state assessment that can be used for positive elements in communications as well as potential quick wins that can be leveraged from a change enablement perspective.
Programme management (PM) tasks	Define problems and opportunities: 1. Review and evaluate the outline business case, programme feasibility and potential return on investment (ROI). 2. Assign roles, responsibilities and process ownership and ensure commitment and support of affected stakeholders in the definition and execution of the programme. 3. Identify challenges and success factors.
Input	• Outline business case • High-level roles and responsibilities • Identified stakeholder map, including support and involvement required, influence and impact, and readiness and ability to implement or buy into the change • Programme wake-up call (all stakeholders) • Programme kick-off communication (key stakeholders) • Business and IT plans and strategies • IT process descriptions, policies, standards, procedures, technical specifications • Understanding of business and IT contribution • Audit reports, risk management policy, IT performance reports/dashboards/ scorecards • Business continuity plans (BCPs), impact analyses, regulatory requirements, enterprise architectures, service level agreements (SLAs), operational level agreements (OLAs) • Investment programme and project portfolios, programme and project plans, project management methodologies, project reports
ISACA resources	• COBIT 5 (enterprise goals—IT-related goals cascade and mapping of stakeholder needs to goals), *www.isaca.org/cobit* • *COBIT 5: Enabling Processes* APO01; APO02; APO05; APO12; BAI01; MEA01; MEA02; MEA03 (used for process selection as well as implementation and programme planning) • *COBIT 5 Implementation* (chapter 5. Enabling Change and appendix E. COBIT 4.1 Maturity Attribute Table) • COBIT 5 self-assessment guide (planned publication) • ISACA supporting products as currently defined at *www.isaca.org*
Output	• Agreed-on enterprise goals for IT and impact on IT • An agreed-on understanding of the risk and impacts resulting from misaligned IT-related goals and service and project delivery failures • Selected processes and goals • Current capability rating for selected processes • Risk acceptance position and risk profile • Benefit/value enablement risk, programme/project delivery and service delivery/IT operations risk assessments • Strengths on which to build • Change agents in different parts and at different levels in the enterprise • Core team and assigned roles and responsibilities • Evaluated outline business case • An agreed-on understanding of the issues and challenges (including process capability levels)

Figure 22—Phase 2 RACI Chart

	Responsibilities of Implementation Role Players								
Key Activities	Board	IT Executive Committee	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Programme Steering
Identify key IT goals supporting business goals (CI1).	I	C	R	C	R	C	C	C	A
Identify processes critical to support IT and business goals (CI4).		I	R	C	R	C	C	C	A
Assess risk related to achievement of goals (CI5).		I	R	C	R	R	C	R	A
Identify processes critical to ensure that key risk is avoided (CI6).		I	R	R	R	C	C	R	A
Assess current performance of critical processes (CI1 to CI11).		I	R	C	R	R	C	C	A
Assemble a core team from the business and IT (CE1).		I	R	R	C	C	C	C	A
Review and evaluate the business case (PM1).	I	A	R	R	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Phase 3—Where Do We Want To Be?

Figures 23, 24, 25 and **26** describe phase 3.

Figure 23—Continual Improvement Life Cycle Phase 3

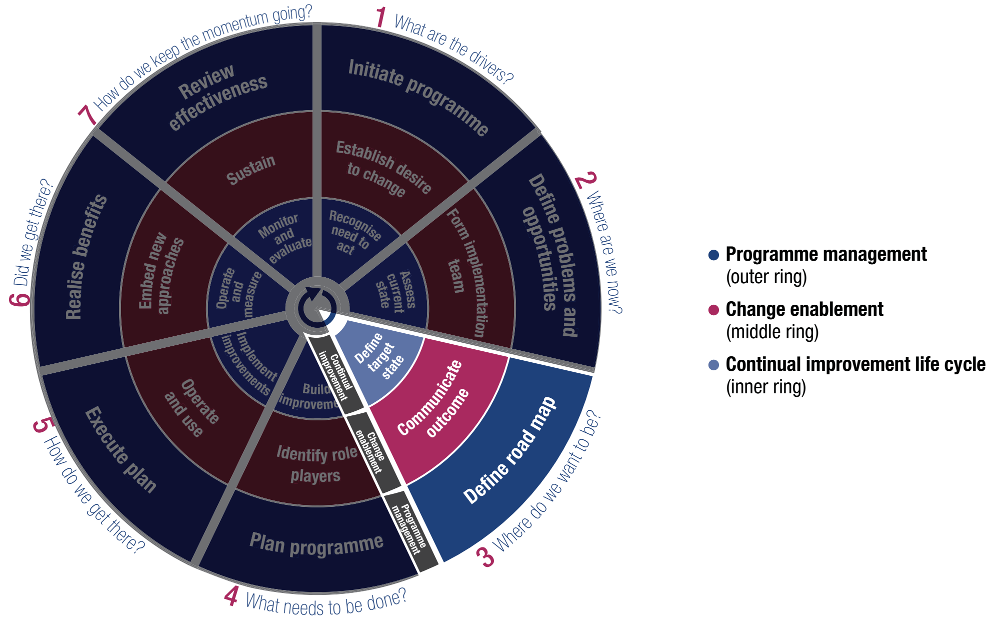


Figure 24—Roles in Phase 3

When you are...	Your role in this phase is to...
Board and executive	Set priorities, time scales and expectations regarding the future capability required from IT.
Business management	Assist IT with the setting of capability targets. Ensure that the envisaged solutions are aligned to enterprise goals.
IT management	Apply professional judgement in formulating improvement priority plans and initiatives. Obtain consensus on a required capability target. Ensure that the envisaged solution is aligned to IT-related goals.
Internal audit	Provide advice and assist with target-state positioning and gap priorities. If required, independently verify assessment results.
Risk, compliance and legal	Review plans to ensure that risk, compliance and legal issues have been addressed adequately.

Figure 25—Phase 3 Description

Phase 3	Where Do We Want To Be?
Phase objective	Determine the targeted capability for each of the selected processes. Determine the gaps between the as-is and the to-be positions of the selected processes, and translate these gaps into improvement opportunities. Use this information to create a detailed business case and high-level programme plan.
Phase description	Based on the assessed current-state process capability levels, and using the results of the enterprise goals to IT-related goals analysis and identification of process importance performed earlier, an appropriate target capability level should be determined for each process. The chosen level should take into account available external and internal benchmarks. It is important to ensure the appropriateness to the business of the level chosen. After the current capability of the process has been determined and the target capability planned, the gaps between as-is and to-be states should be evaluated and opportunities for improvement identified. After the gaps have been defined, the root causes, common issues, residual risk, existing strengths and best practices to close those gaps need to be determined. This phase may identify some relatively easy-to-achieve improvements such as improved training, the sharing of good practices and standardising procedures; however, the gap analysis is likely to require considerable experience in business and IT management techniques to develop practical solutions. Experience in undertaking behavioural and organisational change will also be needed. Understanding of process techniques, advanced business and technical expertise, and knowledge of business and system management software applications and services may be needed. To ensure that this phase is executed effectively, it is important for the team to work with the business and IT process owners and other required stakeholders, engaging internal expertise. If necessary, external advice should also be obtained. Risk that will not be mitigated after closing the gaps should be identified and formally accepted by management.
Continual improvement (CI) tasks	Define target state and analyse gaps: 1. Define target for improvement: • Based on enterprise requirements for performance and conformance, decide initial ideal short- and long-term target capability levels for each process. • To the extent possible, benchmark internally to identify better practices that can be adopted. • To the extent possible, benchmark externally with competitors and peers to help decide appropriateness of the chosen target level. • Do a ‘sanity check’ of the reasonableness of the targeted level (individually and as a whole), looking at what is achievable and desirable and can have the greatest positive impact within the chosen time frame. 2. Analyse gaps: • Use understanding of current capability (by attribute) and compare it to the target capability level. • Leverage existing strengths wherever possible to deal with gaps, and seek guidance from COBIT 5 management practices and activities and other specific good practices and standards such as ITIL, ISO/IEC 27000, TOGAF and Project Management Body of Knowledge (PMBOK) to close other gaps. • Look for patterns that indicate root causes to be addressed. 3. Identify potential improvements: • Collate gaps into potential improvements. • Identify unmitigated residual risk and ensure to accept formally.
Change enablement (CE) tasks	Describe and communicate desired outcome: 1. Describe the high-level change enablement plan and objectives, which will include the following tasks and components. 2. Develop a communication strategy (including core audience groups, behavioural profile and information requirements per group, core messages, optimal communication channels, and communication principles) to optimise awareness and buy-in. 3. Secure willingness to participate (picture of the change). 4. Articulate the rationale for, and benefits of, the change to support the vision and describe the impact(s) of not making the change (purpose of the change). 5. Link back to objectives for the initiative in the communications and demonstrate how the change will realise the benefit. 6. Describe the high-level road map to achieving the vision (plan for the change) as well as the involvement required of various stakeholders (role within the change). 7. Use senior management to deliver key messages to ‘set the tone at the top’. 8. Use change agents to communicate informally in addition to formal communications. 9. Communicate through action—the guiding team should set an example. 10. Appeal to their emotions where required to get people to change behaviours. 11. Capture initial communication feedback (reactions and suggestions) and adapt the communication strategy accordingly.

Figure 25—Phase 3 Description *(cont.)*

Phase 3	Where Do We Want To Be?
Programme management (PM) tasks	Define road map: 1. Set programme direction, scope, benefits and objectives at a high level. 2. Ensure alignment of the objectives with business and IT strategies. 3. Consider risk and adjust scope accordingly. 4. Consider change enablement implications. 5. Obtain necessary budgets and define programme accountabilities and responsibilities. 6. Create and evaluate a detailed business case, budget, time lines and high-level programme plan.
Input	• Agreed-on enterprise goals and impact on IT-related goals • Current capability rating for selected processes • Definition of IT-related goals • Selected processes and goals • Risk acceptance position and risk profile • Assessed benefit/value enablement risk, programme/project delivery and service delivery/IT operations risk assessment • Strengths on which to build • Change agents in different parts and at different levels in the enterprise • Core team and assigned roles and responsibilities • Evaluated outline business case • Challenges and success factors • Internal and external capability benchmarks • Good practices from COBIT 5 and other references • Stakeholder analysis
ISACA resources	• COBIT 5 (enterprise goals), *www.isaca.org/cobit* • *COBIT 5: Enabling Processes* (management practices and activities for the target-state definition and gap analysis; APO01, APO02) • COBIT 5 self-assessment guide (planned publication) • ISACA supporting products—e.g., mappings of COBIT 4.1 to other frameworks and best practices—as currently defined at *www.isaca.org*
Output	• Target capability rating for selected processes • Description of improvement opportunities • Risk response document including risk not mitigated • Change enablement plan and objectives • Communication strategy and communication of the change vision covering the four Ps (picture, purpose, plan, part) • Detailed business case • High-level programme plan • Key metrics that will be used to track programme and operational performance

Figure 26—Phase 3 RACI Chart

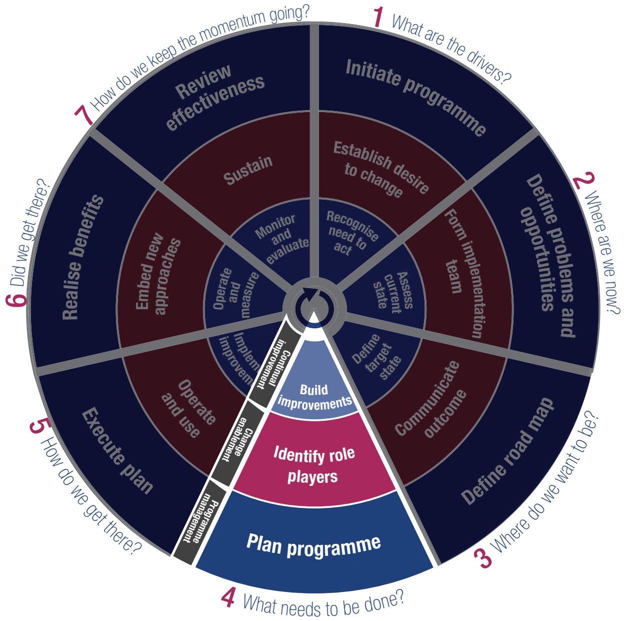
	Responsibilities of Implementation Role Players								
Key Activities	Board	IT Executive Committee	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Programme Steering
Agree on target for improvement (CI1).	I	A	R	C	R	R	C	C	R
Analyse gaps (CI2).		I	R	C	R	R	C	C	A
Identify potential improvements (CI3).		I	R	C	R	R	C	C	A
Communicate change vision (CE3).		A	R	R	C	I	I	I	R
Set programme direction and prepare detailed business case (PM1, PM6).	I	A	R	C	C	C	I	I	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Phase 4—What Needs To Be Done?

Figures 27, 28, 29 and **30** describe phase 4.

Figure 27—Continual Improvement Life Cycle Phase 4



- ● **Programme management** (outer ring)
- ● **Change enablement** (middle ring)
- ● **Continual improvement life cycle** (inner ring)

Figure 28—Roles in Phase 4

When you are...	Your role in this phase is to...
Board and executive	Consider and challenge proposals, support justified actions, provide budgets, and set priorities as appropriate.
Business management	Together with IT, ensure that the proposed improvement actions are aligned with agreed-on enterprise and IT-related goals and that any activities requiring business input or action are supported. Ensure that required business resources are allocated and available. Agree with IT on the metrics for measuring the outcomes of the improvement programme.
IT management	Ensure viability and reasonableness of the programme plan. Ensure that the plan is achievable and that there are resources available to execute the plan. Consider the plan together with priorities of the enterprise's portfolio of IT-enabled investments to decide a basis for investment funding.
Internal audit	Provide independent assurance that issues identified are valid, business cases are objectively and accurately presented, and plans appear achievable. Provide expert advice and guidance where appropriate.
Risk, compliance and legal	Ensure that any identified risk, compliance and legal issues are being addressed, and proposals conform with any relevant policies or regulations.

Figure 29—Phase 4 Description

Phase 4	What Needs To Be Done?
Phase objective	Translate improvement opportunities into justifiable contributing projects. Prioritise and focus on the high-impact projects. Integrate the improvement projects into the overall programme plan. Execute quick wins.
Phase description	When all of the potential initiatives for improvement have been identified, these initiatives should be prioritised into formal and justifiable projects. The projects with high benefit and that are relatively easy to implement should be selected first and translated into formal and justifiable projects, each with a project plan that includes the project's contribution to the programme objectives. It is important to check whether the objectives still conform to the original value and risk drivers. The projects will be included in an updated business case for the programme. Details of any unapproved improvement project proposals should be recorded in a register for potential future consideration and opportunities presented for sponsors to reappraise and, when appropriate, resubmit their recommendations at a later date. Based on an opportunity grid, the project definitions, the resource plan and the IT budget, the identified and prioritised improvements are now turned into a set of documented projects that support the overall improvement programme. The impact on the enterprise of executing the programme is determined and a change plan is prepared that describes the programme activities that will ensure, in practical terms, that the improvements delivered by the projects will be rolled into the enterprise in a sustainable manner. An important element in this phase is the definition of metrics—i.e., the programme's success metrics—that will measure whether the process improvements are likely to deliver the original business benefits. The complete improvement programme schedule should be documented on a Gantt chart. New projects may identify a need to change or improve the organisational structures or other enablers required to sustain effective governance. If required, it may be necessary to include actions to improve the environment (as described in chapter 5).

Figure 29—Phase 4 Description *(cont.)*

Phase 4	What Needs To Be Done?
Continual improvement (CI) tasks	Design and build improvements: 1. For each improvement, consider the potential benefit and ease of implementation (cost, effort, sustainability). 2. Plot improvements onto an opportunity grid to identify priority actions (based on benefit and ease of implementation). 3. Focus on alternatives showing high benefit/high ease of implementation. 4. Consider any other actions showing high benefit/low ease of implementation for possible scaled-down improvements (decompose into smaller improvements and look again at benefits and ease of implementation). 5. Prioritise and select improvements. 6. Analyse selected improvements to the detail required for high-level project definition, considering approach, deliverables, resources required, estimated costs, estimated time scales, dependencies and project risk. Use available best practices and standards to further refine detailed improvement requirements. Discuss with managers and teams responsible for the process area. 7. Consider feasibility, link back to the original value and risk drivers, and agree on projects to be included in the business case for approval. 8. Record unapproved projects and initiatives in a register for potential future consideration.
Change enablement (CE) tasks	Empower role players and identify quick wins: 1. Obtain buy-in by engaging those affected by the change in the design through mechanisms such as workshops or review processes and giving them responsibility to accept the quality of results. 2. Design change response plans to proactively manage change impacts and maximise engagement throughout the implementation process (could include organisational changes such as job content or organisational structure; people management changes such as training; performance management systems; or incentives/remuneration and reward systems). 3. Identify quick wins that prove the concept of the improvement programme. These should be visible and unambiguous, build momentum, and provide positive reinforcement of the process. 4. Where possible, build on any existing strengths identified in phase 2 to realise quick wins. 5. Identify strengths in existing enterprise processes that could be leveraged. For example, strengths in project management may exist in other areas of the business such as product development (avoid reinventing the wheel, and align wherever possible to current enterprisewide approaches).
Programme management (PM) tasks	Develop programme plan: 1. Organise potential projects into the overall programme, in preferred sequence, considering contribution to desired outcomes, resource requirements and dependencies. 2. Use portfolio management techniques to ensure that the programme conforms to strategic goals and IT has a balanced set of initiatives. 3. Identify the impact of the improvement programme on the IT and business organisations and indicate how the improvement momentum is to be maintained. 4. Develop a change plan documenting any migration, conversion, testing, training, process or other activities that must be included within the programme as part of implementation. 5. Identify and agree on metrics for measuring the outcomes of the improvement programme in terms of the original programme success factors. 6. Guide the allocation and prioritisation of business, IT and audit resources necessary to achieve programme and project objectives. 7. Define a portfolio of projects that will deliver the required outcomes for the programme. 8. Define the required deliverables, considering the full scope of activities required to meet objectives. 9. Nominate, if required, project steering committees for specific projects within the programme. 10. Establish project plans and reporting procedures to enable progress to be monitored.
Input	• Target maturity rating for selected processes • Description of improvement opportunities • Risk response document • Change enablement plan and objectives • Communication strategy and communication of the change vision covering four Ps (picture, purpose, plan, part) • Detailed business case • Opportunity worksheet, best practices and standards, external assessments, technical evaluations • Opportunity grid, project definitions, project portfolio management plan, resource plan, IT budget • Strengths identified in earlier phases
ISACA resources	• COBIT 5 (enabler models), *www.isaca.org/cobit* • *COBIT 5: Enabling Processes* (APO5, APO12, BAI01; goals and metrics) • ISACA supporting products as currently defined at *www.isaca.org*
Output	• Improvement project definitions • Defined change response plans • Identified quick wins • Record of unapproved projects • Programme plan that sequences individual plans with allocated resources, priorities and deliverables • Project plans and reporting procedures enabled through committed resources, e.g., skills, investment • Success metrics

Figure 30—Phase 4 RACI Chart

Key Activities	Board	IT Executive Committee	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Programme Steering
	Responsibilities of Implementation Role Players								
Prioritise and select improvements (CI5).		A	R	C	C	R	C	C	R
Define and justify projects (CI6 and CI7).		I	R	C	R	R	C	C	A
Design change response plans (CE2).		I	R	R	C	C	C	C	A
Identify quick wins and build on existing strengths (CE3).		I	C	C/I	R	R	C/I	C/I	A
Develop programme plan with allocated resources and project plans (PM1 to PM10).		A	C	C	R	C	I	I	R

A **R**ACI chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Phase 5—How Do We Get There?

Figures 31, 32, 33 and **34** describe phase 5.

Figure 31—Continual Improvement Life Cycle Phase 5

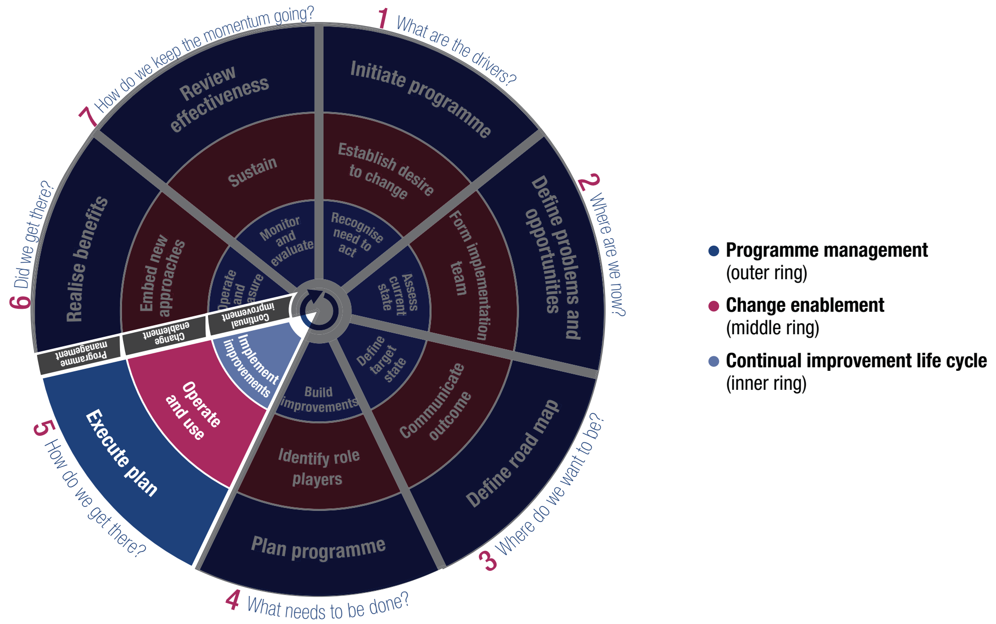


Figure 32—Roles in Phase 5

When you are...	Your role in this phase is to...
Board and executive	Monitor implementation and provide support and direction as required.
Business management	Take ownership for business participation in the implementation, especially where business processes are affected and IT processes require user/customer involvement.
IT management	Make sure that the implementation includes the full scope of activities required (e.g., policy and process changes, technology solutions, organisational changes, new roles and responsibilities, other enablers) and that they are practical and achievable and likely to be adopted and used. Make sure that process owners are involved, buy into the new approach and own the resulting processes. Resolve issues and manage risk as encountered during the implementation.
Internal audit	Review and provide input during implementation to avoid identification of missing enablers and especially key controls after the fact. Provide guidance on implementation of control aspects. If required, provide a project/implementation risk review service, monitoring risk that could jeopardise implementation and providing independent feedback to the programme and project teams.
Risk, compliance and legal	Provide guidance as required on risk, compliance and legal aspects during implementation.

Figure 33—Phase 5 Description

Phase 5	How Do We Get There?
Phase objective	Implement the detailed improvement projects, leveraging enterprise programme and project management capabilities, standards and practices. Monitor, measure and report on project progress.
Phase description	The approved improvement projects, including required change activities, are now ready for implementation, so the solutions as defined by the programme can now be acquired or developed and implemented into the enterprise. In this way, projects become part of the normal development life cycle and should be governed by established programme and project management methods. The roll-out of the solution should be in line with the established project definitions and change plan such that the improvements are sustainable. This phase will typically involve the most effort and longest elapsed time of all the life cycle phases. It is recommended, however, that the size and overall time taken not be excessive to ensure that it is manageable and that benefits are delivered in a reasonable time frame. This is especially true for the first few iterations when it will also be a learning experience for all involved. Monitor performance of each project to ensure that goals are being achieved. Report back to stakeholders at regular intervals to ensure that progress is understood and on track.
Continual improvement (CI) tasks	Implement improvements: 1. Develop and, where necessary, acquire solutions that include the full scope of activities required, e.g., culture, ethics, and behaviour; organisational structures; principles and policies; processes; service capabilities; skills and competencies; and information. 2. When using best practices, adopt and adapt available guidance to suit the enterprise's approach to policies and procedures. 3. Test the practicality and suitability of the solutions in the real working environment. 4. Roll out the solutions, taking into account any existing processes and migration requirements.
Change enablement (CE) tasks	Enable operation and use: 1. Build on the momentum and credibility that can be created by quick wins, then introduce more widespread and challenging change aspects. 2. Communicate quick-win successes and recognise and reward those involved in them. 3. Implement the change response plans. 4. Ensure that the broader base of role players has the skills, resources and knowledge, as well as buy-in and commitment to the change. 5. Balance group and individual interventions to ensure that a holistic view of the change is obtained by key stakeholders. 6. Plan cultural and behavioural aspects of the broader transition (dealing with fears of loss of responsibility/independence/decision authority, new expectations and unknown tasks). 7. Communicate roles and responsibilities for use. 8. Define measures of success, including those from a business viewpoint and perception measures. 9. Set in place mentoring and coaching to ensure uptake and buy-in. 10. Close the loop and ensure that all change requirements have been addressed. 11. Monitor the change enablement effectiveness and take corrective action where necessary.
Programme management (PM) tasks	Execute plan: 1. Ensure that the execution of the programme is based on an up-to-date and integrated (business and IT) plan of the projects within the programme. 2. Direct and monitor the contribution of all the projects in the programme to ensure delivery of the expected outcomes. 3. Provide regular update reports to stakeholders to ensure that progress is understood and on track. 4. Document and monitor significant programme risk and issues, and agree on remediation actions. 5. Approve the initiation of each major programme phase and communicate it to all stakeholders. 6. Approve any major changes to the programme and project plans.
Input	• Improvement project definitions • Defined change response plans • Identified quick wins • Record of unapproved projects • Programme plan with allocated resources, priorities and deliverables • Project plans and reporting procedures • Success metrics • Project definitions, project Gantt chart, change response plans, change strategy • Integrated programme and project plans
ISACA resources	• *COBIT 5: Enabling Processes* (as best practice input and BAI01), *www.isaca.org/cobit* • ISACA supporting products as currently defined at *www.isaca.org*
Output	• Implemented improvements • Implemented change response plans • Realised quick wins and visibility of change success • Success communications • Defined and communicated roles and responsibilities in the business-as-usual environment • Project change logs and issue/risk logs • Defined business and perception success measures • Benefits tracked to monitor realisation

Figure 34—Phase 5 RACI Chart

	Responsibilities of Implementation Role Players								
Key Activities	Board	IT Executive Committee	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Programme Steering
Develop and, if required, acquire solutions (CI1).		A	C	C	R	R	C	C	R
Adopt and adapt best practices (CI2).		I	R	C	R	R	C	C	A
Test and roll out solutions (CI3 and CI4).		I	R	C	R	R	C	C	A
Capitalise on quick wins (CE1 and CE2).		I	C	C/I	R	R	C/I	C/I	A
Implement change response plans (CE3).	I	I	R	C	R	R	I	I	A
Direct and monitor projects within the programme (PM2).	I	A	C	C	R	C	I	I	R

Phase 6—Did We Get There?

Figures 35, 36, 37 and **38** describe phase 6.

Figure 35—Continual Improvement Life Cycle Phase 6

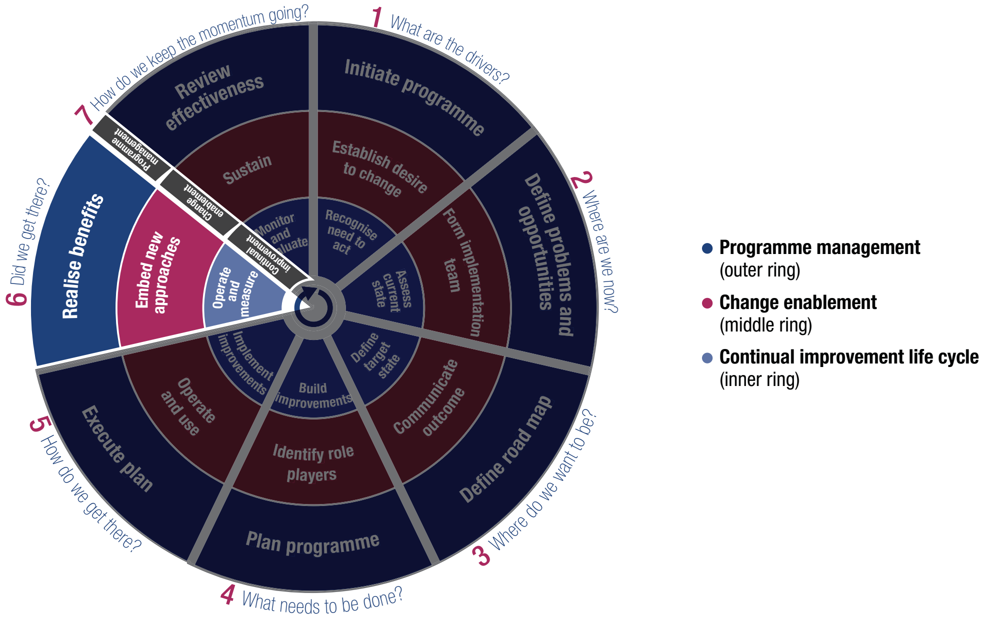


Figure 36—Roles in Phase 6

When you are...	Your role in this phase is to...
Board and executive	Assess performance in meeting the original objectives and confirm realisation of desired outcomes. Consider the need to redirect future activities and take corrective action. Assist in the resolution of significant issues, if required.
Business management	Provide feedback and consider the effectiveness of the business's contribution to the initiative. Use positive results to improve current business-related activities. Use lessons learned to adapt and improve the business's approach to future initiatives.
IT management	Provide feedback and consider the effectiveness of IT's contribution to the initiative. Use positive results to improve current IT-related activities. Monitor projects based on project criticality as they are developing, using both programme management and project management techniques, and be prepared to change the plan and/or cancel one or more projects or take other corrective action if early indications are that a project is off track and may not meet critical milestones. Use lessons learned to adapt and improve IT's approach to future initiatives.
Internal audit	Provide independent assessment of the overall efficiency and effectiveness of the initiative. Provide feedback and consider the effectiveness of audit's contribution to the initiative. Use positive results to improve current audit-related activities. Use lessons learned to adapt and improve audit's approach to future initiatives.
Risk, compliance and legal	Assess whether the initiative has improved the ability of the enterprise to identify and manage risk and legal, regulatory and contractual requirements. Provide feedback and make any necessary recommendations for improvements.

Figure 37—Phase 6 Description

Phase 6	Did We Get There?
Phase objective	Integrate the metrics for project performance and benefits realisation of the overall governance improvement programme into the performance measurement system for regular and ongoing monitoring.
Phase description	It is essential that the improvements described in the programme be monitored via IT-related goals and process goals using suitable techniques such as an IT balanced scorecard (BSC) and benefits register to verify that the change outcomes have been achieved. This will ensure that the initiatives remain on track according to original enterprise and IT-related goals and continue to deliver the desired business benefits. For each metric, targets need to be set, compared regularly against reality and communicated using a performance report. To ensure success, it is crucial that positive and negative results from the performance measurements be reported to all stakeholders, which will build confidence and enable any corrective actions to be taken on time. Projects should be monitored as they are developing, using both programme management and project management techniques, and preparation should be made to change the plan and/or cancel the project if early indications are that a project is off track and may not meet critical milestones.
Continual improvement (CI) tasks	Operate and measure: 1. Set targets for each metric for an agreed-on time period. The targets should enable IT performance and improvement actions to be monitored and success or potential failure determined. 2. Where possible, obtain current actual measures for these metrics. 3. Gather actual measures and compare them to targets on a regular, e.g., monthly, basis and investigate any significant variances. 4. Where variances indicate that corrective actions are required, develop and agree on proposed corrective measures. 5. Adjust long-term targets based on experience, if required. 6. Communicate both positive and negative results from performance monitoring to all interested stakeholders, with recommendations for any corrective measures.
Change enablement (CE) tasks	Embed new approaches: 1. Ensure that new ways of working become part of the enterprise's culture (the way we do things around here), i.e., rooted in the enterprise's norms and values. This is important for concrete results to be achieved. 2. In transitioning from project mode to business as usual, behaviours need to be shaped by revised job descriptions, remuneration and reward systems, KPIs, and operating procedures as implemented through the change response plans. 3. Monitor whether assigned roles and responsibilities have been assumed. 4. Track the change and assess the effectiveness of the change response plans, linking the results back to the original change objectives and goals. This should include both hard business measures and perception measures, e.g., perception surveys, feedback sessions, training evaluation forms. 5. Leverage pockets of excellence to provide a source of inspiration. 6. Maintain the communication strategy to achieve ongoing awareness and highlight successes. 7. Ensure that there is open communication amongst all role players to resolve issues. 8. Where issues cannot be resolved, escalate to sponsors. 9. Where still required, enforce the change through management authority. 10. Document change enablement lessons learned for future implementation initiatives.
Programme management (PM) tasks	Realise benefits: 1. Monitor the overall performance of the programme against the business case objectives. 2. Monitor the investment performance (cost against budget and realisation of benefits). 3. Document lessons learned (both positives and negatives) for subsequent improvement initiatives.
Input	• Implemented improvements • Implemented change response plans • Realised quick wins and success communications • Defined and communicated roles and responsibilities in the business-as-usual environment • Project change logs and issue/risk logs • Defined business and perception success measures • IT goals and IT process goals identified as a result of requirements analysis • Existing measures and/or scorecards • Business case benefits • Change response plans and communication strategy
ISACA resources	• *COBIT 5: Enabling Processes* (as best practice input and EDM05, APO05, BAI01, MEA01), *www.isaca.org/cobit* • ISACA supporting products as currently defined at *www.isaca.org*
Output	• Updated project and programme scorecards • Change effectiveness measures (both business and perception measures) • Report explaining scorecard results • Improvements entrenched in operations • Key metrics added into ongoing IT performance measurement approach

Figure 38—Phase 6 RACI Chart

	Responsibilities of Implementation Role Players								
Key Activities	**Board**	**IT Executive Committee**	**CIO**	**Business Executive**	**IT Managers**	**IT Process Owners**	**IT Audit**	**Risk and Compliance**	**Programme Steering**
Operate the solutions and gain performance feedback (CI1 to CI3).		I	A	R	R	R	I	I	I
Monitor performance against success metrics (CI4 to CI5).		I	A	C	R	R	C	C	I
Communicate positive and negative results (CI6).	I	I	A	C	R	C	I	I	I
Monitor ownership of roles and responsibilities (CE3).		A	R	C	C	C	C	C	I
Monitor programme results (achievement of goals and realisation of benefits) (PM1 and PM2).	I	A	C	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Phase 7—How Do We Keep the Momentum Going?

Figures 39, 40, 41 and **42** describe phase 7.

Figure 39—Continual Improvement Life Cycle Phase 7

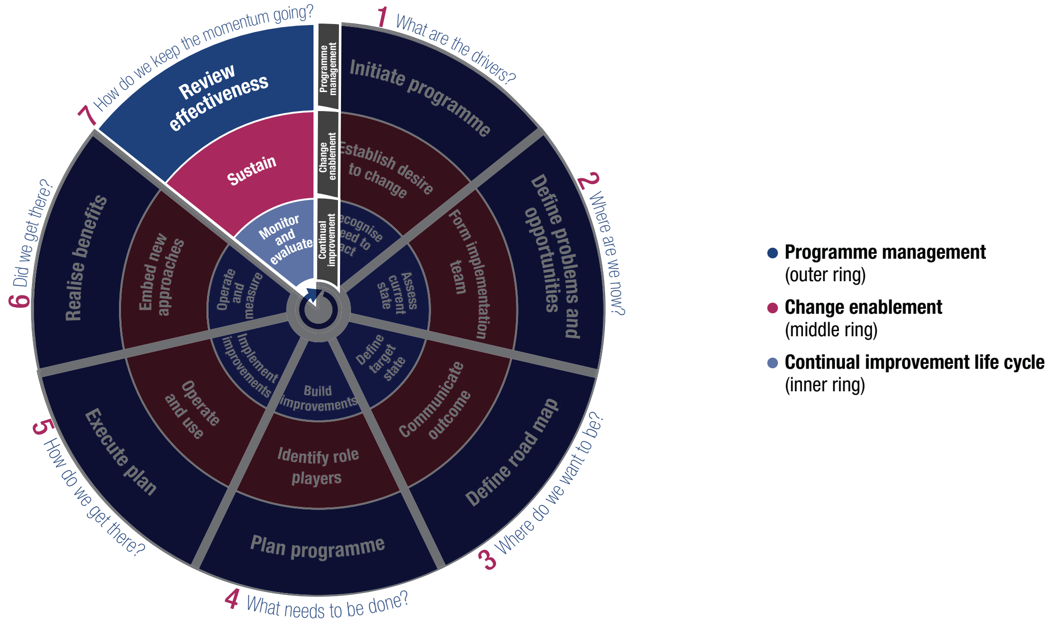


Figure 40—Roles in Phase 7

When you are...	Your role in this phase is to...
Board and executive	Provide direction, set objectives, and allocate roles and responsibilities for the enterprise's ongoing approach to, and improvement of, GEIT. Continue to 'set the tone at the top', develop organisational structures, and encourage a culture of good governance and accountability for IT amongst business and IT executives. Ensure that IT is aware of, and, as appropriate, involved in, new business objectives and requirements in as timely a manner as possible.
Business management	Provide support and commitment by continuing to work positively with IT to improve GEIT and make it business as usual. Verify that new GEIT objectives are aligned with current enterprise objectives.
IT management	Drive and provide strong leadership to sustain the momentum of the improvement programme. Engage in governance activities as part of normal business practice. Create policies, standards and processes to ensure that governance becomes business as usual.
Internal audit	Provide objective and constructive input, encourage self-assessment, and provide assurance to management that governance is working effectively, thus building confidence in IT. Provide ongoing audits based on an integrated governance approach using criteria shared with IT and the business based on the COBIT framework.
Risk, compliance and legal	Work with IT and the business to anticipate legal and regulatory requirements, and identify and respond to IT-related risk as a normal activity in GEIT.

Figure 41—Phase 7 Description

Phase 7	How Do We Keep the Momentum Going?
Phase objective	Assess the results and experience gained from the programme. Record and share any lessons learned. Improve organisational structures, processes, roles and responsibilities to change the enterprise's behaviour so that GEIT becomes business as usual and is continually optimised. Ensure that new required actions drive further iterations of the life cycle. Continually monitor performance, ensure that results are regularly reported, and drive commitment and ownership of all accountabilities and responsibilities.
Phase description	This phase enables the team to determine whether the programme delivered against expectations. This can be done by comparing the results to the original success criteria and gathering feedback from the implementation team and stakeholders via interviews, workshops and satisfaction surveys. The lessons learned can contain valuable information for team members and project stakeholders for use in ongoing initiatives and improvement projects. It involves continual monitoring, regular and transparent reporting, and confirmation of accountabilities. Further improvements are identified and used as input to the next iteration of the life cycle. In this phase, the enterprise should build on the successes and lessons learned from the governance implementation project(s) to build and reinforce commitment amongst all IT and business stakeholders for continually improved governance of IT. Policies, organisational structures, roles and responsibilities, and governance processes should be developed and optimised so that GEIT operates effectively as part of normal business practice, and there is a culture supporting this, demonstrated by top management.
Continual improvement (CI) tasks	Monitor and evaluate: 1. Identify new governance objectives and requirements based on experiences gained, current business objectives for IT or other trigger events: a. Gather feedback and perform a stakeholder satisfaction survey. b. Measure and report actual results against originally established project measures of success, and embed continual monitoring and reporting. c. Perform a facilitated project review process with project team members and project stakeholders to record and pass on lessons learned. d. Look for further high-impact, low-cost opportunities to improve GEIT further. 2. Identify lessons learned. 3. Communicate requirements for further improvements to the stakeholders and document for use as input to the next iteration of the life cycle.
Change enablement (CE) tasks	Sustain: 1. Provide conscious reinforcement and an ongoing communication campaign, as well as demonstrated continual top management commitment. 2. Confirm conformance to objectives and requirements. 3. Continually monitor the effectiveness of the change itself, change enablement activities and buy-in of stakeholders. 4. Implement corrective action plans where required. 5. Provide feedback on performance, reward achievers and publicise successes. 6. Build on lessons learned. 7. Share knowledge from the initiative to the broader enterprise.
Programme management (PM) tasks	Review programme effectiveness: 1. At programme closure, ensure that a programme review takes place and approve conclusions. 2. Review programme effectiveness.
Input	• Updated project and programme scorecards • Change effectiveness measures (both business and perception measures) • Report explaining scorecard results • Post-implementation review report • Performance reports • Business and IT strategy • New triggers such as new regulatory requirements
ISACA resources	• *COBIT 5: Enabling Processes* (EDM01, APO01, BAI08, MEA01), *www.isaca.org/cobit* • ISACA supporting products as currently defined at *www.isaca.org*
Output	• Recommendations for further GEIT activities • Stakeholder satisfaction survey • Documented success stories and lessons learned • Ongoing communication plan • Performance reward scheme

Figure 42—Phase 7 RACI Chart

	Responsibilities of Implementation Role Players								
Key Activities	**Board**	**IT Executive Committee**	**CIO**	**Business Executive**	**IT Managers**	**IT Process Owners**	**IT Audit**	**Risk and Compliance**	**Programme Steering**
Identify new governance objectives (CI1).	C	A	R	R	C	C	C	C	I
Identify lessons learned (CI2).		I	A	C	R	R	C	C	I
Sustain and reinforce changes (CE1).		A	R	R	R	R	C	C	I
Confirm conformance to objectives and requirements (CE2).	I	A	R	C	R	R	R	I	R
Close programme with formal review of effectiveness (PM1).	I	A	C	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

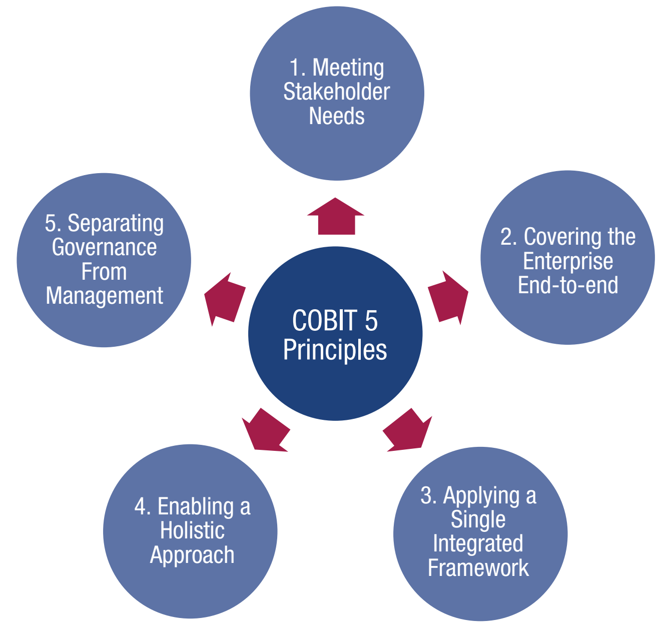
Page intentionally left blank

Chapter 7
Using the COBIT 5 Components

Transition Considerations for COBIT 4.1, Val IT and Risk IT Users

COBIT 4.1, Val IT and Risk IT users who are already engaged in GEIT implementation activities can transition to use COBIT 5 and benefit from the latest and improved guidance that it provides during the next iterations of their enterprise's improvement life cycle. COBIT 5 builds on previous versions of COBIT, Val IT and Risk IT so enterprises can also build on what they have developed using earlier versions. Implementations will always be tailored to suit a specific enterprise's environment and needs while adopting the latest COBIT and other guidance as appropriate. These materials will continue to evolve over time as conditions change and practices improve. COBIT 5 principles are shown in **figure 43**.

Figure 43—COBIT 5 Principles


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

The following summarises the major changes in COBIT 5 and how they may impact implementation.

New GEIT principles:

- **Increased focus on enablers**—COBIT 5 introduces an increased focus on the enablers required for effective GEIT in addition to the familiar process enabler models. These additional enablers are also referenced in various COBIT 5 processes as described in chapter 2.
- **New Process Reference Model**—COBIT 5 is based on a revised process 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. COBIT 5 consolidates COBIT 4.1, Val IT and Risk IT into one framework, and has been updated to align with current best practices. The new model can be used as a guide for adjusting, as necessary, the enterprise's own process model.
- **New and modified processes:**
  - COBIT 5 introduces five new governance processes that have leveraged and improved COBIT 4.1, Val IT and Risk IT governance approaches and will help to further refine and strengthen executive-management-level GEIT practices integrated with existing enterprise governance practices and aligned with ISO/IEC 38500.
  - COBIT 5 has clarified management-level processes and integrated COBIT 4.1, Val IT and Risk IT content into one model. *COBIT 5: Enabling Processes* provides a full cross-reference in appendix A. There are several new and modified processes that reflect current thinking, in particular:
    - APO03 Manage enterprise architecture.
    - APO04 Manage innovation.
    - APO05 Manage portfolio.
    - APO06 Manage budget and costs.
    - APO08 Manage relationships.
    - APO13 Manage security.
    - BAI05 Manage organisational change enablement.

    - BAI08 Manage knowledge.
    - BAI09 Manage assets.
    - DSS05 Manage security service.
    - DSS06 Manage business process controls.
  - COBIT 5 processes now cover end-to-end business and IT activities, i.e., a full enterprise-level view. This provides for a more holistic and complete coverage of practices reflecting the pervasive enterprisewide nature of IT use. It makes the involvement, responsibilities and accountabilities of business stakeholders explicit and transparent.
- **Practices and activities:**
  - The COBIT 5 governance or management practices are equivalent to the COBIT 4.1 control objectives and Val IT and Risk IT processes.
  - The COBIT 5 activities are equivalent to the COBIT 4.1 control practices and Val IT and Risk IT management practices.
  - COBIT 5 integrates and updates all of the previous content into the one new model, with a consistent level of detail, with all the guidance provided in *COBIT 5: Enabling Processes*, making it easier for users to understand and use this material when implementing improvements.
- **Goals and metrics:**
  - COBIT 5 follows the same goals and metrics concepts as COBIT 4.1, Val IT and Risk IT, but these are renamed enterprise goals, IT-related goals and process goals, reflecting an enterprise-level view.
  - COBIT 5 provides a revised goals cascade now based on enterprise goals driving IT-related goals and then supported by critical processes. This is similar to the COBIT 4.1 goals cascade with an updated set of goals and relationships and more detailed primary and secondary relationships. This cascade continues to be a key tool for establishing strategic alignment and scoping of important processes.
  - COBIT 5 provides examples of goals and metrics at the enterprise, process and management practice levels. This is different from COBIT 4.1, Val IT and Risk IT, which covered one level lower.
- **Inputs and outputs:**
  - COBIT 5 provides inputs and outputs for every management practice, whereas COBIT 4.1 provided these only at the process level. This provides additional detailed guidance for designing processes to include essential work products and to assist with inter-process integration.
- **RACI charts:**
  - COBIT 5 provides RACI charts describing roles and responsibilities in a similar way to COBIT 4.1, Val IT and Risk IT.
  - COBIT 5 provides a more complete, detailed and clearer range of generic business and IT role players and charts than COBIT 4.1 for each management practice, enabling better definition of role player responsibilities or level of involvement when designing and implementing processes.
- **Process capability maturity models and assessments** (refer also to phases 2 and 3 in the implementation life cycle discussion):
  - COBIT 5 discontinues the COBIT 4.1, Val IT and Risk IT capability maturity model (CMM)-based capability maturity modelling approach, and now supports a new capability assessment scheme based on ISO/IEC 15504. Guidance on how to perform a capability self-assessment will be provided in the planned COBIT 5 self-assessment guide.

The following summarises how to perform a gap analysis based on the standard:

- Identify and prioritise improvement areas (as outlined in phase 3) by considering:
  - Identified strengths, weaknesses and risk
  - Enterprise goals
  - Opportunities for improving customer satisfaction
  - COBIT 5 guidance and other related standards and best practice
  - Benchmarks that provide a basic comparison framework for assessment results
  - Existing process performance goals and metrics that may indicate root causes of the drivers for improvement
  - Risk of not achieving the stated improvement objectives
- Analyse assessment strengths and weaknesses:
  - Strengths are identified as the processes with the highest process capability level ratings. Consider the:
    - Experience of good practices that could be adopted and institutionalised
    - Opportunity for improving the effectiveness of interrelated processes
  - Weaknesses are identified and derived from:
    - Low process attribute ratings
    - Processes with missing practices (consider the COBIT 5 management practices and activities and other enablers as well as related standards and best practices) needed to achieve a process purpose
    - Unbalanced process attribute ratings within capability levels that are necessary to achieve a specific enterprise goal
  - Low process attribute ratings across a group of assessed processes may indicate weakness in specific process categories (for example, low scores at process capability level 2 may show weaknesses in the Management and Support process categories).
  - Similarly, the process attribute ratings of related processes should be compared. Improvement actions may be needed to correct any imbalance.

The COBIT 4.1, Val IT and Risk IT CMM-based approaches are not considered compatible with the COBIT 5 ISO/IEC 15504 approach because the methods use different attributes and measurement scales. The COBIT 5 approach is considered by ISACA to be more robust, reliable and repeatable and will also support a formal assessment by accredited assessors, enabling an enterprise to obtain an independent and certified assessment aligned to the ISO/IEC standard. COBIT 5 chapter 8 provides a full description of the new COBIT 5 process capability model and how it compares with the previous approach used in COBIT 4.1,Val IT and Risk IT.

COBIT 4.1, Val IT and Risk IT users wishing to move to the new COBIT 5 approach will need to realign their previous ratings, adopt and learn the new method, and initiate a new set of assessments to gain the benefits of the new approach. Although some of the information gathered from previous assessments may be reusable, care will be needed in migrating this information forward because there are significant differences in requirements.

COBIT 4.1, Val IT and Risk IT users wishing to continue with the CMM-based approach, either as an interim or ongoing approach, can use the COBIT 5 guidance, but must use the COBIT 4.1 generic attribute table without the high-level maturity models. The procedure in outline form is as follows:

1. Compare the scope of the process with the COBIT 5 governance or management practices and activities to identify any gaps (assuming management has accepted and agreed to the full scope of COBIT 5 guidance). To satisfy level 3 (defined) and above, all of the practices should have been addressed.
2. Compare the detail of the process to the COBIT 4.1 maturity attribute table (appendix E) and assess the level attained for each attribute. In addition, when assessing each attribute consider how well the following COBIT 5 process guidance is being generally applied:
   - Awareness and communication—EDM01.02 and APO01.04
   - Policies, plans and procedures—EDM01.02, APO01.03 and APO01.08
   - Tools and automation—APO03.02
   - Skills and expertise—APO07.03
   - Responsibility and accountability—Process RACI chart and EDM01.02 and APO01.02
   - Goal setting and measurement—APO07.04 and MEA01
3. Compare to any available benchmarks and models that may exist to check on the reasonableness of the assessment.
4. Set the overall maturity level to the lowest attribute level (unless an attribute is not considered materially significant to the process capability) while also considering the coverage of governance or management practices. Use whole number ratings rather than ‘in-between’ or percentages. Attainment of a level is reached only if everything is satisfied. Management needs a transparent and realistic view if it is to sponsor improvements.
5. Analyse the gap between current and target levels by considering the current process strengths and weaknesses compared to COBIT 5 governance or management practice and activity guidance, the COBIT 5 enablers, and other relevant standards and best practices.

Planning and Scoping

COBIT 5 and supporting material in this guide provide an effective way to understand business and governance priorities and requirements, and this knowledge can be used when implementing improved governance and management enablers. This approach also enhances the preparation of business cases for governance improvements, obtaining the support of stakeholders, and the realisation and monitoring of the expected benefits.

The relationship can be summarised in this top-down flow. COBIT 5 helps ensure strategic alignment and drives what to do, supported by the enterprise goals to IT-related goals to IT processes cascade provided and explained further as follows:

- Enterprise goals
  - IT-related goals
    - Governance and management requirements
      - Critical IT processes
        - Prioritised governance or management practices and activities

Having a clear appreciation of current stakeholder needs relating to GEIT (as described in chapter 3, **figures 6** and **7** and referred to in COBIT 5) and current enterprise goals and how they impact GEIT is very helpful for three reasons:

- The stakeholder needs and enterprise objectives influence the requirements and priorities of GEIT. For example, there could be a focus on cost reduction, compliance or launching a new business product, each of which could put a different emphasis on current governance priorities.
- The stakeholder needs and enterprise objectives help to focus where attention should be given when improving GEIT.
- It assists the business and IT functions to do better forward planning of opportunities to add value to the enterprise.

COBIT 5 provides useful guidance and examples for defining enterprise and IT-related objectives and how they relate to each other. A generic set of enterprise goals and IT-related goals is presented as a cascade in COBIT 5 and *COBIT 5: Enabling Processes*. These examples enable COBIT users to relate their enterprise's current business and IT environment to specific objectives, and then map them to the processes that are likely to be relevant in successfully achieving these goals.

Performance Measurement

An important principle of good governance is that management should provide direction using clearly defined and communicated objectives, and then manage adherence to objectives by applying appropriate practices. Monitoring of performance using metrics enables management to ensure that goals are achieved.

The COBIT 5 enterprise and IT-related goals are used as the basis for setting IT objectives and for establishing a performance measurement framework. IT objectives are expressed as goals and need to be aligned with enterprise goals. COBIT 5 provides structures for defining goals at three levels: for the enterprise, IT overall and IT processes. These goals are supported by metrics known as outcome measures because they measure the outcome of a desired goal. The metrics at a specific level also act as performance drivers for achieving higher-level goals. These goals and metrics can be used to set objectives and monitor performance by establishing scorecards and performance reports as well as for driving improvements.

COBIT 5 provides guidance on how to define and break down business objectives and create monitoring metrics based on the BSC.

Governance and Management Practices and Activities

COBIT 5 clarifies the distinction between governance and management practices with the addition of a new governance domain. The COBIT 5 framework provides explanations on the differences between governance and management of enterprise IT. The design of specific processes and procedures based on COBIT 5 should always fit the needs of the enterprise's culture, management style and IT environment. The guidance in COBIT 5 must be tailored appropriately. It is suggested to adopt the best practices that are recommended, but to adapt them so that they will be practical and appropriate to each specific enterprise's objectives and needs. The activities provide guidance on what must be implemented to achieve a specific management practice.

The COBIT 5 practices and activities are based on current relevant standards and best practices that should also be utilised to obtain more detailed guidance.

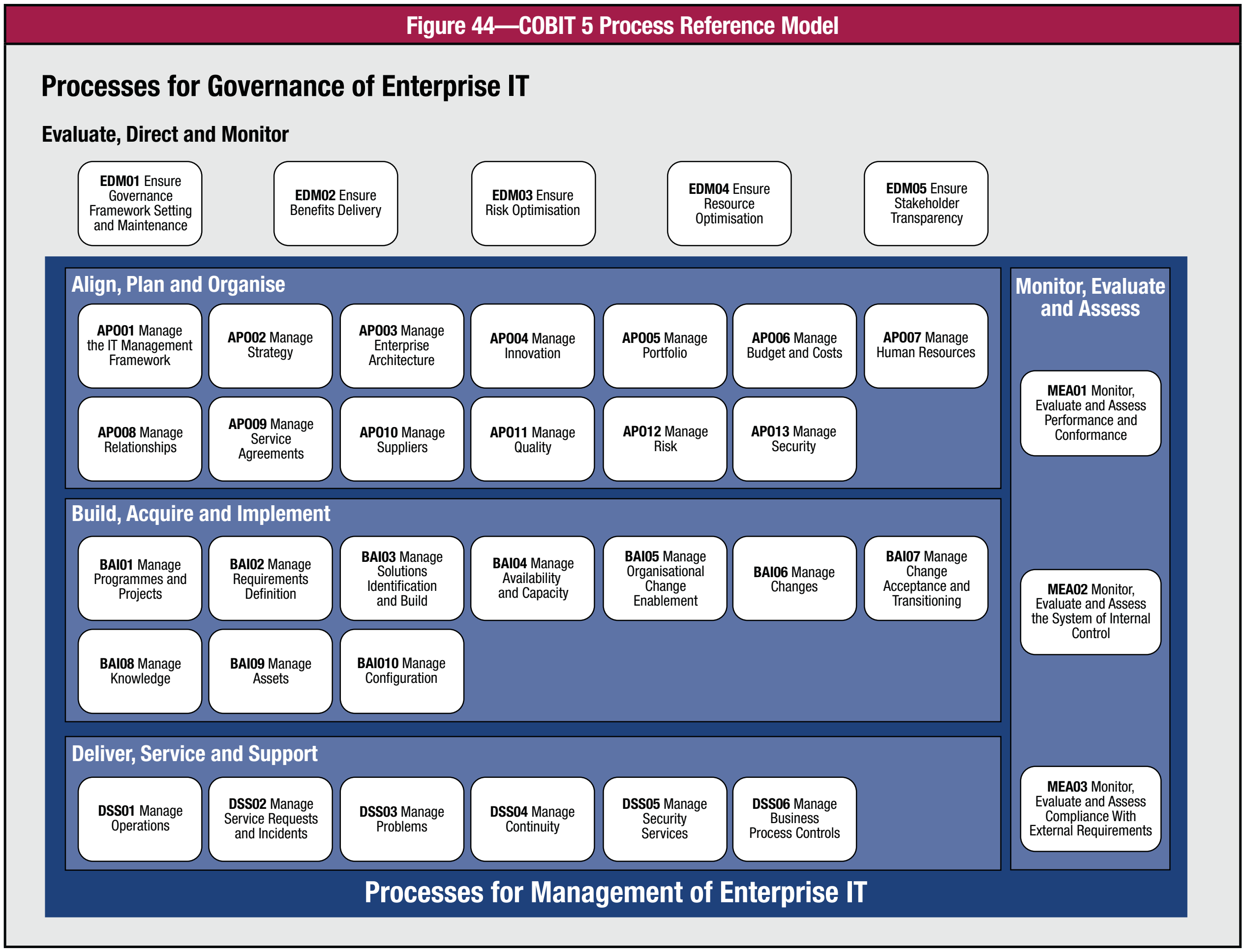
Roles and Responsibilities

For each process, COBIT 5 provides example RACI charts that indicate who is responsible or accountable, and who needs to be consulted or informed of process activities for a range of typical role players (end to end, business and IT). The role players could be individuals (such as the CFO or chief operating officer [COO]) or structures (such as the board or enterprise risk committee). Defining responsibility and accountability is an important principle of GEIT. These charts can be used as a basis for tailoring specific RACI charts for IT processes.

Appendix A
Mapping Pain Points to COBIT 5 Processes

Figure 44 shows the complete set of 37 governance and management processes within COBIT 5. The details of all processes, according to the process model described previously, are included in *COBIT 5: Enabling Processes.*

Figure 44—COBIT 5 Process Reference Model



Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- **EDM01** Ensure Governance Framework Setting and Maintenance
- **EDM02** Ensure Benefits Delivery
- **EDM03** Ensure Risk Optimisation
- **EDM04** Ensure Resource Optimisation
- **EDM05** Ensure Stakeholder Transparency

Align, Plan and Organise

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

Build, Acquire and Implement

- **BAI01** Manage Programmes and Projects
- **BAI02** Manage Requirements Definition
- **BAI03** Manage Solutions Identification and Build
- **BAI04** Manage Availability and Capacity
- **BAI05** Manage Organisational Change Enablement
- **BAI06** Manage Changes
- **BAI07** Manage Change Acceptance and Transitioning
- **BAI08** Manage Knowledge
- **BAI09** Manage Assets
- **BAI010** Manage Configuration

Deliver, Service and Support

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

Monitor, Evaluate and Assess

- **MEA01** Monitor, Evaluate and Assess Performance and Conformance
- **MEA02** Monitor, Evaluate and Assess the System of Internal Control
- **MEA03** Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

Figure 45 provides examples of pain points (as discussed in chapter 3) and examples of COBIT 5 processes that could be selected for guidance corresponding to these pain points.

Figure 45—Pain Points Mapped to COBIT 5 Processes

Pain Point	COBIT 5 Processes
Business frustration with failed initiatives, rising IT costs and a perception of low business value	EDM02, APO01, APO02, APO05, APO07, BAI01, BAI02
Significant incidents related to IT-related business risk such as data loss or project failure	EDM03, APO09, APO12, DSS domain
Outsourcing service delivery problems such as agreed–on service levels consistently not being met	EDM04, APO09, APO10
Failure to meet regulatory or contractual requirements	EDM03, MEA03
IT limiting the enterprise's innovation capabilities and business agility	EDM04, APO02, APO04
Regular audit findings about poor IT performance or reported IT quality-of-service problems	MEA02
Hidden and rogue IT spending	EDM02, APO05, APO06
Duplication or overlap between initiatives, or resource wastage	EDM02, EDM04, APO05, BAI01
Insufficient IT resources, staff with inadequate skills or staff burn-out/dissatisfaction	EDM04, APO07
IT-enabled changes frequently failing to meet business needs and delivered late or over budget	APO02, APO05, BAI01
Multiple and complex IT assurance efforts	MEA02
Board members or senior managers who are reluctant to engage with IT, or a lack of committed and satisfied business sponsors for IT	EDM01, EDM02, APO01, APO02
Complex IT operating models	EDM01, APO01, APO02, MEA01

Appendix B
Example Decision Matrix

Figure 46 is an example of how to identify key topic areas requiring clear decision-making roles and responsibilities. It is provided as a guide and, if found useful, could be modified and adapted to suit an enterprise's specific organisation and requirements.[8]

Figure 46—Example Decision Matrix

Decision Topic	Scope	Responsible, Accountable, Consulted, Informed (RACI)							
		Executive Committee	IT Strategy Committee	Security Committee	Programme Steering Committee	Project Steering Committee	IT Management	Business Management	Employees
Governance	• Aligning with enterprise governance • Establishing principles, structures, objectives	A/R	R	C			C	R	I
Business strategy	• Defining enterprise goals and objectives • Deciding where and how IT can enable and support business objectives	A/R	R	C			C	R	I
IT policies	• Providing accurate, understandable and approved policies, procedures, guidelines and other documentation to stakeholders • Developing and rolling out IT policies • Enforcing IT policies	I	A	C			R	C	C
IT strategy	• Incorporating IT and business management in the translation of business requirements into service offerings, and developing strategies to deliver these services in a transparent and effective manner • Engaging with business and senior management in aligning IT strategic planning with current and future business needs • Understanding current IT capabilities • Providing for a prioritisation scheme for the business objectives that quantifies the business requirements	I	A	C	I		R	C	C
IT technology direction	• Providing appropriate platforms for the business applications in line with the defined IT architecture and technology standards • Producing a technology acquisition plan that aligns to the technology infrastructure plan • Planning infrastructure maintenance	I	C	C			A/R	C	C
IT methods and frameworks	• Establishing transparent, flexible and responsive IT organisational structures and defining and implementing IT processes that integrate owners, roles and responsibilities into business and decision processes • Defining an IT process framework • Establishing appropriate organisational bodies and structure • Defining roles and responsibilities	I	C	C	I	I	A/R	I	I
Enterprise architecture	• Defining and implementing, architecture and standards that recognise and leverage technology opportunities • Establishing a forum to guide architecture and verify compliance • Establishing the architecture plan balanced against cost, risk and requirements • Defining the information architecture, including the establishment of an enterprise data model that incorporates a data classification scheme • Ensuring the accuracy of the information architecture and data model • Assigning data ownership • Classifying information using an agreed-on classification scheme	A	C	C	I	I	R	R	C

[8] This example is based on the GEIT matrix used internally by Deloitte South Africa and developed by IT Winners, used with their permission.

Figure 46—Example Decision Matrix *(cont.)*

		Responsible, Accountable, Consulted, Informed (RACI)							
Decision Topic	**Scope**	**Executive Committee**	**IT Strategy Committee**	**Security Committee**	**Programme Steering Committee**	**Project Steering Committee**	**IT Management**	**Business Management**	**Employees**
IT-enabled investment and portfolio prioritisation	• Making effective and efficient IT-enabled investment and portfolio decisions • Forecasting and allocating budgets • Defining formal investment criteria • Measuring and assessing business value against forecast	I	A		C	C	R		
IT-enabled investment and programme prioritisation	• Setting and tracking IT budgets in line with IT strategy and investment decisions • Measuring and assessing business value against forecast • Defining a programme and project management approach that is applied to IT projects and enables stakeholder participation in and monitoring of project risk and progress • Defining and enforcing programme and project frameworks and approach • Issuing project management guidelines • Performing project planning for each project detailed in the project portfolio	I	A		R	C	C/I	C/I	C/I
Managing, monitoring and evaluating SLAs	• Identifying service requirements, agreeing on service levels and monitoring the achievement of service levels • Formalising internal and external agreements in line with requirements and delivery capabilities • Reporting on service level achievements (reports and meetings) • Identifying and communicating new and updated service requirements to strategic planning • Meeting operational service levels for scheduled data processing, protecting sensitive output, and monitoring and maintaining infrastructure	I	A	R			R	R	I
IT application management	• Identifying technically feasible and cost-effective solutions • Defining business and technical requirements • Undertaking feasibility studies as defined in the development standards • Approving (or rejecting) requirements and feasibility study results • Ensuring that there is a timely and cost-effective development process • Translating business requirements into design specifications • Adhering to development standards for all modifications • Separating development, testing and operational activities	I	I	C			A/R	C	C
IT infrastructure management	• Operating the IT environment in line with agreed-on service levels and defined instructions • Maintaining the IT infrastructure	I	I	C			A/R	C	C
IT security	• Defining IT security policies, plans and procedures, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents • Understanding security requirements, vulnerabilities and threats in line with business requirements and impact • Managing user identities and authorisations in a standardised manner • Testing security regularly	I	A	R			R	R	C/I

Figure 46—Example Decision Matrix *(cont.)*

		Responsible, Accountable, Consulted, Informed (RACI)							
Decision Topic	**Scope**	**Executive Committee**	**IT Strategy Committee**	**Security Committee**	**Programme Steering Committee**	**Project Steering Committee**	**IT Management**	**Business Management**	**Employees**
Procurement and contracts	• Acquiring and maintaining IT resources that respond to the delivery strategy, establishing an integrated and standardised IT infrastructure, and reducing IT procurement risk • Obtaining professional legal and contractual advice • Defining procurement procedures and standards • Procuring requested hardware, software and services in line with defined procedures	I	I	C			A/R	C	C
IT compliance	• Identifying all applicable laws, regulations and contracts and the corresponding level of IT compliance, and optimising IT processes to reduce the risk of non-compliance • Identifying legal, regulatory and contractual requirements related to IT • Assessing the impact of compliance requirements • Monitoring and reporting on compliance with these requirements	C/I	A	C			A/R	C	C/I

Page intentionally left blank

Appendix C
Mapping Example Risk Scenarios to COBIT 5 Processes

Figure 47—Risk Scenarios and COBIT 5 Process Capabilities

Risk Scenario		**COBIT 5 Process Capabilities**
If the scenario is relevant and inherently likely…	*…given these negative examples…*	*…then consider whether these COBIT 5 processes need improvement.* Note: In this column, next to each process number is an example from the process to consider. These are not the process names.
Benefit/value enablement risk		
IT programme selection	• Incorrect programmes selected for implementation and misaligned with corporate strategy and priorities • Duplication among different initiatives • New and important programme creates long-term incompatibility with the enterprise architecture	• APO02 Aligned business and IT strategy • APO03 Compatibilities with enterprise architecture • APO04 Identification of innovation opportunities • APO05 Portfolio management decisions • BAI01 Programme management planning and co-ordination
New technologies	• Failure to adopt and exploit new technologies (i.e., functionality, optimisation) in a timely manner • New and important technology trends not identified • Inability to use technology to realise desired outcomes (e.g., failure to make required business model or organisational changes)	• EDM04 Resource management direction and/or oversight • APO02 Strategy identifying technology opportunities • APO03 Enterprise architecture aligned with current technology trends • APO04 New and important technology trends identified • BAI02 Ability to use new technology to define new business models • BAI03 Adoption and exploitation of new technologies
Technology selection	• Incorrect technologies (i.e., cost, performance, features, compatibility) selected for implementation	• APO02 Effective strategic technology selection • APO03 Enterprise architecture technology consistency • BAI03 Identifying and building solutions • APO13 Security impacts of technology selection
IT investment decision making	• Business managers or representatives not involved in important IT investment decision making regarding new applications, prioritisation or new technology opportunities	• EDM02 Value management direction and/or oversight • APO02 Business involvement in IT strategic planning • APO03 Investment fit with target enterprise architecture • APO05 Portfolio management decisions • APO06 Investment monitoring • APO08 Understanding of business expectations and opportunities to leverage IT • BAI01 Programme management stage-gating
Accountability over IT	• Business not assuming accountability over those IT areas it should such as functional requirements, development priorities and assessing opportunities through new technologies	• EDM01-05 Executive management accountability for IT-related decisions • APO01 Business and IT-related roles and responsibilities • APO09 Clear and approved service agreements • APO10 Defined and managed supplier agreements and relationships • BAI05 Enabling organisational changes with respect to IT accountability and GEIT
IT project termination	• Projects that are failing due to cost, delays, scope creep or changed business priorities not terminated in a timely manner	• EDM01 GEIT policies, organisation structures and roles • EDM02 Value governance monitoring • EDM04 Resource governance monitoring • BAI01 Programme/project management stage-gating • APO05 Effective portfolio management decision making • APO06 Investment monitoring • MEA01 Performance monitoring
IT project economics	• Isolated IT project budget overrun • Consistent and important IT projects budget overruns • Absence of view on portfolio and project economics	• EDM01 GEIT policies, organisation structures and roles • EDM02 Value governance monitoring • EDM04 Resource governance monitoring • APO06 Investment monitoring • BAI01 Programme/project management planning and monitoring

Figure 47—Risk Scenarios and COBIT 5 Process Capabilities *(cont.)*

Risk Scenario		COBIT 5 Process Capabilities
If the scenario is relevant and inherently likely…	*…given these negative examples…*	*…then consider whether these COBIT 5 processes need improvement.* Note: In this column, next to each process number is an example from the process to consider. These are not the process names.
Programme/project delivery risk		
Architectural agility and flexibility	• Complex and inflexible IT architecture obstructing further evolution and expansion	• APO01 Efficient and defined business and IT-related processes • EDM04 Governance over resource optimisation • APO02 Responsive strategic planning • APO03 Maintenance of enterprise architecture • APO04 Innovation and initiation of change • APO05 Portfolio management decision taking • BAI02,03 Agile development life cycle methods • APO13 Maintaining security in an agile and flexible environment
Integration of IT within business processes	• Extensive dependency and use of end-user computing and *ad hoc* solutions for important information needs • Separate and non-integrated IT solutions to support business processes	• EDM01 GEIT policies, organisation structures and roles • APO01 Business and IT-related roles and responsibilities • APO02 Alignment of business and IT strategies • APO03 Architectural designs and decisions • APO08 Business and IT relations • BAI02 Definition and understanding of business requirements • BAI03 Adaptation of business processes to new IT solutions • BAI05 Managing organisational changes with regards to IT
Software implementation	• Operational glitches when new software is made operational • Users not prepared to use and exploit new application software	• APO11 Consistent and effective quality management activities • BAI01 Project management • BAI02 Requirements definitions • BAI03 Solution development • BAI05 Managing organisational changes with regards to software implementation • BAI06 Change management • BAI07 Extensive solution testing • BAI08 Knowledge support
Project delivery	• Occasional late IT project delivery by internal development department • Routinely important delays in IT project delivery • Excessive delays in outsourced IT development project	• EDM01 GEIT policies, organisation structures and roles • EDM02 Value governance monitoring • APO06 Investment monitoring • BAI01 Programme/project management planning and monitoring
Project quality	• Insufficient quality of project deliverables due to software, documentation or compliance with functional requirements	• APO03 Architecture standards • APO11 Consistent and effective quality management activities • BAI01 Programme/project quality management planning and monitoring
Service delivery/IT operations risk		
State of infrastructure technology	• Obsolete IT technology cannot satisfy new business requirements such as networking, security and storage	• EDM04 Resource management direction and/or oversight • APO02 Recognising and strategically addressing current IT capability issues • APO03 Maintaining enterprise architecture • APO04 Identifying important technology trends • BAI03 Maintaining infrastructure • BAI04 Planning for and addressing capacity and performance issues • BAI09 Maintaining assets
Ageing of application software	• Application software that is old, poorly documented, expensive to maintain, difficult to extend or not integrated in current architecture	• EDM04 Resource management direction and/or oversight • APO02 Recognising and strategically addressing current IT capability issues • APO03 Maintaining enterprise architecture • APO04 Identifying new and important technology trends • BAI03 Maintaining applications • BAI09 Maintaining assets • DSS06 Business process controls

Figure 47—Risk Scenarios and COBIT 5 Process Capabilities *(cont.)*

Risk Scenario		**COBIT 5 Process Capabilities**
If the scenario is relevant and inherently likely…	*…given these negative examples…*	*…then consider whether these COBIT 5 processes need improvement.* Note: In this column, next to each process number is an example from the process to consider. These are not the process names.
Service delivery/IT operations risk *(cont.)*		
Regulatory compliance	• Non-compliance with regulations of accounting or manufacturing	• EDM01 GEIT compliance policies and roles • APO01 Policies and guidance on regulatory compliance • APO02 Planning for regulatory requirements • BAI02 Identifying and defining regulatory requirements • MEA03 Monitoring compliance requirements and current status
Selection/performance of third-party suppliers	• Inadequate support and services delivered by vendors, not in line with SLAs • Inadequate performance of outsourcer in large-scale, long-term outsourcing arrangement	• APO10 Effective supplier selection, management and relationships • BAI03 Effective management of procurements
Infrastructure theft	• Theft of laptop with sensitive data • Theft of a substantial number of development servers	• APO01 Policies and guidance on protection of assets • APO07 References and background checks on new hires and contractors • BAI03 Protection of critical assets during maintenance activities • DSS05 Physical security measures
Destruction of infrastructure	• Destruction of data centre due to sabotage or other causes • Accidental destruction of individual laptops	• DSS01 Environmental protection and facilities management • DSS05 Physical security measures
IT staff	• Departure or extended unavailability of key IT staff • Key development team leaving the enterprise • Inability to recruit IT staff	• APO07 Development and retention of IT staff resources • BAI08 Managing tacit knowledge
IT expertise and skills	• Lack or mismatch of IT-related skills within IT due to new technologies or other causes • Lack of business understanding by IT staff	• APO07 Definition and development of business and IT staff competency requirements • BAI08 Knowledge support
Software integrity	• Intentional modification of software leading to wrong data or fraudulent actions • Unintentional modification of software leading to unexpected results • Unintentional configuration and change management errors	• BAI02 Definition of application control requirements • BAI06 Change management • BAI07 Testing and acceptance practices • BAI10 Configuration data • DSS05 Access controls • DSS06 Business process controls
Infrastructure (hardware)	• Misconfiguration of hardware components • Damage of critical servers in the computer room due to accident or other causes • Intentional tampering with hardware such as security devices	• BAI03 Protection of critical assets during maintenance activities • BAI10 Configuration data • DSS05 Physical security measures
Software performance	• Regular software malfunctioning of critical application software • Intermittent performance problems with important system software	• BAI03 Software development quality assurance • BAI04 Planning for and addressing capacity and performance issues • DSS03 Root cause analysis and problem resolution
System capacity	• Inability of systems to handle transaction volumes when user volumes increase • Inability of systems to handle system load when new applications or initiatives are deployed	• APO03 Architecture principles for scalability and agility • BAI03 Maintaining infrastructure • BAI04 Planning for and addressing capacity and performance issues
Ageing of infrastructural software	• Use of unsupported versions of operating system software • Use of old database system	• EDM04 Resource management direction and/or oversight • APO02 Recognising and strategically addressing current IT capability issues • APO03 Maintaining enterprise architecture • APO04 Identifying new and important technology trends • BAI03 Maintaining infrastructure • DSS08 Problems relating to business process controls
Malware	• Intrusion of malware on critical operational servers • Regular infection of laptops with malware	• APO01 Policies and guidance on use of software • DSS05 Malicious software detection

Figure 47—Risk Scenarios and COBIT 5 Process Capabilities *(cont.)*

Risk Scenario		**COBIT 5 Process Capabilities**
If the scenario is relevant and inherently likely…	*…given these negative examples…*	*…then consider whether these COBIT 5 processes need improvement.* Note: In this column, next to each process number is an example from the process to consider. These are not the process names.
Service delivery/IT operations risk *(cont.)*		
Logical attacks	• Virus attack • Unauthorised users trying to break into systems • Denial-of-service attack • Web site defacing • Industrial espionage	• APO01 Policies and guidance on protection and use of IT assets • BAI03 Security requirements in solutions • DSS05 Access controls and security monitoring
Information media	• Loss/disclosure of portable media (e.g., CD, universal serial bus [USB] drives, portable disks) containing sensitive data • Loss of backup media • Accidental disclosure of sensitive information due to failure to follow information handling guidelines	• APO01 Policies and guidance on protection and use of IT assets • DSS05, 06 Protection of mobile and/or removable storage and media devices
Utilities performance	• Intermittent utilities (e.g., telecom, electricity) failure • Regular, extended utilities failures	• APO08 Relationships/management of key utility suppliers • DSS01 Environmental protection and facilities management
Industrial action	• Inaccessible facilities and building due to labour union strike • Unavailable key staff due to industrial action	• APO07 Staff relationships and key individuals • BAI08 Managing staff knowledge
Data(base) integrity	• Intentional modification of data (e.g., accounting, security-related data, sales figures) • Database (e.g., client or transactions database) corruption	• APO03 Information architecture and data classification • BAI03 Development standards • BAI06 Change management • DSS01 Managing data storage • DSS05 Access controls
Logical trespassing	• Users circumventing logical access rights • Users obtaining access to unauthorised information • Users stealing sensitive data	• APO01 Policies and guidance on protection and use of IT assets • DSS05 Access controls and security monitoring • APO07 Contract staff policies
Operational IT errors	• Operator errors during backup, upgrades of systems or maintenance of systems • Incorrect information input	• APO07 Staff training • DSS01 Operations procedures • DSS06 Business process controls
Contractual compliance	• Non-compliance with software licence agreements (e.g., use and/or distribution of unlicenced software) • Contractual obligations as service provider with customers/clients not met	• APO09 Monitoring service agreements • APO10 Supplier agreements and relationship monitoring • DSS02 Software licence management • MEA03 Contractual compliance requirements and current status monitoring
Environmental	• Use of equipment that is not environmentally friendly (e.g., high level of power consumption, packaging)	• APO03 Incorporation of environmentally friendly principles in enterprise architecture • BAI03 Selection of solutions and procurement policies • DSS01 Environmental and facilities management
Acts of nature	• Earthquake • Tsunami • Major storm/hurricane • Major wildfire	• DSS01 Environmental and facilities management • DSS05 Physical security • DSS04 Manage continuity

Appendix D
Example Business Case

Note: This example is provided as a non-prescriptive generic guide to encourage preparation of a business case to justify investment in a GEIT implementation programme. 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 existing internal business case and investment justification approaches, if they exist, and use this example and the guidance in this publication to help focus on all of the issues that should be addressed. Further guidance on developing business cases can be found in COBIT 5 process APO05 and in the *The Business Case Guide: Using Val IT™ 2.0*.

The example scenario 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, which they have used centrally for some time. They want to make sure that the rapid expansion and adoption of advanced IT in many of its businesses will deliver the value expected and also manage significant new risk. They have 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 of 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 programme for Acme Corporation based on COBIT.

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 realised.

The scope in terms of business entities that make up Acme Corporation is all-inclusive. It must be acknowledged that some form of prioritisation process will be applied across all entities for initial coverage by the GEIT programme due to limited programme resources.

There is a range of stakeholders that have an interest in the outcomes of the GEIT programme, 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 implementation of the GEIT programme 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 decentralised or federal business model that exists within Acme Corporation.

The GEIT programme will be achieved by focussing on the capability of the Acme processes and other enablers in relation to those that are defined in COBIT, relevant to each business unit. The relevant and prioritised processes that will receive focus at each entity will be identified through a facilitated workshop approach by the members of the GEIT programme, 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 objective of the GEIT programme is 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 realised 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 would continue within each business unit as normal business practice.

The GEIT programme will be delivered in two distinct phases. The first phase 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 the final approval has been obtained in the form of an approved business case, the GEIT programme 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 programme to implement the remedial actions identified at each business unit. The GEIT programme 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 programme is the one of 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 programme has been developed. The budget is detailed in a separate schedule. A detailed budget will also be completed for phase 2 of the project and submitted for approval by group management.

Background (See chapter 2. Positioning GEIT)

GEIT is an integral part of overall enterprise governance and is focussed 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 decentralised 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. Such a 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 (See chapter 3, section 3. Getting Started—Identify the Need to Act: Recognising Pain Points and Trigger Events)

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 to 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 with 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 decentralised/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
- Delivering new and innovative services in a highly competitive market successfully and on time

Gap Analysis and Goal

There is currently no groupwide approach or framework for GEIT or use of IT best 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 programme is therefore to increase the level of capability and adequacy of IT-related processes and controls appropriate to each business unit, in a prioritised manner.

The outcome should be that significant risk has been 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 the IT-related business risk profile of each entity should decrease and quality and efficiency should 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 framework is regarded by many as the world's leading GEIT and control framework. The COBIT framework has been implemented by some subsidiaries of the group. It is also specifically mentioned in the King III[9] report as a potential framework to be implemented for GEIT.

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

COBIT 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
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 for reasons of reporting, audit and clarity of internal control.

Proposed Solution

The GEIT programme is being planned in two distinct phases.

Phase 1. Pre-planning (See chapter 3. Taking the First Steps Towards GEIT)

Phase 1 of the GEIT programme is the development stage. During this stage of the programme the following steps would have been undertaken:

1. Core team structure finalised between risk management support and group IT
2. Core team COBIT foundation training completed
3. Workshop with the core team conducted to define an approach for the group
4. Creation of an online community within Acme Corporation to act as a repository for knowledge sharing
5. Identification of all stakeholders and their needs
6. Clarification and realignment, if required, of current committee structures, roles and responsibilities, decision rules, and reporting arrangements
7. Development and maintenance of a business case for the GEIT programme as a foundation for the successful implementation of the programme
8. Communication plan for guiding principles, policies and expected benefits throughout the programme
9. Development of the assessment and reporting tools for use during the life of the programme and beyond
10. Test of the approach at one local entity. This activity was chosen for ease of logistics, and to ease the refinement of the approach and tools.

[9] King III is the Corporate Governance Code in South Africa.

11. Pilot of the refined approach at one of the foreign entities. This is to understand and quantify the difficulties of running the GEIT programme assessment phase under more challenging business conditions.
12. Presentation of the final business case and approach, including a roll-out plan to Acme Corporation executive management for approval

Phase 2. Programme Implementation (See chapter 3, section 2. Applying a Continual Improvement Life Cycle Approach)

The GEIT programme is designed to start an ongoing programme 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 at 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 improvement projects at the local business unit level.
6. Realise and monitor the benefits.
7. Sustain the new way of working by keeping the momentum going.

Programme Scope

The GEIT programme will cover the following:

1. All of the group entities; however, the entities will have to be prioritised for interaction due to limited programme resources.
2. The method of prioritisation. 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 a through c.
3. The list of entities to be covered during the current financial year. This is still to be finalised and agreed on with Acme Corporation management.

Programme Methodology and Alignment (See chapter 6. Implementation Life Cycle Tasks, Roles and Responsibilities)

The GEIT programme 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 programme 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 guidance) that will provide a set of focus areas within the COBIT processes for consideration by the business unit. In this fashion, the business unit will be able to prioritise its remediation effort to address the areas of IT risk.

Programme Deliverables (See chapter 6. Implementation Life Cycle Tasks, Roles and Responsibilities)

As mentioned earlier, an overall goal of the GEIT programme 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 programme to enable Acme Corporation to gauge the delivery of the intended outcomes by the GEIT programme. These will include the following:

1. The GEIT programme will facilitate internal knowledge sharing via the intranet platform, as well as 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 prioritised business objectives, and consequent IT objectives based on COBIT
   b. The IT-related risk identified by the business unit in a standardised format, and the agreed-on focus areas for attention by the business unit based on COBIT processes and practices and other recommended enablers
   c. The above to be derived from the GEIT programme assessment tool
3. Overall progress reports on the intended coverage of the Acme Corporation business units by the GEIT programme 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 programme budget vs. actual amount spent will be generated.
6. Benefit monitoring and reporting against business-unit-defined value objectives and metrics will be created.

Programme Risk (See chapter 5. Enabling Change)

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

1. Management commitment and support for the programme, both at group level as well as the local business unit level
2. Demonstrating actual value delivery and benefits to each local entity through the adoption of the programme. 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 programme
4. Identifying key stakeholders at each entity for participation in the programme
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 programme. For example, the progress of the GEIT programme overall could become an agenda item of the IT executive committee. Local equivalents would also need to be constituted. This could be replicated geographically, as well as at local holding company level where appropriate.

Stakeholders (See chapter 3, section 4. Recognising Stakeholders' Roles and Requirements)

The following role players have been identified as stakeholders in the outcome of the GEIT programme:

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 individual names of the role players will be compiled and published after consultation with group management.

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

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

Cost-benefit Analysis

The programme should identify the expected benefits, and monitor that real business value is being generated from the investment. Local management should motivate and sustain the programme. 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 realised:

1. Maximising the realisation 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 as well as 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 programme 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 as well as overall. This will enable the group to maximise efficiency and standardisation.

Challenges and Success Factors (See chapter 4. Identifying Implementation Challenges and Success Factors)

Figure 48 summarises the challenges that could affect the GEIT programme during the implementation period of the programme and the critical success factors that should be addressed to ensure a successful outcome.

Figure 48—Challenges and Planned Actions for Acme Corporation

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 the benefit identification.
Lack of trust and good relationships between IT and the enterprise	• Foster open and transparent communication 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. • Formalise 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 enablement planning.
Lack of understanding of the Acme environment by those responsible for the GEIT programme	Apply a consistent assessment methodology.
Various levels of complexity (technical, organisational, 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.
Failure to realise 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 programme and project management principles. • Use milestones. • Prioritise 80/20 tasks (80 percent of the benefit with 20 percent of the effort) and be careful about sequencing in the correct order; capitalise 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 prioritising 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 prioritising 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.

Appendix E
COBIT 4.1 Maturity Attribute Table

Figure 49—COBIT 4.1 Maturity Table

Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement
1 Recognition of the need for the process is emerging. There is sporadic communication of the issues.	There are *ad hoc* approaches to processes and practices. The process and policies are undefined.	Some tools may exist; usage is based on standard desktop tools. There is no planned approach to the tool usage.	Skills required for the process are not identified. A training plan does not exist and no formal training occurs.	There is no definition of accountability and responsibility. People take ownership of issues based on their own initiative on a reactive basis.	Goals are not clear and no measurement takes place.
2 There is awareness of the need to act. Management communicates the overall issues.	Similar and common processes emerge, but are largely intuitive because of individual expertise. Some aspects of the process are repeatable because of individual expertise, and some documentation and informal understanding of policy and procedures may exist.	Common approaches to use of tools exist but are based on solutions developed by key individuals. Vendor tools may have been acquired, but are probably not applied correctly, and may even be shelfware.	Minimum skill requirements are identified for critical areas. Training is provided in response to needs, rather than on the basis of an agreed plan, and informal training on the job occurs.	An individual assumes his/her responsibility and is usually held accountable, even if this is not formally agreed. There is confusion about responsibility when problems occur, and a culture of blame tends to exist.	Some goal setting occurs; some financial measures are established but are known only by senior management. There is inconsistent monitoring in isolated areas.
3 There is understanding of the need to act. Management is more formal and structured in its communication.	Usage of good practices emerges. The process, policies and procedures are defined and documented for all key activities.	A plan has been defined for use and standardisation of tools to automate the process. Tools are being used for their basic purposes, but may not all be in accordance with the agreed plan, and may not be integrated with one another.	Skill requirements are defined and documented for all areas. A formal training plan has been developed, but formal training is still based on individual initiatives.	Process responsibility and accountability are defined and process owners have been identified. The process owner is unlikely to have the full authority to exercise the responsibilities.	Some effectiveness goals and measures are set, but are not communicated, and there is a clear link to business goals. Measurement processes emerge, but are not consistently applied. IT balanced scorecard ideas are being adopted, as is occasional intuitive application of root cause analysis.
4 There is understanding of the full requirements. Mature communication techniques are applied and standard communication tools are in use.	The process is sound and complete; internal best practices are applied. All aspects of the process are documented and repeatable. Policies have been approved and signed off on by management. Standards for developing and maintaining the processes and procedures are adopted and followed.	Tools are implemented according to a standardised plan, and some have been integrated with other related tools. Tools are being used in main areas to automate management of the process and monitor critical activities and controls.	Skill requirements are routinely updated for all areas, proficiency is ensured for all critical areas, and certification is encouraged. Mature training techniques are applied according to the training plan, and knowledge sharing is encouraged. All internal domain experts are involved, and the effectiveness of the training plan is assessed.	Process responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities. A reward culture is in place that motivates positive action.	Efficiency and effectiveness are measured and communicated and linked to business goals and the IT strategic plan. The IT balanced scorecard is implemented in some areas with exceptions noted by management and root cause analysis is being standardised. Continuous improvement is emerging.
5 There is advanced, forward-looking understanding of requirements. Proactive communication of issues based on trends exists, mature communication techniques are applied, and integrated communication tools are in use.	External best practices and standards are applied. Process documentation is evolved to automated workflows. Processes, policies and procedures are standardised and integrated to enable end-to-end management and improvement.	Standardised tool sets are used across the enterprise. Tools are fully integrated with other related tools to enable end-to-end support of the processes. Tools are being used to support improvement of the process and automatically detect control exceptions.	The organisation formally encourages continuous improvement of skills, based on clearly defined personal and organisational goals. Training and education support external best practices and use of leading-edge concepts and techniques. Knowledge sharing is an enterprise culture, and knowledge-based systems are being deployed. External experts and industry leaders are used for guidance.	Process owners are empowered to make decisions and take action. The acceptance of responsibility has been cascaded down throughout the organisation in a consistent fashion.	There is an integrated performance measurement system linking IT performance to business goals by global application of the IT balanced scorecard. Exceptions are globally and consistently noted by management and root cause analysis is applied. Continuous improvement is a way of life.

Page intentionally left blank