With information and technology at the heart of creating value for enterprises, it is more important than ever for organizations to optimize their IT assurance approach in order to effectively identify related risks and opportunities.

This guide is designed to enable efficient and effective development of IT assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews using a road map based on well-accepted assurance approaches.

The preceding pages provide a preview of the information contained in COBIT 5 for Assurance.

To purchase COBIT 5 for Assurance, or to learn more visit www.isaca.org/cobit5.

**Not a member?** Learn the value of ISACA membership. Additional information is available at www.isaca.org/membervalue.
About ISACA®
With more than 100,000 constituents in 180 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® (Cgeois®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA continually updates and expands the practical guidance and product family based on the COBIT framework. COBIT 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 and created COBIT® 5 for Assurance (the ‘Work’) primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights
© 2013 ISACA. All rights reserved. For usage guidelines, see www.isaca.org/COBITuse.

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

Provide 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 ISACA on LinkedIn: ISACA (Official), http://linkd.in/ISACAOfficial
Like ISACA on Facebook: www.facebook.com/ISACAHQ

COBIT® 5 for Assurance

1
ACKNOWLEDGEMENTS

ISACA wishes to recognise:

COBIT for Assurance Task Force
Anthony Noble, CISA, Viacom Inc., USA, Chairman
Pippa G. Andrews, CISA, CRISC, ACA, CIA, CMIIA, KPMG, Australia
Joseph M. Fodor, CISA, CPA, Ernst & Young LLP, USA
Robert D. Johnson, CISA, CISM, CGEIT, CRISC, CISSP, Bank of America, USA
Waleed Khalid, CISA, MetLife, UK

Development Team
Floris Ampe, CISA, CGEIT, CRISC, CIA, ISO 27000, PwC, Belgium
Stefanie Grijp, PwC, Belgium
Bart Peeters, CISA, PwC, Belgium
Dirk Steuperaert, CISA, CGEIT, CRISC, ITIL, IT In Balance BVBA, Belgium
Sven Van Hoorebeck, PwC, Belgium

Workshop Participants
Michael Berardi, CISA, CGEIT, CRISC, Bank of America, USA
Kamal Dave, CISA, CISM, CGEIT, HP, USA
Roger Debreceny, Ph.D., CGEIT, FCPA, University of Hawaii - Manoa, USA
Seda Demircioglu Foppen, CISA, CRISC, PwC, Turkey
Michael Dickson, CISA, CISM, CRISC, CPA, GBQ Partners, USA
Andreas Eschbach, PwC, Switzerland
Norm Kelson, CISA, CGEIT, CPA, CPE Interactive Inc, USA
Marty King, CISA, CGEIT, CPA, ITIL, Blue Cross Blue Shield NC, USA
Andreas Louca, CISA, Eurobank Ergasias, Greece
Lucio Augusto Molina Focazzi, CISA, CISM, CRISC, ITIL, Independent Consultant, Colombia
Robert Parker, CISA, CRISC, CPA-CA, CMC, FCA, Canada
Maria Patricia Prandini, CISA, CRISC, Universidad de Buenos Aires, Argentina
Abdul Rafeq, CISA, CGEIT, CIA, FCA, A.Rafeq and Associates, India
Mark Stacey, CISA, FCA, BG Group plc, UK
Wim van Greemeren, Ph.D., University of Antwerp Management School, Belgium

Expert Reviewers
Sushil Chatterji, CGEIT, CEA, CMC, Edutech Enterprises, Singapore
Steven De Haes, PhD, University of Antwerp—Antwerp Management School, Belgium
Seda Demircioglu Foppen, CRISC, PwC, Turkey
Michael Dickson, CISA, CISM, CRISC, CPA, GBQ Partners LLC, USA
Yalcin Gerek, CISA, CGEIT, CRISC, ITIL Expert, PRINCE2, TAC A.S., Turkey
J. Winston Hayden, CISA, SISM, CGEIT, CRISC, South Africa
John Jasinski, CISA, CGEIT, ISO20000, ITIL Expert, SSBB, MOF, USA
Masatoshi Kajimoto, CISA, CRISC, Independent Consultant, Japan
Joanna Karczewska, CISA, Poland
John W. Lainhart, IV, CISA, CISM, CGEIT, CRISC, CIPP/G, CIPP/US, IBM Global Business Services, USA
Lynn Lawton, CISA, CRISC, FCA, FBICS CITP, FCA, FIIA, KPMG Limited, Russia
Robert Parker, CISA, CRISC, CA, CMC, CPA, FCA, Canada
Andre Pitkowski, CGEIT, CRISC, OCTAVE, APIT Informatica Ltd, Brazil
Maria Patricia Prandini, CISA, CRISC, Universidad de Buenos Aires, Argentina
Abdul Rafeq, CISA, CGEIT, CIA, FCA, A. Rafeq and Associates, India
Eduardo Rietegno, CISA, CRISC, QAR (IIA), Banco de la Nacion Argentina, Argentina
Claus Rosenquist, CISA, CISSP, Nets Holding A/S, Denmark
Tichaona Zororo, CISA, CISM, CGEIT, CRISC, CIA, EGIT|Enterprise Governance of IT (PTY) Ltd., South Africa
ACKNOWLEDGEMENTS (CONT.)

ISACA Board of Directors
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, International President
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Vice President
Juan Luis Carselle, CISA, CGEIT, CRISC, Wal-Mart, Mexico, Vice President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., USA, Vice President
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Past International President
Emil D’Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (retired), USA, Past International President
John Ho Chi, CISA, CISM, CRISC, CBIP, CFE, Ernst & Young LLP, Singapore, Director
Krysten McCabe, CISA, The Home Depot, USA, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Australia, Director

Knowledge Board
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Thomas E. Borton, CISA, CISM, CRISC, CISSP, Cost Plus, USA
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Salomon Rico, CISA, CISM, CGEIT, Deloitte, Mexico

Framework Committee
Steven A. Babb, CGEIT, CRISC, Betfair, UK, Chairman
Charles Betz, Enterprise Management Associates, USA
David Cau, ISO, ITIL, MSP, PRINCE2, France
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Frank J. Cindrich, CGEIT, CIPP, CIPP/G, Deloitte & Touche LLP, USA
Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Austria
Anthony P. Noble, CISA, Viacom, USA
Andre Pitkowski, CGEIT, CRISC, APIT Informatica, Brazil
Paras Kesharichand Shah, CISA, CGEIT, CRISC, CA, Australia

Special recognition for financial support:
Los Angeles Chapter

ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors
Information Security Forum
Institute of Management Accountants Inc.
ISACA chapters
ITGI France
ITGI Japan
Norwich University
Socitum Performance Management Group
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School

ASIS International
Hewlett-Packard
IBM
Symantec Corp.
# Table of Contents

## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9</td>
</tr>
</tbody>
</table>

## Executive Summary

1. Introduction and Objectives .......................................................... 11
2. Drivers for Assurance .................................................................... 11
3. Benefits of the Publication ............................................................ 11
4. Target Audience for the Publication .............................................. 12
5. Document Overview and Guidance on Its Use ............................... 13
6. Prerequisite Knowledge ................................................................ 14

## Section 1. Assurance

### Chapter 1. Assurance Defined .................................................... 15
1.1 Three-party Relationship ............................................................. 15
1.2 Subject Matter ........................................................................... 16
1.3 Suitable Criteria ........................................................................ 16
1.4 Execution .................................................................................... 16
1.5 Conclusion .................................................................................. 16
1.6 The Assurance Process ............................................................... 17

### Chapter 2. Scope of the Publication ............................................ 19
2.1 Perspectives on Assurance ......................................................... 19
2.2 Related Publications and Scope of the Publication ..................... 20

### Chapter 3. Principles of Providing Assurance ............................... 21
3.1 Meeting Stakeholder Needs ......................................................... 21
3.2 Covering the Enterprise End-to-end ............................................. 23
3.3 Applying a Single Integrated Framework ..................................... 23
3.4 Enabling a Holistic Approach ..................................................... 23
3.5 Separating Governance From Management ............................... 24

## Section 2A. Assurance Function Perspective: Using COBIT 5 Enablers for Governing and Managing an Assurance Function

### Chapter 1. Introduction to Enablers ............................................. 25
1.1 Introduction ................................................................................ 25
1.2 Dimensions of the Generic Enabler Model ..................................... 25
1.3 The Publication and Enablers ....................................................... 26

### Chapter 2. Enabler: Principles, Policies and Frameworks .............. 27
2.1 The Principles, Policies and Frameworks Model ............................ 27
2.2 Assurance Function Perspective: Assurance-related Principles, Policies and Frameworks ......................................................... 28
2.3 ISACA Code of Professional Ethics ............................................... 29

### Chapter 3. Enabler: Processes ..................................................... 31
3.1 The Process Model ...................................................................... 31
3.2 Assurance Function Perspective: Processes Supporting the Assurance Function ................................................................. 32

### Chapter 4. Enabler: Organisational Structures ............................ 35
4.1 The Organisational Structures Model ........................................... 35
4.2 Assurance Function Perspective: Assurance-related Organisational Structures ................................................................. 36

### Chapter 5. Enabler: Culture, Ethics and Behaviour ...................... 39
5.1 The Culture, Ethics and Behaviour Model .................................... 39
5.2 Assurance Function Perspective: Assurance-related Culture, Ethics and Behaviour ................................................................. 40

### Chapter 6. Enabler: Information .................................................. 43
6.1 The Information Model ............................................................... 43
6.2 Assurance Function Perspective: Assurance-related Information Entities ................................................................. 45
<table>
<thead>
<tr>
<th>Section/Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1. ITAF, 2nd Edition</td>
<td>83</td>
</tr>
<tr>
<td>Chapter 2. International Professional Practices Framework (IPPF) for Internal Auditing Standards 2013</td>
<td>89</td>
</tr>
<tr>
<td>Chapter 3. Statement on Standards for Attestation Engagements No. 16 (SSAE 16)</td>
<td>95</td>
</tr>
<tr>
<td>Section 3. How This Publication Relates to Other Standards</td>
<td>83</td>
</tr>
<tr>
<td>Chapter 5. Generic Approach for Communicating on an Assurance Initiative (Phase C)</td>
<td>81</td>
</tr>
<tr>
<td>Chapter 4. Understand the Enablers, Set Suitable Assessment Criteria and Perform the Assessment (Phase B)</td>
<td>67</td>
</tr>
<tr>
<td>4.1 Introduction</td>
<td>67</td>
</tr>
<tr>
<td>4.2 Achievement of Goals</td>
<td>68</td>
</tr>
<tr>
<td>4.3 Enabler: Principles, Policies and Frameworks</td>
<td>68</td>
</tr>
<tr>
<td>4.4 Enabler: Processes</td>
<td>70</td>
</tr>
<tr>
<td>4.5 Enabler: Organisational Structures</td>
<td>71</td>
</tr>
<tr>
<td>4.6 Enabler: Culture, Ethics and Behaviour</td>
<td>73</td>
</tr>
<tr>
<td>4.7 Enabler: Information</td>
<td>74</td>
</tr>
<tr>
<td>4.8 Enabler: Services, Infrastructure and Applications</td>
<td>76</td>
</tr>
<tr>
<td>4.9 Enabler: People, Skills and Competencies</td>
<td>77</td>
</tr>
<tr>
<td>Chapter 3. Statement on Standards for Attestation Engagements No. 16 (SSAE 16)</td>
<td>95</td>
</tr>
<tr>
<td>Section 2B. Assessment Perspective: Providing Assurance Over a Subject Matter</td>
<td>53</td>
</tr>
<tr>
<td>Chapter 1. Core Assurance Processes</td>
<td>53</td>
</tr>
<tr>
<td>Chapter 2. Introduction and Overview of the Assessment Approach</td>
<td>55</td>
</tr>
<tr>
<td>2.1 Assurance and Enabler Performance Management</td>
<td>55</td>
</tr>
<tr>
<td>2.2 Assurance Engagement Approach Based on COBIT 5</td>
<td>55</td>
</tr>
<tr>
<td>2.3 Generic Audit/Assurance Programme</td>
<td>56</td>
</tr>
<tr>
<td>Chapter 3. Determine Scope of the Assurance Initiative (Phase A)</td>
<td>59</td>
</tr>
<tr>
<td>3.1 Workflow</td>
<td>59</td>
</tr>
<tr>
<td>3.2 Example Scope</td>
<td>62</td>
</tr>
<tr>
<td>3.3 Useful COBIT 5 Constructs for Scope Development</td>
<td>65</td>
</tr>
<tr>
<td>3.4 Assurance Assignment Scoping Summary</td>
<td>66</td>
</tr>
<tr>
<td>Chapter 4. Understand the Enablers, Set Suitable Assessment Criteria and Perform the Assessment (Phase B)</td>
<td>67</td>
</tr>
<tr>
<td>4.1 Introduction</td>
<td>67</td>
</tr>
<tr>
<td>4.2 Achievement of Goals</td>
<td>68</td>
</tr>
<tr>
<td>4.3 Enabler: Principles, Policies and Frameworks</td>
<td>68</td>
</tr>
<tr>
<td>4.4 Enabler: Processes</td>
<td>70</td>
</tr>
<tr>
<td>4.5 Enabler: Organisational Structures</td>
<td>71</td>
</tr>
<tr>
<td>4.6 Enabler: Culture, Ethics and Behaviour</td>
<td>73</td>
</tr>
<tr>
<td>4.7 Enabler: Information</td>
<td>74</td>
</tr>
<tr>
<td>4.8 Enabler: Services, Infrastructure and Applications</td>
<td>76</td>
</tr>
<tr>
<td>4.9 Enabler: People, Skills and Competencies</td>
<td>77</td>
</tr>
<tr>
<td>Chapter 5. Generic Approach for Communicating on an Assurance Initiative (Phase C)</td>
<td>81</td>
</tr>
<tr>
<td>Section 3. How This Publication Relates to Other Standards</td>
<td>83</td>
</tr>
<tr>
<td>Chapter 1. ITAF, 2nd Edition</td>
<td>83</td>
</tr>
<tr>
<td>Chapter 2. International Professional Practices Framework (IPPF) for Internal Auditing Standards 2013</td>
<td>89</td>
</tr>
<tr>
<td>Chapter 3. Statement on Standards for Attestation Engagements No. 16 (SSAE 16)</td>
<td>95</td>
</tr>
</tbody>
</table>
# Table of Contents

## Appendices

**Appendix A. Glossary** ................................................................................................................................. 101

**Appendix B. Detailed Enablers for Assurance Governance and Management** ................................................................. 103
  B.1 Principles, Policies and Frameworks ........................................................................................................ 103
  B.2 Processes .................................................................................................................................................. 105
  B.3 Organisational Structures .......................................................................................................................... 131
  B.4 Culture, Ethics and Behaviour ................................................................................................................... 139
  B.5 Information .................................................................................................................................................. 143
  B.6 Services, Infrastructure and Applications .................................................................................................. 177
  B.7 People, Skills and Competencies ................................................................................................................ 185

**Appendix C. Core Assurance Processes** ........................................................................................................ 193
  C.1 Core Assurance Processes ......................................................................................................................... 193

**Appendix D. Example Audit/Assurance Programmes** ....................................................................................... 209
  D.1 COBIT 5-based Audit/Assurance Programme: Change Management ...................................................... 211
  D.2 COBIT 5-based Audit/Assurance Programme: Risk Management ............................................................ 243
  D.3 COBIT 5-based Audit/Assurance Programme: Bring Your Own Device (BYOD) .................................... 283
LIST OF FIGURES

Figure 1—COBIT 5 Product Family..................................................................................11
Figure 2—COBIT 5 for Assurance Target Audience and Benefits.............................................12
Figure 3—COBIT 5 for Assurance Overview........................................................................13
Figure 4—Assurance Components......................................................................................15
Figure 5—Two Perspectives on Assurance Provided by COBIT 5........................................19
Figure 6—Scope of COBIT 5 for Assurance .........................................................................20
Figure 7—COBIT 5 Principles............................................................................................21
Figure 8—Comparison of Assurance Engagement Types..........................................................22
Figure 9—Assurance Types Compared................................................................................23
Figure 10—COBIT 5 Enterprise Enablers...............................................................................24
Figure 11—COBIT 5 Enablers: Generic ..............................................................................25
Figure 12—COBIT 5 Enabler: Principles, Policies and Frameworks.....................................27
Figure 13—Principles, Policies and Frameworks Addressed in ITAF ....................................28
Figure 14—COBIT 5 Enabler: Processes................................................................................51
Figure 15—COBIT 5 Process Reference Model: Supporting Processes for the Assurance Function ......................................................................................................................32
Figure 16—Key Processes Supporting Assurance Provisioning .............................................33
Figure 17—Other Supporting Processes for Assurance Provisioning ...................................34
Figure 18—COBIT 5 Enabler: Organisational Structures ....................................................35
Figure 19—Core Organisational Structures Supporting Assurance ......................................36
Figure 20—Other Relevant Structures................................................................................37
Figure 21—COBIT 5 Enabler: Culture, Ethics and Behaviour .............................................39
Figure 22—Relevant Behaviour for Assurance Provisioning ..............................................40
Figure 23—COBIT 5 Enabler: Information .........................................................................43
Figure 24—Information Items Supporting Assurance ..........................................................45
Figure 25—Additional Information Inputs...........................................................................46
Figure 26—COBIT 5 Enabler: Services, Infrastructure and Applications .............................47
Figure 27—IT Assurance-related Services............................................................................48
Figure 28—IT Assurance-related Supporting Applications..................................................49
Figure 29—COBIT 5 Enabler: People, Skills and Competencies .........................................51
Figure 30—COBIT 5 MEA Domain Processes ....................................................................53
Figure 31—COBIT 5 for Assurance Enabler: Performance Management.............................55
Figure 32—Generic COBIT 5-based Assurance Engagement Approach..............................56
Figure 33—COBIT 5 Goals Cascade ..................................................................................65
Figure 34—Assurance Engagement Scoping Summary..........................................................66
Figure 35—ITAF Components Related to COBIT 5 for Assurance.....................................84
Figure 36—IPPF Components Related to COBIT 5 for Assurance ......................................89
Figure 37—SSAE 16 Components Related to COBIT 5 for Assurance ...............................95
Figure 38—Key Processes Supporting Assurance Provisioning .........................................105
Figure 39—Generic COBIT 5-based Assurance Engagement Approach .............................209
Figure 40—COBIT 5 Enterprise Goals ..............................................................................210
Figure 41—IT-related Goals ..............................................................................................210
Executive Summary

1. Introduction and Objectives

Information is a key resource for all enterprises and, from the time information is created to the moment it is destroyed, technology plays a significant role. Technology is increasingly advanced and has become pervasive in enterprises and the social, public and business environments.

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises to create optimal value from information technology (IT) by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking into account the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

COBIT 5 for Assurance builds on the COBIT 5 framework as shown in figure 1. It focuses on assurance, and it provides more detailed and practical guidance for assurance professionals and other interested parties at all levels of the enterprise on how to use COBIT 5 to support a variety of IT assurance activities.

Figure 1—COBIT 5 Product Family

If an enterprise is already using COBIT 5 as its framework for the governance and management of enterprise IT, this publication will enable the enterprise to leverage COBIT 5 when planning and performing assurance reviews, so that the business, IT and assurance professionals are aligned around a common framework and common objectives. However, the enterprise does not have to be currently using COBIT 5 to use COBIT 5 for Assurance.

This guide is designed to enable efficient and effective development of IT assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews using a road map based on well-accepted assurance approaches.

2. Drivers for Assurance

The main drivers for assurance in its different forms include:
• Providing interested parties substantiated opinions on governance and management of enterprise IT according to assurance objectives
• Defining assurance objectives in line with enterprise objectives, thus maximising the value of assurance initiatives
• Satisfying regulatory or contractual requirements for enterprises to provide assurance over their IT arrangements
To that purpose, this guide:

- Provides guidance on how to use the COBIT 5 framework to establish and sustain assurance provisioning and an assurance function for the enterprise
- Provides a structured approach on how to provide assurance over enablers (all of COBIT 5’s defined enablers, e.g., Processes, Information, Organisational Structures)
- Illustrates the structured approach with a number of concrete examples of audit/assurance programmes

### 3. Benefits of the Publication

A major benefit of this guide is that users can rely on the consistency, structure, context and vocabulary of the COBIT 5 framework and its related products. The COBIT 5 framework addresses the governance and management of enterprise IT, helping to align business and IT management and providing a basis for improving IT performance. If assurance professionals base their reviews on the same framework as that used by business and IT managers who are improving value of IT for the enterprise, everyone involved will be using a common language, and it will be easier to agree on and implement any necessary control improvements.

This guide can be used by assurance professionals for many different purposes, including:

- Obtaining a view (based on COBIT 5 concepts such as the enablers) on current good practices on assurance
- Learning how to use different COBIT 5 components and related concepts for planning, scoping, executing and reporting on various types of IT assurance initiatives
- Obtaining a view of the extent to which the value objective of the enterprise—delivering benefits while optimising risk and resource use—is achieved

### 4. Target Audience for the Publication

The target audience for this publication is broad, and includes:

- Assurance professionals at various governance and management layers
- Boards and audit committees, as stakeholders who commission assurance activities
- Business and IT management, as responsible parties
- External stakeholders, including external auditors, regulators and customers

The intended audience for COBIT 5 for Assurance is extensive, as are the reasons for adopting and using the framework and the benefits each group can find in it (figure 2). All of the roles listed in figure 2 can be considered stakeholders for assurance provisioning.

<table>
<thead>
<tr>
<th>Role</th>
<th>Benefit of/Reason for Adopting and Adapting COBIT 5 for Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boards and executive management</td>
<td>Better understanding of their responsibilities and roles with regard to assurance provisioning</td>
</tr>
<tr>
<td>Audit committee</td>
<td></td>
</tr>
<tr>
<td>Auditors</td>
<td>Better understanding of their responsibilities and roles with regard to assurance provisioning</td>
</tr>
<tr>
<td>External auditors</td>
<td>Having a structured framework that provides a common language amongst all stakeholders to provide assurance over specific IT areas</td>
</tr>
<tr>
<td>Chief information officer (CIO) and IT management</td>
<td>Having a structured framework that provides a common language to assess performance and conformance of IT</td>
</tr>
<tr>
<td>Business management</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td>Better understanding of their responsibilities and roles with regard to assurance provisioning</td>
</tr>
<tr>
<td>Regulators</td>
<td>Having a structured framework that provides a common language to express regulatory requirements</td>
</tr>
</tbody>
</table>

Although this guide is aimed primarily at assurance professionals, it may also be of interest to IT professionals and advisors. The publication will be most useful to experienced professionals and is not intended to provide a tutorial on IT assurance.
## 5. Document Overview and Guidance on Its Use

**COBIT 5 for Assurance** addresses a number of fundamental questions and issues pertaining to providing assurance over IT. **Figure 3** depicts these questions and explains how and where this publication addresses them (or not).

### Figure 3—COBIT 5 for Assurance Overview

<table>
<thead>
<tr>
<th>Question</th>
<th>Where to Find Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is assurance?</td>
<td><strong>Section 1</strong> defines assurance, and describes briefly how the COBIT 5 principles can be applied to assurance-specific needs.</td>
</tr>
<tr>
<td>How do COBIT 5 enablers relate to providing assurance?</td>
<td>In general, two perspectives on how to use COBIT 5 in an assurance context can be identified: 1. The assurance function perspective, describing what is needed in an enterprise to build and sustain an efficient and effective assurance function. 2. The assessment perspective, describing how different types of assurance engagements or assessments can be supported by the COBIT 5 enablers.</td>
</tr>
</tbody>
</table>
| How do I set up and maintain an efficient assurance function?            | **Section 2A** provides guidance on what is needed to set up and maintain an effective and efficient assurance function. It lists and briefly describes the COBIT 5 enablers required, e.g., processes, organisational structures. Putting these enablers in place will result in an effective and efficient assurance function that adds value to the enterprise.  
Appendix B.1–7 includes detailed descriptions for each enabler listed in section 2A. |
| How does COBIT 5 help me to provide assurance?                          | COBIT 5 helps to provide assurance in several ways: 1. COBIT 5 includes an enabler model, after which all seven COBIT 5 enablers are structured. Part of this enabler model is the performance assessment dimension, which is used to structure any assessment of any enabler. This is explained in **Section 2B**. 2. COBIT 5, and especially the COBIT 5 process reference model as described in the **COBIT 5: Enabling Processes** publication, provides a comprehensive reference model for all governance and management aspects of IT. As such, it constitutes the perfect set of suitable criteria on which to base any assessment. |
| What does a COBIT 5-based audit/assurance programme look like?           | **Section 2B** explains the audit/assurance process in detail, and it describes a generic, skeleton audit/assurance programme. This programme builds on the COBIT 5 enablers, which results in a comprehensive and holistic programme. |
| Are there any examples of COBIT 5-based audit/assurance programmes?     | Yes. **Section 2B** explains the generic structure of an audit/assurance programme.  
Appendix D contains a set of example audit/assurance programmes based on this template. More sample audit/assurance programmes will be published separately by ISACA. |
| Does COBIT 5 align with assurance standards?                            | Yes. A detailed comparison, in the form of a mapping or qualitative description, is included in **section 3**. The following related standards are referred to in this section: ITAF, IPPF and ISAE 3402/SSAE 16. |
| Does COBIT 5 for Assurance include detailed instructions on how to perform an assessment? | No. **COBIT 5 for Assurance** assumes that the reader is familiar with, and can apply, basic auditing and assessment techniques. A brief overview of auditing techniques is included in **section 2B**, chapter 4.1, but details are not provided. |
COBIT 5 for Assurance refers to the seven enablers of COBIT 5: Principles, Policies and Frameworks; Processes; Organisational Structures; Culture, Ethics and Behaviour; Information; Services, Infrastructure and Applications; and People, Skills and Competencies. The unique character of each enterprise will result in these enablers being implemented and used in many different ways to provide assurance in an optimal manner. This publication provides a pervasive view that explains each concept of COBIT 5 from an assurance function perspective through additional guidance and examples.

To facilitate and guide the reader through the comprehensive collection of information, COBIT 5 for Assurance is divided into three sections and four appendices.

Following is a brief description of each section and how those sections are interconnected.

Section 1—Elaborates on assurance, and describes briefly how the COBIT 5 principles can be applied to assurance-specific needs. This section provides the reader with a conceptual baseline that will be followed throughout the rest of the publication.

Section 2A—Elaborates on using COBIT 5 enablers for governing and managing assurance. Governance of enterprise IT, which includes an assurance activity, is systemic and supported by a set of enablers. In this section, the assurance function perspective on how to apply the COBIT 5 enablers is elaborated on, i.e., all COBIT 5 enablers required to have an effective and efficient assurance function and provisioning are explained. Detailed guidance regarding these enablers is provided in appendix B.

Section 2B—Elaborates on providing assurance over COBIT 5 enablers. In this section, the assessment perspectives on how to provide/obtain assurance over COBIT 5 enablers (Processes, Organisational Structures, Information, etc.) are elaborated. This section also includes a generic audit/assurance programme based on COBIT 5.

Section 3—Discusses the relationship between COBIT 5 and relevant auditing standards and practices

Appendix A—Glossary

Appendix B—Detailed guidance on the seven COBIT 5 enablers for governing and managing assurance
- B.1—Detailed guidance on the Principles, Policies and Frameworks enabler
- B.2—Detailed guidance on the Processes enabler
- B.3—Detailed guidance on the Organisational Structures enabler
- B.4—Detailed guidance on the Culture, Ethics and Behaviour enabler
- B.5—Detailed guidance on the Information enabler
- B.6—Detailed guidance on the Services, Infrastructure and Applications enabler
- B.7—Detailed guidance on the People, Skills and Competencies enabler

Appendix C—Detailed description of core assurance processes

Appendix D—Example audit/assurance programmes, supporting the provisioning of assurance over the COBIT 5 enablers. These programmes are based on the generic audit/assurance programme described in section 2B.

6. Prerequisite Knowledge

COBIT 5 for Assurance builds on COBIT 5. Most key concepts of COBIT 5 are repeated and elaborated on in this publication, making it a fairly standalone book—in essence, not requiring any prerequisite knowledge. However, an understanding of COBIT 5 at the foundation level will accelerate comprehension of this publication.

Should readers wish to know more about COBIT 5 concepts beyond what is required for assurance purposes, they are referred to the COBIT 5 framework publication.

COBIT 5 for Assurance also refers to the COBIT® 5 Process Assessment Model (PAM): Using COBIT® 5 and the COBIT 5 process details described therein. If readers wish to know more about the process capability assessment approach, they are referred to the COBIT Assessment Programme guides.1

1 Links to the COBIT Assessment Programme guides can be found at www.isaca.org/cobit-assessment-programme
SECTION 1. ASSURANCE

CHAPTER 1
ASSURANCE DEFINED

Assurance means that, pursuant to an accountability relationship between two or more parties, an IT audit and assurance professional may be engaged to issue a written communication expressing a conclusion about the subject matters to the accountable party.

Assurance refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter. For example, assurance engagements could include support for audited financial statements; assessment of value provided by IT to the enterprise; reviews of controls; compliance with required standards and practices; and compliance with agreements, licences, legislation and regulations.

Formal standards such as ISACA’s Information Technology Assurance Framework (ITAF), Institute of Internal Auditor’s (IIA) International Professional Practices Framework (IPPF) and the American Institute of Certified Public Accountants’ (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 16 exist and may be referenced, but in this publication assurance also covers evaluation activities not governed by internal and/or external audit standards.

An assurance initiative consists of five components, as illustrated in figure 4. Each of those components is described in further detail in the following subsections.

Figure 4—Assurance Components

1.1 Three-party Relationship

An accountable party is the individual, group or entity (auditee), usually involving management, that is ultimately responsible for subject matter, process or scope. An assurance engagement involves two other parties:

- Depending on the circumstances, the user could include a variety of stakeholders, such as shareholders, creditors, customers, the board of directors, the audit committee, legislators or regulators. For some types of assurance activities, the auditee and the user can be identical, e.g., IT management.
- The assurance professional (auditor) is the person who has overall responsibility for the performance of the assurance engagement and for the issuance of the report on the subject matter.
In conducting an assurance assignment, an accountability relationship exists amongst the three parties. The accountability relationship is a prerequisite for an assurance engagement, and it exists when one party (the auditee) is responsible to another party (the user) for a subject matter, or voluntarily chooses to report to another party on a subject matter. The accountability relationship may arise as a result of an (contractual) agreement or legislation, or because a user can be expected to have an interest in how the accountable party has discharged its responsibility for a subject matter.

1.2 Subject Matter

Subject matter is the specific information, practices or controls, such as any of the seven COBIT 5 enablers, that are the subject of an audit and assurance professional’s review, examination and report. This subject matter can include the design or operation of internal controls and management practices over any aspect of the enterprise, or compliance with privacy practices or standards or specified laws and regulations.

1.3 Suitable Criteria

Criteria are the standards and benchmarks, such as COBIT 5, used to measure and present the subject matter and against which the practitioner evaluates the subject matter.

Criteria can be formal or less formal. There can be different criteria for the same subject matter. Suitable criteria are required for reasonably consistent evaluation or measurement of a subject matter within the context of professional judgement. Suitable criteria must have the necessary information quality goal attributes as defined in the COBIT 5 Information model, in particular:

- **Objectivity**—Criteria should be free from bias.
- **Measurability**—Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- **Understandability**—Criteria should be communicated clearly and not be subject to significantly different interpretations by intended users.
- **Completeness**—Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about the subject matter are not omitted.
- **Relevance**—Criteria should be relevant to the subject matter.

Where criteria are established by management, assurance professionals must ensure that the scope covers what would normally be considered appropriate based on generally accepted definitions of the scope of the subject matter, or identify any scope limitations in their reports.

1.4 Execution

When undertaking an assurance activity, the audit and assurance professional eventually executes the assignment by following a structured approach, dependent on other enablers, to reach a conclusion on the evaluation of the subject matter.

1.5 Conclusion

The process of evaluating the results of audit or assurance testing, after confirmation, to arrive at conclusions and recommendations can be complex. What appears to be a problem may, in fact, be the effect of a problem, not the cause. Therefore, it is important for the audit and assurance professional to follow the conclusion process, from confirming facts with key individuals in the areas being audited to determining root causes. The individual findings can then be used to provide examples that support higher-level analysis:

- Developing various scenarios leading to potential recommendations
- Selecting an appropriate recommendation that is practical and achievable
- Identifying steps necessary to ensure buy-in of key stakeholders

Indeed, audit and assurance professionals should obtain an adequate understanding of the subject matter and its business environment. They should see the bigger picture, link the impact of the issues/findings to the overall organisational strategic goals and objectives to tell the ‘the story behind the story’, and communicate value insights. Executives are not very interested in knowing the observations; they need to understand the insights behind the findings.
Recommendations resulting from the conduct of audit and assurance engagements may be reported in a separate report, not as part of the audit or assurance report. The recommendations—which, as part of the reporting process require review and agreement by management and the auditee or other stakeholders—should be presented in a clear, concise and actionable manner. Reports to senior management and executives should address issues and concepts, with detailed audit findings used as illustrations of the issue, problem or result. Reports to middle and line management should contain the same information, but with a different level of detail, to allow them to fully understand the issue and handle the problem. Where appropriate, recommendations should include provision for timely monitoring and follow-up.

1.6 The Assurance Process

The assurance process includes the four components described previously in subsections 1.2 through 1.5, i.e., it defines a scope relating to the subject matter, it sets suitable criteria based on a sound reference model, and it executes the assignment, after which it issues a conclusion to the user. This is also depicted in figure 3.

The assurance process is defined in detail in section 2B of this publication.