

# **COBIT<sup>®</sup> 5:** The Framework

Exposure Draft

# *COBIT 5: The Framework Exposure Draft*

## **ISACA®**

With 95,000 constituents in 160 countries, ISACA ([www.isaca.org](http://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: The Framework Exposure Draft* (the 'Work'), primarily as an educational resource for control 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 control circumstances presented by the particular systems or information technology environment.

## **Reservation of Rights**

© 2011 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and non-commercial use and for consulting/advisory engagements and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

## **ISACA**

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Phone: +1.847.253.1545  
Fax: +1.847.253.1443  
E-mail: [info@isaca.org](mailto:info@isaca.org)  
Web site: [www.isaca.org](http://www.isaca.org)

*COBIT® 5: The Framework Exposure Draft*

CRISC is a trademark/service mark of ISACA. The mark has been applied for or registered in countries throughout the world.

## Acknowledgements

### ISACA wishes to recognise:

#### COBIT 5 Task Force (2009-2011)

John W. Lainhart, IV, CISA, CISM, CGEIT, IBM Global Consulting Services, USA, Co-chair  
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CITP, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd, UK, Co-chair  
Pippa G. Andrews, CISA, ACA, CIA, KPMG, Australia  
Elisabeth Antonsson, CISM, BSc, BA, Nordea Bank, Sweden  
Steven A. Babb, CGEIT, KPMG, 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, Austria  
Robert D. Johnson, CISA, CISM, CGEIT, ING US Financial Services, USA  
Erik Pols, CISA, CISM, Shell International-ITCI, Netherlands  
Vernon Poole, CISM, CGEIT, Sapphire, UK  
Abdul Rafeq, CISA, CGEIT, CIA, FCA, A. Rafeq and Associates, India

#### Development Team

Floris Ampe, CISA, CGEIT, CIA, ISO27000, PricewaterhouseCoopers, Belgium  
Gert du Preez, CGEIT, PricewaterhouseCoopers, Canada  
Stefanie Grijp, PricewaterhouseCoopers, Belgium  
Gary Hardy, CGEIT, IT Winners, South Africa  
Bart Peeters, PricewaterhouseCoopers, Belgium  
Dirk Steuperaert, CISA, CGEIT, CRISC IT In Balance BVBA, Belgium

#### Workshop Participants

Gary Baker, CA, Canada  
Brian Barnier, USA  
Johannes Hendrik Botha, MBCS-CITP, FSM, getITright Skills Development, South Africa  
Ken Buechler, PMP, Great West Life, Canada  
Don Caniglia, FLMI, USA  
Mark Chaplin, UK  
Roger Debreceny, Ph.D., CGEIT, FCPA, University of Hawaii—Manoa, USA  
Mike Donahue, CISA, CISM, CGEIT, CFE, CGFM, CICA, Towson University, USA  
Urs Fischer, CISA, CRISC, CIA, CPA (Swiss), Switzerland  
Bob Frelinger, CISA, CGEIT, Oracle Corporation, USA  
James Golden, CISM, CGEIT, CISSP, IBM, USA  
Meenu Gupta, CISA, CISM, CBP, CISSP, CIPP, Mittal Technologies, USA  
Gary Langham, CISSP, CPFA, Australia  
Nicole Lanza, CGEIT, IBM, USA  
Philip Mark Le Grand, Prince 2, Datum International Plc, UK  
Debra Malette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, USA  
Stuart MacGregor, Real IM Solutions (Pty) Ltd., South Africa  
Christian Nissen, CISM, CGEIT, FSM, CFN People, Denmark  
Jamie Pasfield, ITIL v3, PRINCE2, Pfizer, UK  
Eddy Schuermans, Esras, Belgium  
Michael Semrau, RWE Germany, Germany  
Max Shanahan, FCPA, Max Shanahan & Associates, Australia  
Alan Simmonds, TOGAF9, UK  
Cathie Skoog, CISM, CGEIT, CRISC, IBM, USA  
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte LLP, Canada  
Roger Southgate, UK  
Nicky Tiesenga, CISA, CISM, CGEIT, IBM, USA  
Wim Van Grembergen, Ph.D., University of Antwerp Mgmt School, Belgium  
Greet Volders, CGEIT, Voquals N.V., Belgium

# COBIT 5: The Framework Exposure Draft

---

Christopher Wilken, CISA, CGEIT, PricewaterhouseCoopers LLP, USA  
Tim M. Wright, GSEC, QSA, CBCI, Kingston Smith Consulting LLP, UK

## Expert Reviewers

Mark Adler, CISA, CISM, CGEIT, Commercial Metals Company, USA  
Wole Akpose, CGEIT, Morgan State University, USA  
Krzysztof Bączkiewicz, CSAM, CSOX, Eracent, Poland  
Roland Bah, MTN Cameroon, Cameroon  
Dave Barnett, CISSP, CSSLP, USA  
Max Herman Blecher, CGEIT, Virtual Allegiance, South Africa  
Johannes Hendrik Botha, MBCS-CITP, FSM, getITright Skills Development, South Africa  
Ricardo Bria, CISA, CGEIT, Meycor GRC, Argentina  
Dirk Bruyndonckx, CISA, CISM, CGEIT, CRISC, MCA, KPMG Advisory, Belgium  
Ken Buechler, PMP, Great West Life, Canada  
Donna Cardall, UK  
Debra Chiplin, Investors Group, Canada  
Sara Cosentino, CA, Great West Life, Canada  
Philip B. de Picker, CISA, MCA, National Bank of Belgium, Belgium  
Abe Deleon, CISA, IBM, USA  
Stephen Doyle, Medicare Australia, Australia  
Heidi L. Erchinger, CISA, CRISC, CISSP, System Security Solutions Inc., USA  
Rafael Fabius, CISA, CRISC, Uruguay  
Bob Frelinger, CISA, CGEIT, Oracle Corporation, USA  
Yalcin Gerek, CISA, CGEIT, ITIL Expert, Turkey  
Edson Gin, CISA, CIPP, CFE, SSCP, USA  
James Golden, CISM, CGEIT, CISSP, IBM, USA  
Marcelo Gonzalez, Banco Central Republic Argentina, Argentina  
Erik Guldentops, University of Antwerp Management School, Belgium  
Meenu Gupta, CISA, CISM, CBP, CISSP, CIPP, Mittal Technologies, USA  
Angelica Haverblad, CGEIT, Verizon Sweden AB, Sweden  
Kim Haverblad, CISM, PCI QSA, Verizon Sweden AB, Sweden  
J. Winston Hayden, CISA, CISM, CGEIT, ITGS Consultants, South Africa  
Eduardo Hernandez, Triara, Mexico  
Jorge Hidalgo, CISA, CISM, CGEIT, Argentina  
Michelle Hoben, Media 24, South Africa  
Linda Horosko, Great West Life, Canada  
Mike Hughes, CISA, CGEIT, CRISC, 123 Consultants, UK  
Grant Irvine, Great West Life, Canada  
Monica Jain, CGEIT, CSQA, CSSBB, Southern California Edison, USA  
John Jasinski, SSBB, ITIL Service Manager, USA  
Masatoshi Kajimoto, CISA, CRISC, Japan  
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia  
Eddy Khoo, KPMG Business Advisory, Malaysia  
Marty King, CISA, CGEIT, CPA, Blue Cross Blue Shield NC, USA  
Alan S. Koch, ITIL, ASK Process Inc., USA  
Jason Lannen, CISA, CISM, TurnKey IT Solutions LLC, USA  
Nicole Lanza, CGEIT, IBM, USA  
Philip Mark Le Grand, Prince 2, Datum International Plc, UK  
Kenny Lee, CISSP, Bank of America, USA  
Brian Lind, CISA, CISM, Topdanmark Forsikring A/S, Denmark  
Bjarne Lonberg, A.P. Moller - Maersk, Denmark  
Stuart MacGregor, Real IM Solutions (Pty) Ltd., South Africa  
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK  
Cindy Marcello, CPA, FLMI, Great West Life, Canada  
Nancy McCuaig, CISSP, Great West Life, Canada  
John A. Mitchell, CFE, FBCS, UK  
Makoto Miyazaki, CISA, CPA, The Bank of Tokyo-Mitsubishi, UF, Ltd., Japan

# COBIT 5: The Framework Exposure Draft

Lucio Molina, ITIL, Colombia  
Christian Nissen, CISM, CGEIT, FSM, CFN People, Denmark  
Tony Noblett, CISA, CISM, CGEIT, CISSP, USA  
Ernest Pages, CISA, CGEIT, MCSE, eGov Consulting Services LLC, USA  
Jamie Pasfield, ITIL v3, PRINCE2, Pfizer, UK  
Thomas Patterson, CISA, CGEIT, CRISC, CPA, IBM, USA  
Robert Payne, CGEIT, MBL, MCSSA, PrM, Lode Star Strategy Consulting, South Africa  
Andre Pitkowski, CGEIT, CRISC, OCTAVE, ISO27000LA, ISO31000LA, APIT Consultoria de Informatica Ltd., Brazil  
Geert Poels, Ghent University, Belgium  
Dirk Reimers, Hewlett-Packard, Germany  
Robert Riley, CISSP, University of Notre Dame, USA  
Martin Rosenberg, Ph.D, Cloud Governance Ltd., UK  
Claus Rosenquist, CISA, CISSP, Nets, Denmark  
J Roth, CISA, CGEIT, CISSP, L-3 Communications, USA  
Cheryl Santor, CISSP, CNA, CNE, Metropolitan Water District, USA  
Eddy Schuermans, Esras, Belgium  
Michael Semrau, RWE Germany, Germany  
Max Shanahan, FCPA, Max Shanahan & Associates, Australia  
Alan Simmonds, TOGAF9, UK  
Jennifer Smith, CISA, CIA, Salt River Pima Maricopa Indian Community, USA  
Marcel Sorouni, CISA, CISM, CISSP, CCNA, Bupa Australia, Australia  
Mark Stacey, FCA, Sara Lee Corporation, Spain  
Karen Stafford-Gustin, MLIS, Great West Life, Canada  
Delton Sylvester, Silver Star IT Governance Consulting, South Africa  
Katalin Szenes, CISA, CISM, CGEIT, CISSP, University Obuda, Hungary  
Halina Tabacek, CGEIT, Oracle Americas, USA  
Nancy Thompson, CISA, CISM, CGEIT, IBM, USA  
Kazuhiro Uehara, CISA, CGEIT, Hitachi Consulting Co. Ltd., Japan  
Johan van Grieken, Deloitte, Belgium  
Flip van Schalkwyk, Provincial Government Western Cape, South Africa  
Andre Viviers, MCSE, IT Project+, Media 24, South Africa  
Greet Volders, CGEIT, Voquals N.V., Belgium  
David Williams, CISA, Westpac, New Zealand  
Tim M. Wright, GSEC, QSA, CBCI, Kingston Smith Consulting LLP, UK  
Amanda Xu, PMP, Southern California Edison, USA  
Tichaona Zororo, CISA, CISM, CGEIT, Standard Bank, South Africa

## ISACA Board of Directors

Emil D'Angelo, CISA, CISM, Bank of Tokyo Mitsubishi UFJ Ltd., USA, International President  
Christos K. Dimitriadis, Ph.D., CISA, CISM, INTRALOT S.A, Greece, Vice President  
Ria Lucas, CISA, CGEIT, Telstra Corp. Ltd., Australia, Vice President  
Hitoshi Ota, CISA, CISM, CGEIT, CRISC, CIA, GSEC (GIAC), Mizuho Corporate Bank Ltd., Japan, Vice President  
Jose Angel Pena Ibarra, CGEIT, Alintec S.A., Mexico, Vice President  
Robert E. Stroud, CGEIT, CA Technologies, USA, Vice President  
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young (retired), USA, Vice President  
Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany, Vice President  
Lynn C. Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President  
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President  
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Director  
Tony Hayes, CGEIT, AFCHE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Director  
Howard Nicholson, CISA, CGEIT, CRISC, City of Salisbury, Australia, Director  
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, USA, ITGI Trustee

## Framework Committee

Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France, Chair  
Steven A. Babb, CGEIT, KPMG, UK

# *COBIT 5: The Framework Exposure Draft*

---

Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore  
Sergio Fleginsky, CISA, Akzonobel, Uruguay  
John W. Lainhart, IV, CISA, CISM, CGEIT, IBM Global Business Services, USA  
Mario C. Micallef, CGEIT, CPAA, FIA, Ganado & Associates, Malta  
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CITP, FBCS, FISM, MInstISP, Ravenswood Consulting Ltd., UK  
Robert G. Parker, CISA, CA, CMA, FCA, Canada  
Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS, RSM Bird Cameron, Australia  
Robert E. Stroud, CGEIT, CA Technologies, USA  
Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany

## **Special Recognition**

ISACA Los Angeles Chapter for its financial support

## **ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors**

American Institute of Certified Public Accountants  
ASIS International  
The Center for Internet Security  
Commonwealth Association for Corporate Governance Inc.  
FIDA Inform  
Information Security Forum  
Institute of Management Accountants Inc.  
ISACA Chapters  
ITGI Japan  
Norwich University  
Solvay Brussels School of Economics and Management  
University of Antwerp Management School  
ASI System Integration  
Hewlett-Packard  
IBM  
SOAProjects Inc.  
Symantec Corp.  
TruArx Inc.

## Table of Contents

<b>TABLE OF FIGURES .....</b>	<b>8</b>
<b>1. INTRODUCTION AND EXECUTIVE SUMMARY.....</b>	<b>9</b>
INTRODUCTION .....	9
COBIT 5 PRINCIPLES.....	9
1. The COBIT 5 Integrator Framework .....	10
2. The Governance Objective: Stakeholder Value .....	11
3. Business Focus .....	11
4. The COBIT 5 Governance Approach—Enabler-driven .....	12
5. Governance- and Management-structured .....	13
OVERVIEW OF THIS PUBLICATION .....	14
<b>2. DRIVERS, BUSINESS BENEFITS AND KEY FEATURES OF COBIT 5 .....</b>	<b>16</b>
COBIT 5 DRIVERS .....	16
NEW CAPABILITIES AND BENEFITS OF COBIT 5 .....	16
<b>3. PRINCIPLE 1: COBIT 5 INTEGRATOR FRAMEWORK—ARCHITECTURE .....</b>	<b>19</b>
PURPOSE AND OVERVIEW OF THIS SECTION .....	19
COBIT 5 ARCHITECTURE.....	20
<b>4. PRINCIPLES 2 AND 3: STAKEHOLDER VALUE-DRIVEN AND BUSINESS-FOCUSED .....</b>	<b>22</b>
PURPOSE AND OVERVIEW OF THIS SECTION .....	22
STAKEHOLDERS AND STAKEHOLDER NEEDS VALUE? .....	22
COBIT 5 GOALS CASCADE .....	23
Step 1. Stakeholder Needs to Governance Objectives .....	25
Step 2. Governance Objectives to Enterprise Goals .....	25
Step 3. Enterprise Goals to IT-related Goals .....	26
Step 4. IT-related Goals to Enabler Goals .....	26
USING THE COBIT 5 GOALS CASCADE .....	26
Benefits of the COBIT 5 Goals Cascade .....	26
Using the COBIT 5 Goals Cascade Carefully .....	27
Using the COBIT 5 Goals Cascade .....	27
<b>5. PRINCIPLE 4: COBIT 5 ENABLERS FOR GOVERNANCE AND MANAGEMENT .....</b>	<b>28</b>
PURPOSE AND OVERVIEW OF THIS SECTION .....	28
COBIT 5 ENABLERS .....	28
SYSTEMIC GOVERNANCE .....	30
THE COBIT 5 GENERIC ENABLER MODEL.....	30
<b>6. PRINCIPLE 5: GOVERNANCE- AND MANAGEMENT-STRUCTURED .....</b>	<b>33</b>
PURPOSE AND OVERVIEW OF THIS SECTION .....	33
GOVERNANCE AND MANAGEMENT .....	33
Governance and Management Defined.....	33
Interactions between Governance and Management .....	34
COBIT 5 PROCESS REFERENCE MODEL.....	35
<b>7. IMPLEMENTATION GUIDANCE .....</b>	<b>38</b>
INTRODUCTION .....	38
CONSIDERING THE ENTERPRISE CONTEXT.....	38
CREATING THE RIGHT ENVIRONMENT .....	39
RECOGNISING PAIN POINTS AND TRIGGER EVENTS .....	39
ENABLING CHANGE .....	40
A LIFE CYCLE APPROACH .....	40
GETTING STARTED: MAKING THE BUSINESS CASE .....	42

<b>8. THE NEW COBIT 5 PROCESS CAPABILITY MODEL .....</b>	<b>44</b>
INTRODUCTION .....	44
DIFFERENCES BETWEEN COBIT 4 MATURITY MODEL AND COBIT 5 PROCESS CAPABILITY MODEL .....	44
DIFFERENCES IN PRACTICE .....	47
BENEFITS OF THE CHANGES.....	49
PERFORMING PROCESS CAPABILITY ASSESSMENTS IN COBIT 5.....	49
<b>APPENDIX A. REFERENCES .....</b>	<b>51</b>
<b>APPENDIX B. DETAILED MAPPING ENTERPRISE GOALS—IT-RELATED GOALS .....</b>	<b>52</b>
<b>APPENDIX C. DETAILED MAPPING IT-RELATED GOALS—IT-RELATED PROCESSES.....</b>	<b>54</b>
<b>APPENDIX D. STAKEHOLDER NEEDS AND ENTERPRISE GOALS .....</b>	<b>57</b>
<b>APPENDIX E. MAPPING OF COBIT 5 WITH MOST RELEVANT RELATED STANDARDS AND FRAMEWORKS .....</b>	<b>60</b>
<b>APPENDIX F. COMPARISON BETWEEN COBIT 5 INFORMATION REFERENCE MODEL AND THE COBIT 4.1     INFORMATION CRITERIA. ....</b>	<b>61</b>
<b>APPENDIX G. COBIT 5 COMPARED TO ITGI FIVE GOVERNANCE FOCUS AREAS .....</b>	<b>63</b>
<b>APPENDIX H. DETAILED DESCRIPTION OF COBIT 5 ENABLER MODELS.....</b>	<b>64</b>
OVERVIEW OF THIS SECTION.....	64
COBIT 5 PROCESS MODEL.....	65
COBIT 5 PROCESS REFERENCE MODEL.....	67
<i>Governance and Management Processes.....</i>	<i>67</i>
<i>COBIT 5 Process Reference Model .....</i>	<i>67</i>
COBIT 5 INFORMATION MODEL .....	70
<i>Introduction—The Information Cycle.....</i>	<i>70</i>
<i>COBIT 5 Information Model .....</i>	<i>70</i>
COBIT 5 ORGANISATIONAL STRUCTURES MODEL.....	75
COBIT 5 SKILLS AND COMPETENCIES MODEL .....	78
COBIT 5 PRINCIPLES AND POLICIES MODEL .....	80
COBIT 5 CULTURE, ETHICS AND BEHAVIOUR MODEL.....	82
COBIT 5 SERVICE CAPABILITIES MODEL.....	84

## Table of Figures

Figure 1—COBIT 5 Principles .....	9
Figure 2—COBIT 5 Architecture.....	10
Figure 3—The Governance Objective: Value Creation .....	13
Figure 4—Governance in COBIT 5 .....	12
Figure 5—Governance Roles, Activities and Relationships .....	13
Figure 6—COBIT 5 Benefits.....	18
Figure 7—COBIT 5 Principles: Integrator Framework.....	19
Figure 8—COBIT 5 Architecture.....	20
Figure 9—COBIT 5 Principles: Business Focus and Stakeholder Driven.....	22
Figure 10—Stakeholder Needs .....	24
Figure 11—COBIT 5 Goals Cascade Overview .....	24
Figure 12—Enterprise Goals Mapped to Governance Objectives .....	25
Figure 13—IT-related Goals.....	26
Figure 14—COBIT 5 Principles: Enabler-based .....	28
Figure 15—COBIT 5 Enablers—Systemic Model with Interacting Enablers.....	29
Figure 16—COBIT 5 Generic Enabler Model.....	30
Figure 17—COBIT 5 Principles: Generic Enabler Capability Model .....	33
Figure 18—COBIT 5 Principles: Governance- and Management-structured .....	34
Figure 19—COBIT 5 Governance and Management Interaction .....	35
Figure 20—COBIT 5 Governance and Management Processes .....	35
Figure 21—COBIT 5 Illustrative Governance and Management Processes .....	37
Figure 22—The Seven Phases of the Implementation Life Cycle .....	41
Figure 23—Summary of the COBIT 4.1 Process Maturity Model .....	45
Figure 24—Summary of the COBIT 5 Process Capability Model.....	46
Figure 25—Comparison table Maturity Levels (COBIT 4.1) and Process Capability Levels (COBIT 5) .....	48
Figure 26—Comparison table Maturity Attributes (COBIT 4.1) and Process Attributes (COBIT 5) .....	48
Figure 27—Mapping COBIT 5 Enterprise Goals to IT-related Goals .....	53
Figure 28—Mapping COBIT 5 IT-related Goals to COBIT 5 Processes .....	55
Figure 29—Mapping COBIT 5 Enterprise Goals to typical Stakeholder Needs.....	58
Figure 30—Mapping COBIT 5 IT-related Goals to typical Stakeholder Needs.....	59
Figure 31—Legacy IT Governance Focus Areas .....	63
Figure 32—COBIT 5 Coverage of Governance Focus Areas .....	66
Figure 33—COBIT 5 Generic Enabler Model (Repeat).....	64
Figure 34—COBIT 5 Process Model .....	65
Figure 35—COBIT 5 Governance and Management Processes .....	67
Figure 36—COBIT 5 Illustrative Governance and Management Processes .....	69
Figure 37—COBIT 5 Metadata—Information Cycle.....	70
Figure 38—COBIT 5 Information Model .....	70
Figure 39—COBIT 5 Organisational Structures Model .....	75
Figure 40—COBIT 5 Roles and Organisational Structures .....	76
Figure 41—COBIT 5 Skills and Competencies Model.....	78
Figure 42—COBIT 5 Skills Categories.....	79
Figure 43—COBIT 5 Principles and Policies Model.....	80
Figure 44—COBIT 5 Culture, Ethics and Behaviour Model.....	82
Figure 45—COBIT 5 Service Capabilities Model .....	84

## 1. Introduction and Executive Summary

### Introduction

**Information is a key resource for all enterprises, and throughout the whole life cycle of information there is a huge dependency on technology.** Information and related information technologies are pervasive in enterprises and they need to be governed and managed in a holistic manner, taking in the full end-to-end business and IT functional areas of responsibility.

Today, more than ever, enterprises need to achieve increased:

- Value creation through enterprise IT
- Business user satisfaction with IT engagement and services
- Compliance with relevant laws, regulations and policies

COBIT 5 is a governance and management framework for information and related technology that starts from stakeholder needs with regard to information and technology. The COBIT 5 framework is intended for all enterprises, including non-profit and public sector.

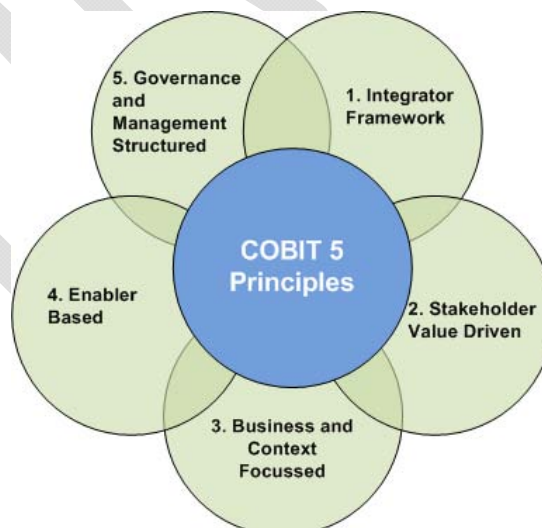
Several global business catastrophes over the last few decades have brought the term ‘governance’ to the forefront of business thinking. On the positive side, several success stories have also demonstrated the importance of good governance. Both have established a clear and widely accepted need for more rigorous governance. Increasingly, legislation is being passed and regulations implemented to address this need, which has moved governance to the top of agendas at all levels of the enterprise.

COBIT 5 allows enterprises to achieve their governance and management objectives, i.e., to create optimal value from information and technology by maintaining a balance amongst realising benefits, managing risk and balancing resources.

### COBIT 5 Principles

The COBIT framework is based on the following principles (**Figure 1**).

Figure 1—COBIT 5 Principles

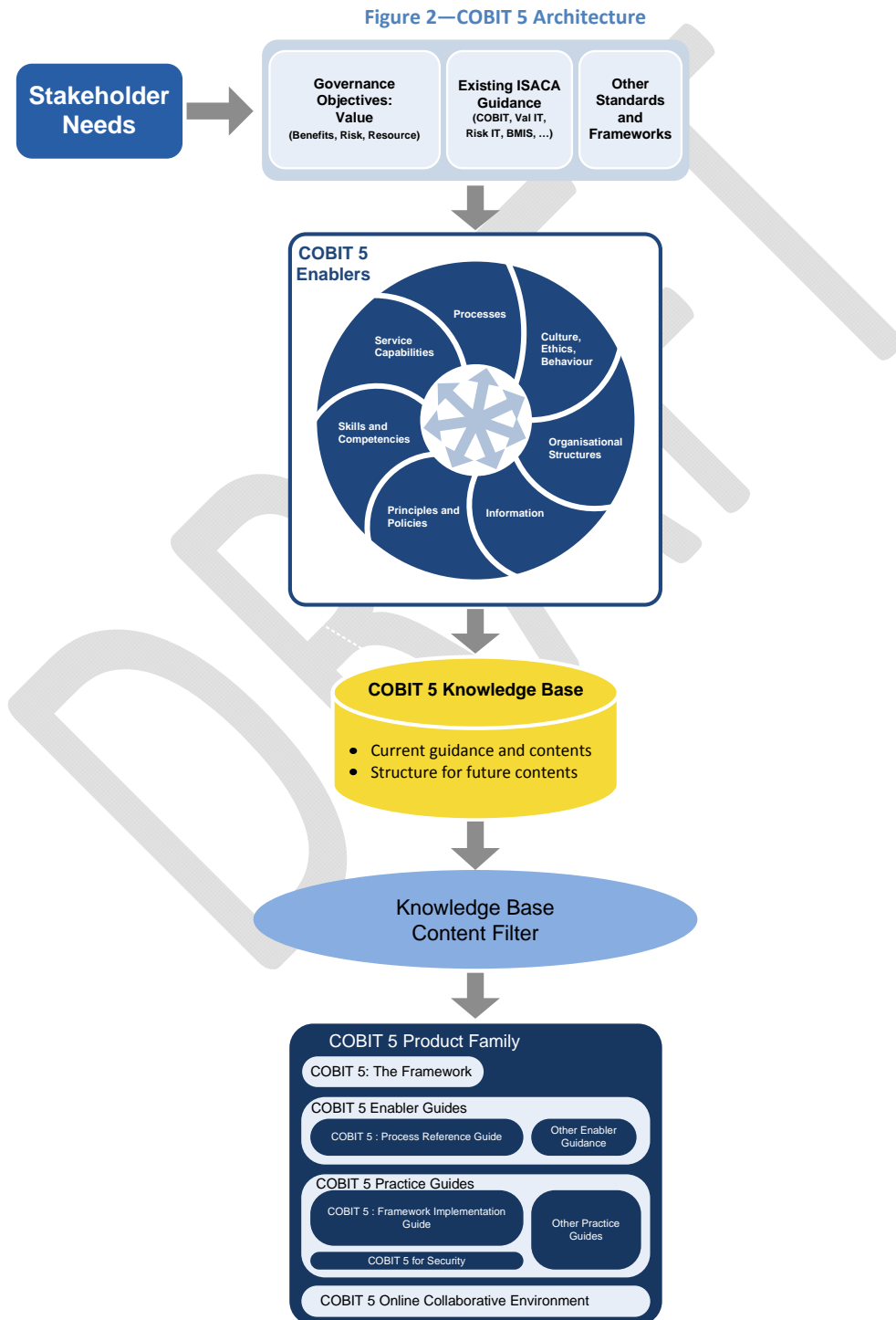


## 1. The COBIT 5 Integrator Framework

COBIT 5 is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used. A single overarching framework serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic common language.

COBIT 5 also integrates all knowledge previously dispersed over different frameworks. ISACA has researched this key area of enterprise governance for many years and has developed frameworks such as COBIT, Val IT, Risk IT, the Business Model for Information Security (BMIS) and the IT Assurance Framework (ITAF) to provide guidance and assistance to enterprises.

Figure 2 provides a graphical description of the COBIT 5 architecture that results from this principle.



The COBIT 5 framework supports governance and management of, and assurance over, enterprise IT by:

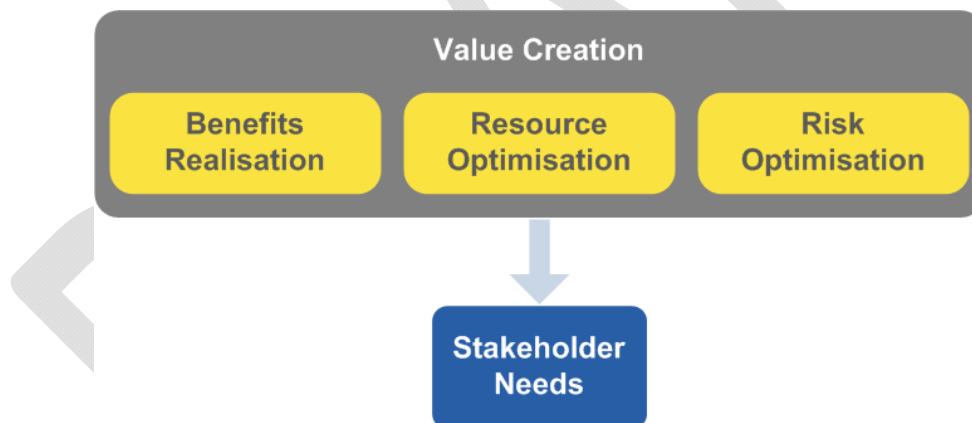
- Taking in:
  - Existing ISACA guidance (COBIT 4.1, Val IT 2, Risk IT, BMIS, etc.)
  - Other relevant standards and frameworks
  - Stakeholder needs
- Structuring guidance around a set of enabler models
- Building a consistent knowledge base for all the guidance currently created and to be created in the future
- Building a series of products from the consistent knowledge base. The first products are:
  - This volume, *COBIT 5: The Framework*
  - *COBIT 5: Process Reference Guide*
  - *COBIT 5: Implementation Guide*
- Planning a series of other products tailored for specific audiences or topics and built on filtered contents from the knowledge base

The COBIT 5 architecture is further discussed in section 3.

## 2. The Governance Objective: Stakeholder Value

Enterprises exist to create value for their stakeholders, so the governance objective for any enterprise—commercial or not—is **value creation**. Value creation means realising benefits at an optimal resource cost whilst optimising risk (see **figure 3**). Enterprises have many stakeholders, and ‘creating value’ means different—and sometimes conflicting—things to each of them. Governance is about negotiating and deciding amongst different stakeholders’ value interests. By consequence, the governance system must consider all stakeholders when making benefit, resource and risk assessments and decisions. For each of these value creation components, the question can and should be asked: for whom are the benefits, and risk, and which resources are required?

Figure 3—The Governance Objective: Value Creation



## 3. Business and Context Focus

Having a business focus means focussing on enterprise goals and objectives. This relates to every enterprise’s objective for benefits realisation, risk optimisation and resource optimisation. COBIT 5 addresses the governance and management of information and related technology from an enterprise-wide, end-to-end perspective, including the activities and responsibilities of both the IT function and non-IT business functions. The end-to-end aspect is further supported by COBIT 5 coverage of all critical business elements, i.e. processes, organisational structures, principles & policies, culture, skills, service capabilities. In addition, a new information model provides a simple link between business information and the IT function, which further supports the business focus.

Every organisation operates in a different context; this context is determined by external factors (market, industry, geopolitical, etc.) and internal factors (culture, organisation, risk appetite, etc.), and requires that every organisation builds their own, customised governance and management system. The structure of COBIT 5, the governance and management model, the enabler models apply to all contexts and facilitate this customisation, e.g., the:

- Goals cascade is the mechanism to translate context specific business drivers and stakeholder needs into specific, actionable and customised IT related and enabler goals
- Quality goals associated with each enabler are to a large extent contextual

The business focus and stakeholder value-driven nature of COBIT 5 are further discussed in section 4.

#### 4. The COBIT 5 Governance Approach—Enabler Based

The governance approach that forms the basis for COBIT 5 is shown in **Figure 4**—Governance in COBIT 5 and it represents the key components of a governance system.<sup>1</sup>

Figure 4—Governance in COBIT 5



In addition to the governance objective, the other main elements of the governance approach include the following.

#### **Governance Enablers**

Governance enablers are the organisational resources for governance, such as frameworks, principles, structure, processes and practices, toward which or through which action is directed and objectives can be attained. Enablers also include the enterprise's resources, e.g., service capabilities (IT infrastructure, applications, etc.), people and information. Given the importance of governance enablers, COBIT 5 includes a single way of looking at and dealing with enablers.

#### **Governance Scope**

Governance can be applied to the whole enterprise, an entity, a tangible or intangible asset, etc. That is, it is possible to define different views of the enterprise to which governance is applied, and it is essential to define this scope of the governance system well. The scope of COBIT 5 is an asset view—the asset being IT.

<sup>1</sup> This governance system is an illustration of ISACA's Taking Governance Forward (TGF) initiative; more information on TGF can be found on page [www.takinggovernanceforward.org/Pages/default.aspx](http://www.takinggovernanceforward.org/Pages/default.aspx).

## Roles, Activities and Relationships

A fourth element is the governance roles, activities and relationships. It defines who is involved in governance, how they are involved, what they do and how they interact, within the scope of any governance system. In COBIT 5, clear differentiation is made between governance and management activities in the governance and management domains, as well as the interfacing between them and the role players that are involved. **Figure 5** repeats the lower part of **figure 4**, but also lists the interactions between the different roles.

Figure 5—Governance Roles, Activities and Relationships



The COBIT 5 enablers and the related model are further discussed in section 6 and appendix H.

## 5. Governance- and Management-Structured

In every enterprise, multiple stakeholders have different and conflicting perceptions of benefits, risk and resources. This has made governance and management no easier task, hence a need for clarity on what should be done and how it should be done to meet the stakeholder objective.

For that reason, the COBIT 5 framework makes a clear distinction between governance and management. These two disciplines include different types of activities, require different organisational structures and serve different purposes. Since this distinction is key to COBIT 5, the following paragraphs contain the COBIT 5 view of governance and management.

### Governance

'Governance' derives from the Greek verb meaning 'to steer'. A governance system refers to all the means and mechanisms that enable multiple stakeholders in an enterprise to have an organised say in evaluating

conditions and options; setting direction; and monitoring compliance, performance and progress against plans, to satisfy specific enterprise objectives. Means and mechanisms include frameworks, principles, policies, sponsorship, structures and decision mechanisms, roles and responsibilities, processes and practices, to set direction and monitor compliance and performance aligned with the overall objectives. In most enterprises, this is the responsibility of the board of directors under the leadership of the chief executive officer (CEO) and chairman.

## Management

Often differentiated from governance as the distinction between being 'committed' (governance) and 'involved' (management), management entails the judicious use of means (resources, people, processes, practices *et al*) to achieve an identified end. It is a means or instrument by which the governance body achieves a result or objective. Management is responsible for execution within the direction set by the guiding body or unit. Management is about planning, building, organising and controlling operational activities to align with the direction set by the governance body.

The distinct governance and management structure of COBIT 5 is further discussed in section 5.

## Overview of This Publication

This publication provides an explanation of the objectives, scope and format of COBIT 5, and introduces the COBIT 5 architecture. It allows various stakeholders to understand how COBIT 5 meets the stakeholder needs for governance and management of enterprise IT and how it can be used, and it provides implementation guidance. Further sections of the document:

### Sections:

1. Describes the benefits brought to the enterprise by appropriate adoption and use of COBIT 5
2. Elaborates on Principle 1, and describes the COBIT 5 architecture
3. Elaborates on Principles 2 and 3, and describes the principal stakeholders for COBIT 5, and their needs with regard to enterprise IT and governance and management over it. It introduces the concept of enterprise goals for IT, which is used to formalise and structure the stakeholder needs. Enterprise goals can be linked to IT-related goals, and these IT-related goals can be achieved through the optimal use and execution of all enablers, including processes. This set of connecting goals is called the COBIT 5 goals cascade.
4. Elaborates on Principle 4, and describes COBIT 5 enablers. Governance of enterprise IT is systemic and supported by a set of enablers. In this section, an overall generic model for all enablers is provided.
5. Elaborates on Principle 5 and discusses the difference between management and governance, and how they interrelate. The high-level COBIT 5 process reference model is included as an example.
6. Contains an introduction to implementation guidance. It describes how the right environment can be created, the enablers required, typical pain points and trigger events for implementation, and the implementation and continual improvement life cycle. This section is based on *COBIT 5: Implementing and Continuously Improving IT Governance*, where full details on how to implement governance of enterprise IT based on COBIT 5 can be found.
7. Elaborates on the new COBIT Assessment Process (CAP) Process Assessment Model (PAM) scheme, how it differs from COBIT 4.1 process maturity assessments, and how users can migrate to the new system

**Appendices** contain reference information, mappings and more detailed information on specific subjects:

- A. References used during COBIT 5 development
- B. Detailed mapping between enterprise goals and IT-related goals, describing how typically enterprise goals are supported by one or more IT-related goals
- C. Detailed mapping between IT-related goals and COBIT 5 processes, describing how processes support the achievement of IT-related goals
- D. Mapping between stakeholder needs and enterprise goals, describing how typical stakeholder needs relate to COBIT 5 enterprise goals
- E. Mapping of COBIT 5 with most relevant related standards and frameworks
- F. Comparison between the COBIT 5 information model and the COBIT 4.1 information criteria
- G. Mapping between COBIT 5 and the five ITGI governance focus areas

## *COBIT 5: The Framework Exposure Draft*

---

- H. Detailed description of COBIT 5 enablers. This appendix builds on section 4: it includes more details on the different enablers, including a detailed enabler model describing specific components, and is illustrated with a number of examples.

Different products and other guidance covering the diverse needs of various stakeholders will be built from the main COBIT 5 knowledge base. This will happen over time, making the COBIT 5 product architecture a living document. The latest COBIT 5 product architecture can be found on the COBIT pages of the ISACA web site ([www.isaca.org/COBIT5](http://www.isaca.org/COBIT5)).

DRAFT

## 2. Drivers, Business Benefits and Key Features of COBIT 5

### COBIT 5 Drivers

COBIT 5 is a major strategic enhancement, providing the next generation of ISACA's guidance on the enterprise governance and management of IT. It builds on more than 15 years of practical usage and application of COBIT by many enterprises and users from the business, IT, risk, security and assurance communities. The major drivers for the development of COBIT 5 include:

- A need to link together and reinforce all major ISACA research, frameworks and guidance, with a primary focus on COBIT, Val IT and Risk IT, but also considering, amongst others, BMIS, ITAF, *Board Briefing on IT Governance*, and *Taking Governance Forward*
- A need to connect to, and, where relevant, align with, other major frameworks and standards in the marketplace, such as Information Technology Infrastructure Library (ITIL®), The Open Group Architecture Forum (TOGAF), Project Management Body of Knowledge (PMBOK), Projects IN Controlled Environments 2 (PRINCE2®) and the International Organization of Standards (ISO) standards. This will help stakeholders understand how various frameworks, best practices and standards are positioned relative to each other and how they can be used together and could augment each other.
- A need to provide further guidance in areas with high interest, such as enterprise architecture, asset and service management, and the management of IT innovation and emerging technologies
- A recognition that there are many current and potential users who wish to focus on specific topics, who find it difficult to navigate current material and identify content that will satisfy their requirements. There is also a general need to improve ease of use and ease of navigation and to bring consistency in concepts, terminology and the level of detail provided by ISACA.
- A need to ensure that the scope covers the full end-to-end business and IT functional responsibilities, and a need to cover all aspects that lead to effective governance and management of enterprise IT, such as organisational structures, policies, culture, etc., over and above processes. This is especially important given the increasing pervasiveness of IT and it helps increase transparency.
- A need to for the enterprise to achieve increased:
  - Value creation through enterprise IT
  - Business user satisfaction with IT engagement and services
  - Compliance with relevant laws, regulations and policies

### New Capabilities and Benefits of COBIT 5

COBIT 5 brings a substantial number of benefits to enterprises, improving on guidance previously available from ISACA. **Figure 6** summarises the business benefits offered by COBIT 5, the impacts that will bring about the benefits, and the key COBIT 5 capabilities delivering the benefits, and points to more information in the framework.

# COBIT 5: The Framework Exposure Draft

**FIGURE 6—COBIT 5 BENEFITS**

BENEFITS	IMPACTS THAT WILL BRING ABOUT THESE BENEFITS	NEW CAPABILITIES DELIVERING THIS BENEFIT	MORE INFORMATION ON THE CHANGES
<p><b>Enterprisewide benefits:</b></p> <ul style="list-style-type: none"> <li>• <b>Increased value creation through enterprise IT</b></li> <li>• <b>Increased business user satisfaction with IT engagement and services. IT seen as a key enabler.</b></li> <li>• <b>Increased compliance with relevant laws, regulations and policies</b></li> </ul>	<p>Key business impacts of COBIT 5 include:</p> <ul style="list-style-type: none"> <li>• Increased business focus on enterprise governance and management of IT. This has become a part of the enterprise's good practices.</li> <li>• Increased transparency in decision making for the enterprise governance of IT</li> </ul>	<p>COBIT 5 provides new capabilities for effective enterprise governance and management of IT:</p> <ul style="list-style-type: none"> <li>• The starting point of governance and management activities are the <b>stakeholder needs</b> related to enterprise IT.</li> <li>• Creates a more holistic, integrated and complete view of enterprise governance and management of IT that:                             <ul style="list-style-type: none"> <li>– Is consistent</li> <li>– Provides an end-to-end view on all IT-related matters</li> <li>– Provides a systemic view</li> </ul> </li> <li>• Creates a common language between IT and business for the enterprise governance and management of IT</li> </ul>	<p>Section 3 provides more information on stakeholders, their typical needs and how these can be linked to practical enabler goals in COBIT 5. This is described by means of the COBIT 5 goals cascade.</p> <p>All good-practice advice contained in COBIT 5 is consolidated into a knowledge base, combining the strengths and experiences of the guidance, research and frameworks of COBIT, Val IT, Risk IT, BMIS, ITAF and the Board Briefing.</p>
<p><b>IT function has become more business-focussed.</b></p>	<p>Key IT impacts of COBIT 5 include:</p> <ul style="list-style-type: none"> <li>• Increased agility of IT to respond to business needs</li> <li>• Increased alignment of IT tasks/activities with business need</li> <li>• Increased optimisation of IT assets and resources</li> <li>• Optimised IT-related business risk</li> <li>• Optimised cost performance of IT</li> </ul>	<ul style="list-style-type: none"> <li>• Is consistent with generally accepted corporate governance standards, and thus helps to meet regulatory requirements</li> <li>• Creates a clear distinction between governance and management of enterprise governance of IT</li> <li>• Increases the content (depth and breadth) and connection to relevant contemporary governance developments</li> <li>• Creates an integrator framework and structure for enablers (including processes) that are uniform across the enterprise for both IT and business to use</li> <li>• <b>COBIT 5 includes an information model (IM).</b> Information is a crucial enabler and key resource for the whole enterprise. Information is stored and processed by IT, but is generated, used and creates value by its business use. By providing a unique model—the IM—COBIT 5 connects the business areas with IT in the most efficient and effective way.</li> </ul>	<p>COBIT 5 is relevant to and aligned with the most important standards and frameworks, e.g., ISO/IEC 38500 and other recent global governmental and market-driven enterprise and IT governance initiatives.</p> <p>In addition, the compliance requirement is covered throughout COBIT 5, from being recognised as one of the enterprise goals to being embedded in processes and practices and other enablers.</p> <p>In <i>COBIT 5: Process Reference Guide</i>, compliance is embedded in the processes and practices.</p> <p>Introduces consistency, linkages and views with other leading frameworks and standards, e.g., generally accepted corporate governance, and standards, regulatory and compliance requirements.</p> <p>Introduces further guidance in high-interest areas for enterprise governance and management of IT, e.g., enterprise architecture, emerging technologies (e.g., cloud) and innovation.</p>

# COBIT 5: The Framework *Exposure Draft*

**FIGURE 6—COBIT 5 BENEFITS**

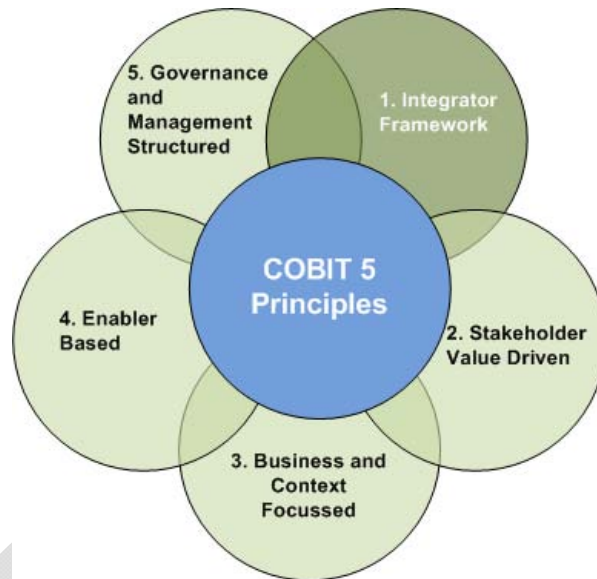
BENEFITS	IMPACTS THAT WILL BRING ABOUT THESE BENEFITS	NEW CAPABILITIES DELIVERING THIS BENEFIT	MORE INFORMATION ON THE CHANGES
			<p>In section 4 and appendix H, COBIT 5 introduces a set of principles and enablers for the enterprise governance and management of IT.</p> <p>Enablers include processes; information; people and skills; organisational structures; culture, ethics and behaviour; principles; and policies. The simple models included with COBIT for governance enablers (policies, structures, processes, etc.) are not specific for IT. They can be used to govern and manage business areas as well, thus providing a uniform way of dealing with all processes in the enterprise.</p> <p>COBIT 5 has integrated—in its enabler model—all IT-related activities an enterprise should undertake, including core IT processes and activities, but also all activities required from business stakeholders. Section 5 describes the overall enabler model.</p>
<p><b>Increases the COBIT 5 users' contribution to the enterprise</b></p>	<p>The users of COBIT 5 have the opportunity to make a greater contribution to the enterprise and enjoy an increased level of satisfaction with using COBIT 5.</p>	<p>COBIT 5 is user-focussed:</p> <ul style="list-style-type: none"> <li>• Increased access to best-practice guidance, research and frameworks on enterprise governance and management of IT</li> <li>• Increased ease of use and navigation to specific topics</li> <li>• Easier transition to and increased take-up of COBIT 5</li> <li>• COBIT 5 builds upon the strengths and experience of its predecessors, recognising that there is a significant user base that made an investment in implementing previous versions of COBIT, Val IT and Risk IT. Clear migration guidance is provided to facilitate this process.</li> </ul>	

## 3. Principle 1: COBIT 5 Integrator Framework—Architecture

### Purpose and Overview of This Section

In this section, the integrator framework principles are further discussed, as shown in **figure 7**.

Figure 7—COBIT 5 Principles: Integrator Framework

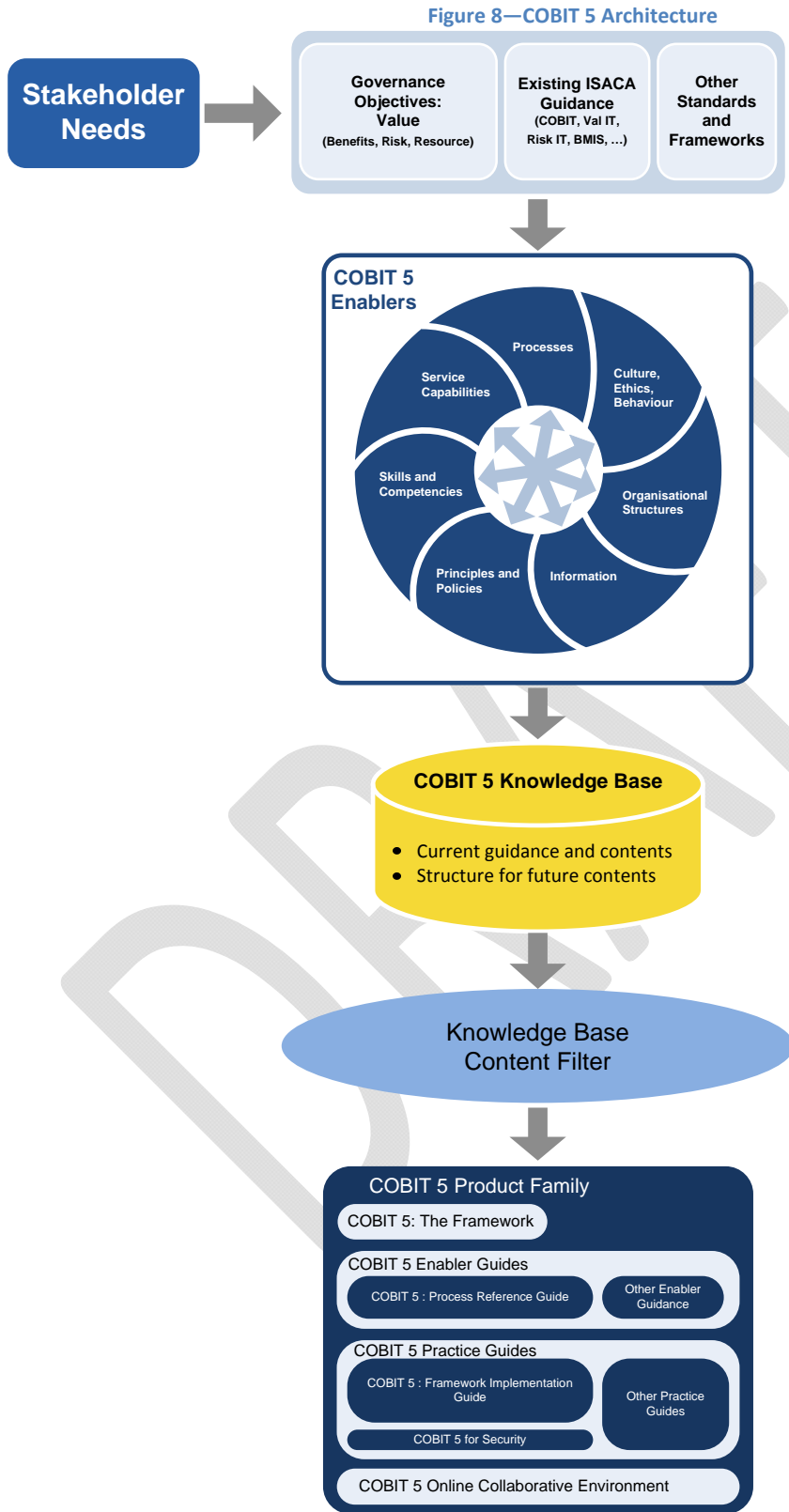


COBIT 5 is an integrator framework because it:

- Brings together existing ISACA guidance on governance and management of enterprise IT
- Aligns with the latest relevant other standards and frameworks
- Provides a simple architecture for structuring guidance materials and producing a consistent product set

## COBIT 5 Architecture

Figure 8 provides a graphical description of the COBIT 5 architecture.



The benefit of the COBIT 5 architecture is to support the COBIT 5 framework goals, i.e., providing to all stakeholders the most complete and up-to-date guidance on governance and management of enterprise IT. To achieve this benefit, the COBIT 5 architecture includes the following major components:

## COBIT 5: The Framework *Exposure Draft*

---

- A set of sources or inputs that have driven the content development, including:
  - The existing ISACA guidance (COBIT 4.1, Val IT 2, Risk IT, BMIS, etc.) in this domain, where these have been evaluated for areas needing further elaboration and updates
  - Other relevant standards and frameworks, such as ITIL, TOGAF and ISO standards. A full list of references can be found in appendix A.
  - Stakeholder needs—COBIT 5 starts from actual questions and needs all stakeholders in an enterprise may have, and provides guidance to deal with those needs.
- A set of inter-related enablers, which provide a structure for all guidance materials and a holistic view on governance and management of enterprise IT. COBIT 5 provides a simple and generic model for all enablers that facilitates dealing with the enablers in a consistent and comprehensive way.
- The COBIT 5 knowledge base to contain all guidance and content produced now and to provide a structure for additional future content
- A series of products in the COBIT 5 product family to be built from the consistent knowledge base. The first products planned are:
  - *COBIT 5: Framework*
  - *COBIT 5 Enablers: Process Reference Guide*
  - *COBIT 5: Implementing and Continuously Improving Governance of Enterprise IT*

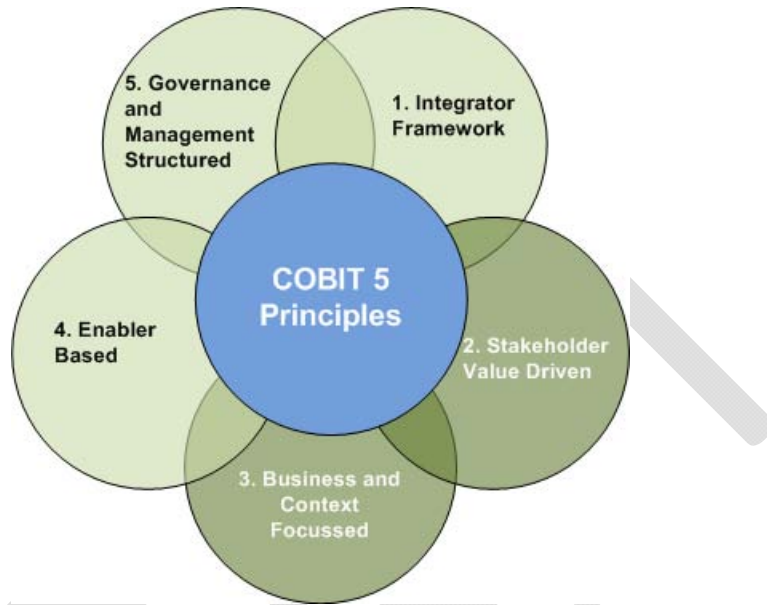
A series of other products is planned, tailored for specific audiences or topics and built on filtered contents extracted from the knowledge base.

## 4. Principles 2 and 3: Stakeholder Value-driven and Business-focused

### Purpose and Overview of This Section

In this section, the first two COBIT 5 principles—Stakeholder Value-driven and Business-focused—are further discussed, as shown in **figure 9**.

Figure 9—COBIT 5 Principles: Business Focus and Stakeholder Driven



The business focus of COBIT 5 is achieved through identifying all stakeholders and their needs and determining how they link to governance and management decisions and activities.

In this section, the typical internal and external stakeholders for Information and related technology in the enterprise are described first, along with some of their typical issues and concerns.

Next, the COBIT 5 goals cascade is described, which provides the link between stakeholder needs and practical goals by translating these into increasing level of detail and specificity: enterprise goals, IT-related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements.

### Stakeholders and Stakeholder Needs –Value?

Stakeholders for Information and related technology in an enterprise can be external and internal, and they can have many different needs—often conflicting in nature—as shown in **figure 10**.

FIGURE 10—STAKEHOLDER NEEDS	
INTERNAL STAKEHOLDERS	INTERNAL STAKEHOLDER NEEDS
Board, CEO, chief financial officer (CFO), chief information officer (CIO), business executives, business process owners, business managers, risk managers, security managers, service managers, HR managers, internal audit, privacy officers, IT users, IT managers, etc.	<ul style="list-style-type: none"> <li>• How do I get value from IT?</li> <li>• How do I manage performance of IT?</li> <li>• How can I best exploit new technology for new strategic opportunities?</li> <li>• How do I know whether I’m compliant with all applicable regulations?</li> <li>• How do I best build and structure my IT department?</li> <li>• What are (control) requirements for Information?</li> </ul>

FIGURE 10—STAKEHOLDER NEEDS

INTERNAL STAKEHOLDER NEEDS	
<b>INTERNAL STAKEHOLDERS</b>	<ul style="list-style-type: none"> <li>• Did I address all IT-related risks?</li> <li>• Am I running an efficient and resilient IT operation?</li> <li>• How do I control cost of IT? How do I use IT resources in the most effective and efficient manner? What are the most effective and efficient sourcing options?</li> <li>• Do I have enough people for IT? How do I develop and maintain their skills, and how do I manage their performance?</li> <li>• How do I get assurance over IT?</li> <li>• Is the information I am processing well secured?</li> <li>• How do I improve business agility through a more flexible IT environment?</li> <li>• Is it clear what IT is doing?</li> <li>• How often do IT projects fail to deliver what they promised?</li> <li>• How critical is IT to sustaining the enterprise?</li> </ul>
<b>EXTERNAL STAKEHOLDERS</b>	<b>EXTERNAL STAKEHOLDER NEEDS</b>
Business partners, suppliers, shareholders, regulators/government, external users, customers, standardisation organisations, external auditors, consultants, etc.	<ul style="list-style-type: none"> <li>• How do I know my business partner's operations are secure and reliable?</li> <li>• How do I know the organisation is compliant with applicable rules and regulations?</li> <li>• How do I know the enterprise is maintaining an effective system of internal control?</li> </ul>

Stakeholder needs are influenced by a number of drivers, e.g., strategy changes, a changing business and regulatory environment, and (use of) technology evolutions.

Stakeholder needs materialise in a series of potential expectations, concerns or requirements; however, all these issues relate to one or more of the three generic governance objectives within COBIT 5: benefits realisation, risk balancing and cost optimisation.

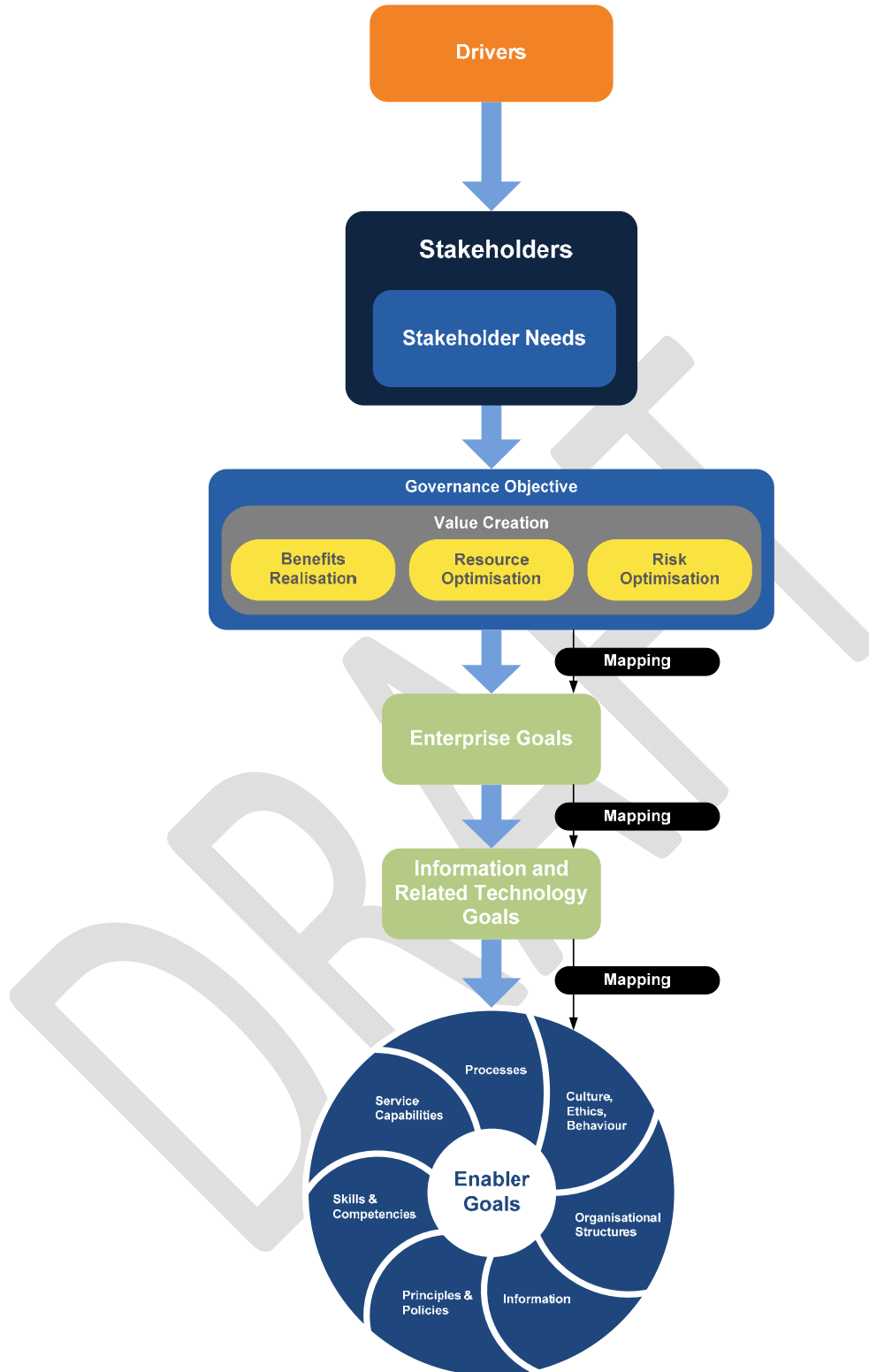
#### EXAMPLE 1

The stakeholder question 'Am I running an efficient and resilient organisation?' can be addressed by achieving the governance objectives of RESOURCE OPTIMISATION, and to some extent RISK OPTIMISATION. If those objectives are achieved, the stakeholder need will likely be addressed.

## COBIT 5 Goals Cascade

COBIT 5 stakeholders have needs relating to Information and related technology. These needs can be related to the governance objectives of any enterprise: deliver benefits, balance risk and optimise the cost of resources.

Figure 11—COBIT 5 Goals Cascade Overview



This applies to every enterprise—commercial entities, non-profit organisations, government bodies, etc. This section explains further how stakeholder concerns can be addressed by the COBIT 5 goals cascade.

The COBIT 5 goals cascade is the mechanism that will translate stakeholder concerns into goals that are more tangible and therefore can be managed more consistently. An overview of the COBIT 5 goals cascade is shown in **figure 11** and can be described as follows:

# COBIT 5: The Framework Exposure Draft

## Step 1. Stakeholder Needs to Governance Objectives

**Stakeholder issues**, which are influenced by a number of **drivers**, can be related to one or more of the **governance objectives** of benefits realisation, risk optimisation and resource optimisation.

## Step 2. Governance Objectives to Enterprise Goals

Overall **governance objectives** for the enterprise translate into and map onto a set of generic **enterprise goals**; these enterprise goals have been developed using the Balanced Scorecard (BSC)<sup>2</sup> dimensions, and they represent a list of commonly used goals an enterprise has defined for itself. Although this list is not exhaustive, most enterprise-specific goals can easily be mapped onto one or more of the generic enterprise goals. COBIT 5 defines 17 generic goals, as shown in **figure 12**, which lists the enterprise goals and how they relate to the governance objectives. In the mapping table, a 'P' stands for primary relationship, and an 'S' for secondary relationship, i.e., a less strong relationship.

**Figure 12—Enterprise Goals Mapped to Governance Objectives**

BSC DIMENSION	ENTERPRISE GOALS	GOVERNANCE OBJECTIVES		
		BENEFITS REALISATION	RISK OPTIMISATION	RESOURCE OPTIMISATION
FINANCIAL	1. STAKEHOLDER VALUE OF BUSINESS INVESTMENTS	P		
	2. PORTFOLIO OF COMPETITIVE PRODUCTS AND SERVICES	P		S
	3. MANAGED BUSINESS RISKS (SAFEGUARDING OF ASSETS)		P	S
	4. COMPLIANCE WITH EXTERNAL LAWS AND REGULATIONS		P	
	5. FINANCIAL TRANSPARENCY	P	S	S
CUSTOMER	6. CUSTOMER-ORIENTED SERVICE CULTURE	P		S
	7. BUSINESS SERVICE CONTINUITY AND AVAILABILITY		P	
	8. AGILE RESPONSES TO A CHANGING BUSINESS ENVIRONMENT	P		S
	9. INFORMATION-BASED STRATEGIC DECISION MAKING	P	P	P
	10. OPTIMISATION OF SERVICE DELIVERY COSTS	P		S
INTERNAL	11. OPTIMISATION OF BUSINESS PROCESS FUNCTIONALITY	P		P
	12. OPTIMISATION OF BUSINESS PROCESS COSTS	P		P
	13. MANAGED BUSINESS CHANGE PROGRAMMES	P	P	S
	14. OPERATIONAL AND STAFF PRODUCTIVITY	P		P
	15. COMPLIANCE WITH INTERNAL POLICIES		P	
LEARNING AND GROWTH	16. SKILLED AND MOTIVATED PEOPLE	S	S	P
	17. PRODUCT AND BUSINESS INNOVATION CULTURE	P		

### EXAMPLE 2

The enterprise goals:

- 5. FINANCIAL TRANSPARENCY relates primarily to the **benefits realisation** governance objective, but also relates in a lesser degree to both other governance objectives.
- 3. MANAGED BUSINESS RISKS (SAFEGUARDING OF ASSETS) relates primarily to the **risk optimisation** governance objective.
- 12. OPTIMISATION OF BUSINESS PROCESSES COST relates primarily to the **resource optimisation** governance objective.

### EXAMPLE 3

Looking at **figure 12** in the other direction, if risk balancing is a key governance objective for an enterprise, a number of enterprise goals will need to be prioritised:

- With highest priority:
  - 3. Managed business risks (safeguarding of assets)
  - 4. Compliance with external laws and regulations
  - 7. Business service continuity and availability
  - 9. Information-based strategic decision making
  - 13. Managed business change programmes
  - 15. Compliance with internal policies

<sup>2</sup> Kaplan, Robert S.; David P. Norton; *The Balanced Scorecard: Translating Strategy into Action*; Harvard University Press, USA, 1996

- With lower priority:
  - 5. Financial transparency
  - 16. Skilled and motivated people

### Step 3. Enterprise Goals to IT-related Goals

Realising **enterprise goals** requires a number of IT related outcomes;<sup>3</sup> these IT-related outcomes are represented by the **IT-related goals**, which are also a set of generic goals (related to IT) for business departments and for IT. Overall, COBIT 5 defines 18 IT-related goals, listed in **figure 13**.

Figure 13—IT-related Goals		
FINANCIAL	1	ALIGNMENT OF IT AND BUSINESS STRATEGY
	2	IT COMPLIANCE AND SUPPORT FOR BUSINESS COMPLIANCE WITH EXTERNAL LAWS AND REGULATIONS
	3	COMMITMENT OF EXECUTIVE MANAGEMENT FOR MAKING IT-RELATED DECISIONS
	4	MANAGED IT-RELATED BUSINESS RISKS
	5	REALISED BENEFITS FROM IT-ENABLED INVESTMENTS AND SERVICES PORTFOLIO
	6	TRANSPARENCY OF IT COSTS, BENEFITS AND RISK
CUSTOMER	7	DELIVERY OF IT SERVICES IN LINE WITH BUSINESS REQUIREMENTS
	8	ADEQUATE USE OF APPLICATIONS, INFORMATION AND TECHNOLOGY SOLUTIONS
INTERNAL	9	IT AGILITY
	10	SECURITY OF INFORMATION AND PROCESSING INFRASTRUCTURE AND APPLICATIONS
	11	OPTIMISATION OF IT ASSETS, RESOURCES AND CAPABILITIES
	12	ENABLEMENT AND SUPPORT OF BUSINESS PROCESSES BY INTEGRATING APPLICATIONS AND TECHNOLOGY INTO BUSINESS PROCESSES
	13	DELIVERY OF PROGRAMMES ON TIME, ON BUDGET, AND MEETING REQUIREMENTS AND QUALITY STANDARDS
	14	AVAILABILITY OF RELIABLE AND USEFUL INFORMATION
	15	IT COMPLIANCE WITH INTERNAL POLICIES
LEARNING AND GROWTH	16	COMPETENT AND MOTIVATED IT PERSONNEL
	17	KNOWLEDGE, EXPERTISE AND INITIATIVES FOR BUSINESS INNOVATION

The mapping table between IT-related goals and enterprise goals is included in appendix D, and it shows how each enterprise goal is supported by a number of IT-related goals.

### Step 4. IT-related Goals to Enabler Goals

For **IT-related goals** to be achieved, the successful application and use of a number of **enablers** is required; the enabler concept is explained in detail in section 5. Enablers include processes, organisational structures and information, and for each enabler a set of goals can be defined in support of the IT-related goals.

## Using the COBIT 5 Goals Cascade

### Benefits of the COBIT 5 Goals Cascade

The goals cascade is important, because it allows the definition of priorities for implementation, improvement and assurance of enterprise governance of IT based on (strategic) objectives of the enterprise. In practice, the goals cascade:

- Defines relevant and tangible goals and objectives at various levels of responsibility
- Filters the knowledge base of COBIT 5 based on enterprise goals to extract relevant guidance for inclusion in specific implementation, improvement or assurance projects
- Clearly identifies and communicates how (sometimes very operational) enablers are important to achieve enterprise goals

The goals cascade is based on research performed by the University of Antwerp Management School (UAMS) IT Alignment and Governance Institute in Belgium.

<sup>3</sup> IT-related outcomes are obviously not the only intermediate benefit required to achieve enterprise goals. All other functional areas in an organisation, such as finance and marketing, also contribute to the achievement of enterprise goals, but within the context of COBIT 5 only IT-related activities and goals are considered.

## Using the COBIT 5 Goals Cascade Carefully

The goals cascade—with its mapping tables between enterprise goals and IT-related goals and between IT-related goals and COBIT 5 processes—does not contain the universal truth, and users should not attempt to use it in a purely mechanistic way, but rather as a guideline. There are various reasons for this, including:

- Every enterprise has different priorities in its goals, and priorities may change over time.
- The mapping tables do not distinguish between size and/or industry of the enterprise. They represent a sort of common denominator of how, in general, the different levels of goals are inter-related.
- The indicators used in the mapping use two levels of importance or relevance, suggesting that there are 'discrete' levels of relevance, whereas, in reality, the mapping will be close to a continuum of various degrees of correspondence.

## Using the COBIT 5 Goals Cascade

From the above disclaimer, it is obvious that the first step an enterprise should always apply when using the goals cascade is to customise the mapping, taking into account its specific situation. For example, the enterprise may wish to:

- Translate the strategic priorities into a specific 'weight' or importance for each of the enterprise goals.
- Validate the mappings of the goals cascade, taking into account its specific environment, industry, etc.

### EXAMPLE 4

An enterprise has defined for itself a number of strategic goals, of which improving customer satisfaction is the most important. From there, it wants to know where it needs to improve in all things related to IT.

The enterprise decides that setting customer satisfaction as a key priority is equivalent to raising the priority of the following enterprise goals (from **figure 12**):

- 6. Customer-oriented service culture
- 7. Business service continuity and availability
- 8. Agile responses to a changing business environment

The enterprise now takes the next step in the goals cascade: analysing which IT-related goals correspond to these enterprise goals. A suggested mapping between them is listed in appendix B.

From there, the following IT-related goals emerge as most important:

- 1. Alignment of IT and business strategy
- 7. Delivery of IT services in line with business requirements
- 8A. User and customer satisfaction with IT services
- 4. Managed IT-related business risk
- 10. Security of information and processing infrastructure and applications
- 9. IT agility
- 17. Knowledge, expertise and initiatives for business innovation

Taking the next step in the cascade, and using the enabler concept (see section 4), these IT-related goals drive a number of enabler goals, which include process goals. In appendix C, a mapping is suggested between IT-related goals and COBIT 5 processes. This table allows identification of the most relevant IT-related processes that support the IT-related goals. But, processes alone are not sufficient: the other enablers, such as culture, behaviour and ethics; organisational structures; or skills and expertise, are equally important and require a set of clear goals.

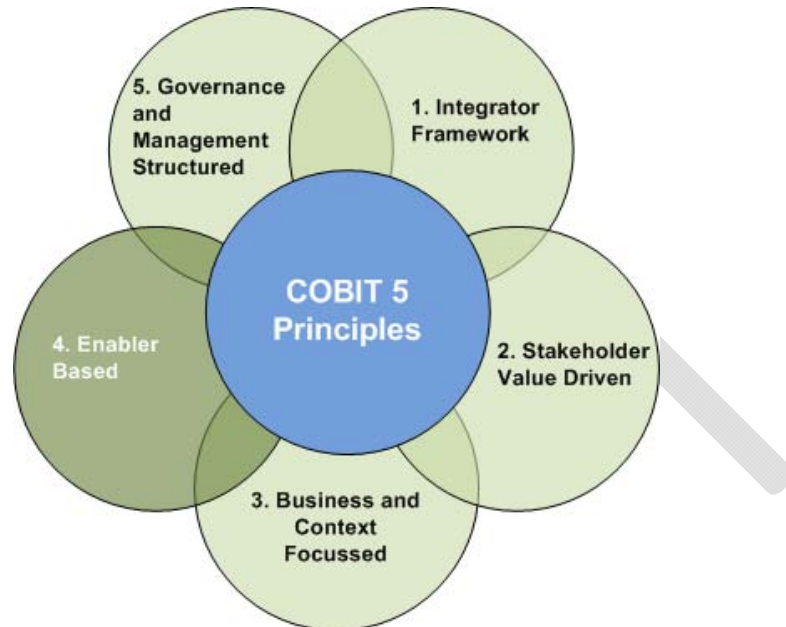
When this exercise is completed, the enterprise has a set of consistent goals for all enablers that allow it to reach the stated strategic objectives and a set of associated metrics to measure performance.

## 5. Principle 4: COBIT 5 Enabler-Based

### Purpose and Overview of This Section

In this section, the enabler-based nature of COBIT 5 is elaborated, as shown in **figure 14**.

Figure 14—COBIT 5 Principles: Enabler-based



The purpose of the enablers is—as the name suggests—implementing a performing governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the governance objectives of the enterprises. This includes resources, such as information and people. The COBIT 5 framework lists seven categories of enablers:

- Processes
- Principles and policies
- Organisational structures
- Skills and competences
- Culture and behaviour
- Service capabilities
- Information

Enablers interact in a systemic way, meaning that a governance and management system cannot succeed unless all enablers are dealt with and the major interactions are understood.

The COBIT 5 framework includes a generic model for all enablers, thus facilitating a standardised way of dealing with each.

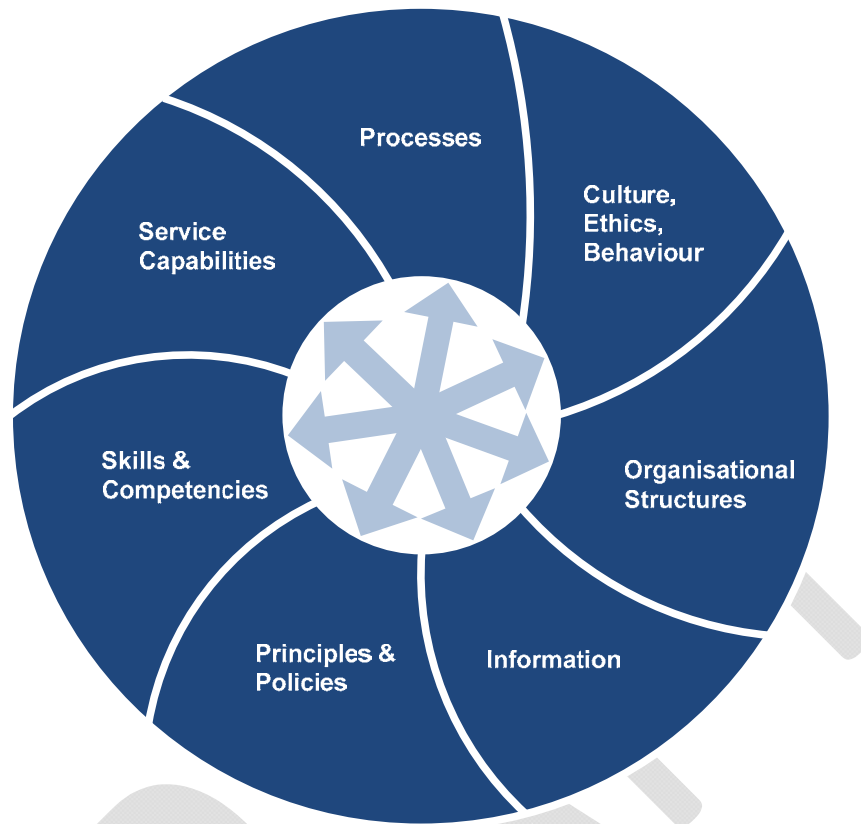
A more detailed description of each enabler is included in appendix H. The generic model is extended with specific details and examples for each enabler, allowing the user to consider all major related issues.

### COBIT 5 Enablers

Enablers are those tangible and intangible elements that make something work—in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade described in section 3: the higher-level IT-related goals define what the different enablers should achieve.

The COBIT 5 framework describes seven categories of enablers (“Enablers”) (figure 15).

Figure 15—COBIT 5 Enablers—Systemic Model With Interacting Enablers



**Figure 15** conveys the mindset that should be adopted for enterprise governance, including governance of IT, i.e., to achieve the main objectives of the enterprise, any organisation must always consider an interconnected set of enablers. **Figure 15** depicts the seven categories of enablers and the fact that they are all interconnected. The interconnections illustrate that one enabler:

- Needs the input of other enablers to be fully effective (e.g., processes need information, organisational structures need people, people need skills and behaviour, and *vice versa*)
- Delivers output to the benefit of other enablers, e.g., processes deliver information, skills and behaviour make processes efficient

The seven categories of COBIT 5 enablers for governance and management are:

- **Processes**—Describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT related goals
- **Culture, ethics, behaviour**—Of individuals and of the organisation; very often underestimated as a success factor in governance and management arrangements
- **Organisational structures**—Are the key decision-making entities in an organisation
- **Information**—Is pervasive throughout any organisation. Information is required for keeping the organisation running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- **Principles and policies**—Are the vehicle to translate the desired behaviour into practical guidance for day-to-day management
- **Skills and competences**—Are linked to people and are required for successful completion of all activities and for taking correct decisions
- **Service capabilities**—Include the infrastructure, technology and applications that provide the enterprise with information and information processing and services

## Systemic Governance

When dealing with governance of enterprise IT, good decisions can be taken only when the systemic nature of governance arrangements is taken into account. This means that to deal with any stakeholder need, all interrelated enablers have to be analysed and addressed. This mindset, illustrated in the following examples, has to be driven by the top of the organisation.

### EXAMPLE 5

Providing operational IT services to all users requires service capabilities (infrastructure, application), for which people with the right skill set and right behaviour are required. A number of service delivery processes need to be implemented as well, supported by the right organisational structures, showing how all enablers are required for successful service delivery.

### EXAMPLE 6

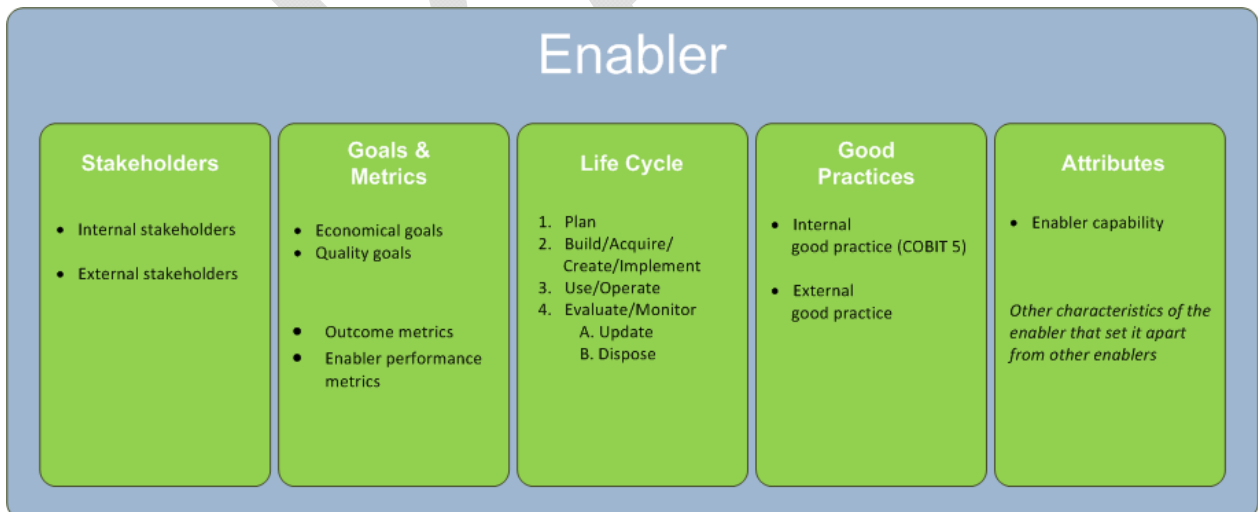
The need for information security requires a number of policies and procedures to be created and put in place. These policies, in turn, require a number of security-related practices to be implemented. However, if the organisation's and personnel's culture and ethics are not right, information security processes and procedures will not be very effective.

## The COBIT 5 Generic Enabler Model

Enablers all have certain elements in common. For that reason, a generic model is proposed to help understand and use them. A governance system is a complex interaction amongst all enablers, and having a simple, structured and uniform way to think of, and deal with, each enabler can facilitate adoption and successful execution.

Figure 16 shows the overall generic structure of the COBIT 5 enablers. This model is a key component of the COBIT 5 framework because it is the basic structure for all seven categories of enablers.

Figure 16—COBIT 5 Generic Enabler Model



The generic model identifies a number of components that are common for each enabler:

- **Stakeholders**—Each enabler has stakeholders. Processes have different parties who execute process activities and/or who have an interest in the process outcomes; organisational structures have stakeholders—each with his/her own roles and interests—that are part of the structures. Stakeholders can be internal or external to the organisation, and they all have their own interests and needs, which can be conflicting. Stakeholders needs translate to enterprise goals, which in turn translate to IT-related goals for the enterprise.

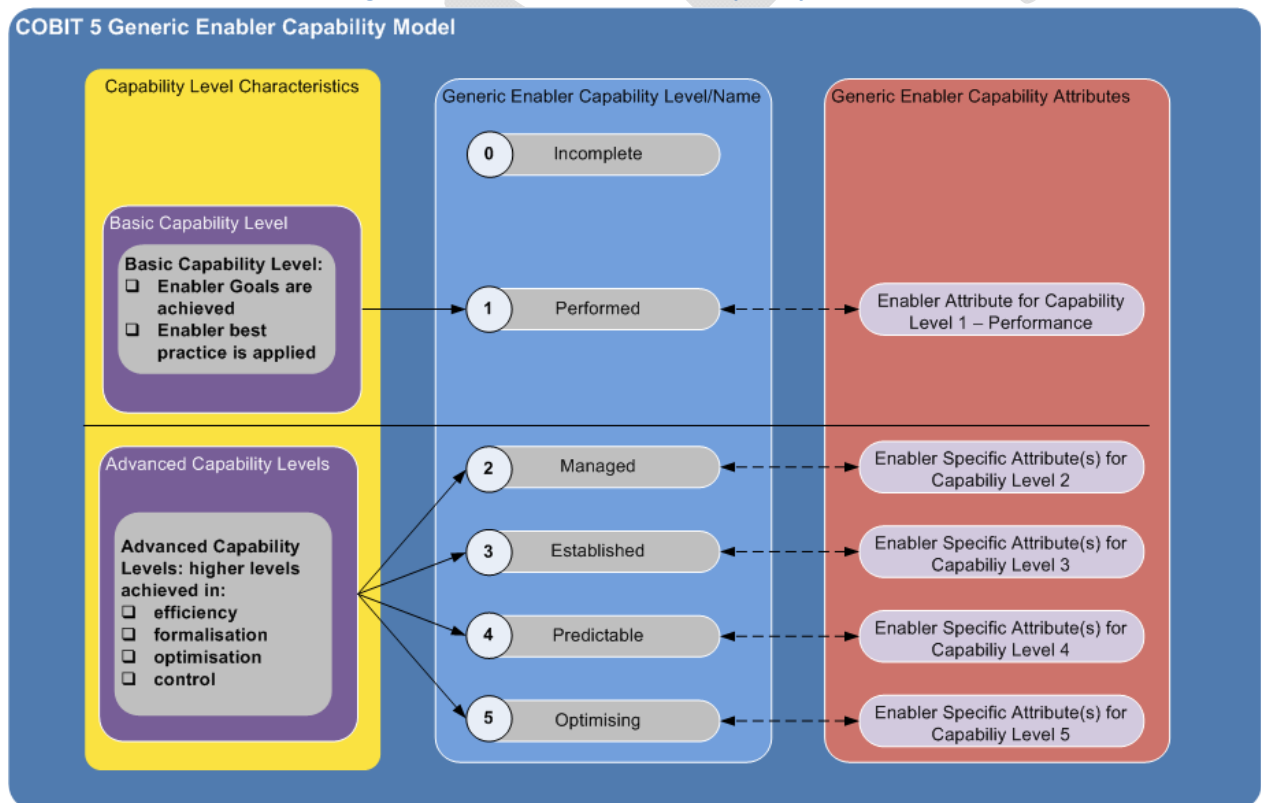
# COBIT 5: The Framework Exposure Draft

- **Goals and metrics**—Each enabler has a set of goals defining what needs to be achieved by the enabler. For processes, this translates to process goals; for information, it translates to different types of quality criteria. Goals can be **economical** (efficiency) or **quality**-related (effectiveness-oriented). Ultimately, goals have to relate to one or more of the governance objectives (benefits, risk, resource). Metrics can be associated to each goal, and they allow measurement of either how well the enabler is performing (enabler performance metrics) or to what extent the enabler goal is achieved (outcome metrics).
- **Life cycle**—Each enabler has a life cycle, from inception through an operational/useful life until disposal. This applies to information, structures, processes, policies, etc.
- **Good practice**—For each of the enablers, there exist good practices—examples or suggestions on how to best implement the enabler. For the process model, this includes all process practices and activities. Good practice can be internal (i.e., provided within the COBIT 5 framework) or external (i.e., good practice for an enabler that already exists in other standards, frameworks, etc., and can be referenced from within the COBIT 5 model).
- **Attributes**—An important attribute for each enabler is the capability attribute, allowing to evaluate the performance of an enabler. This is discussed in the next paragraph. Apart from the capability attribute, the other attributes will be specific to each enabler, e.g., organisational structures may include the type and nature of the structure (decision or organisational, horizontal or vertical) or the decision level of authority; for information, they may include code/language of the information or information type and level.

## The Capability Attribute for Enablers

The COBIT 5 generic capability attribute model is based on the principles of ISO/IEC 15504, which is a process capability assessment model (figure 17).

Figure 17—COBIT 5 Generic Enabler Capability Model



The model makes a distinction between:

- The basic capability level (Level 1-Performed), which indicates that an enabler is generally achieving its stated goals, and that enabler good practices are to a large extent applied. These two criteria—achieving goals and applying good practice—are the attribute of the performed level.
- More advanced capability levels, indicating increasing levels of sophistication in the enabler, providing greater efficiency, formalisation, control, optimisation etc. These advanced capability levels are expressed

## COBIT 5: The Framework Exposure Draft

using a scale from 2 to 5<sup>4</sup>, and for each of these levels a number of attributes will need to be achieved. These attributes are different between enablers and need to be defined per enabler.

In Section 8, the process capability model is discussed in more detail. The COBIT 5 Process Capability Model is aligned to ISO/IEC15504. The capability model for other enablers is not developed in more detail in this publication, although the principles of the model as laid out here should allow organisations to define their own specific set of attributes.

Some examples to illustrate the COBIT 5 enabler model concept follow.

### EXAMPLE 7

For processes, the stakeholders consist of all process actors, i.e., all parties that are responsible, accountable, consulted or informed (RACI) for or during process activities. A process also has goals and associated metrics that are used to measure performance of the process. A process has a life cycle, i.e., it has to be created, executed and monitored, and adjusted when required. Eventually, processes cease to exist. There is good practice for processes, which in COBIT 5 is illustrated by the detailed process guidance (see *COBIT 5: Process Reference Guide*).

### EXAMPLE 8

Organisational structures contain the same generic components. The stakeholders are the members of the organisational structures, as well as all other roles that are affected by their decisions and actions. An organisational structure can have goals and metrics defined both in terms of the expected outcomes and the way they operate. The life cycle concept is relevant as well—organisational structures are created, operational and (hopefully) improved until they cease to exist. Attributes of organisational structures include their span of control, decision rights and authority levels.

**In appendix H, the seven categories of enablers are discussed extensively via a more detailed model encompassing all major components and relations. Reading this appendix is recommended for better understanding the enablers and how powerful they can be in organising governance and management over enterprise IT.**

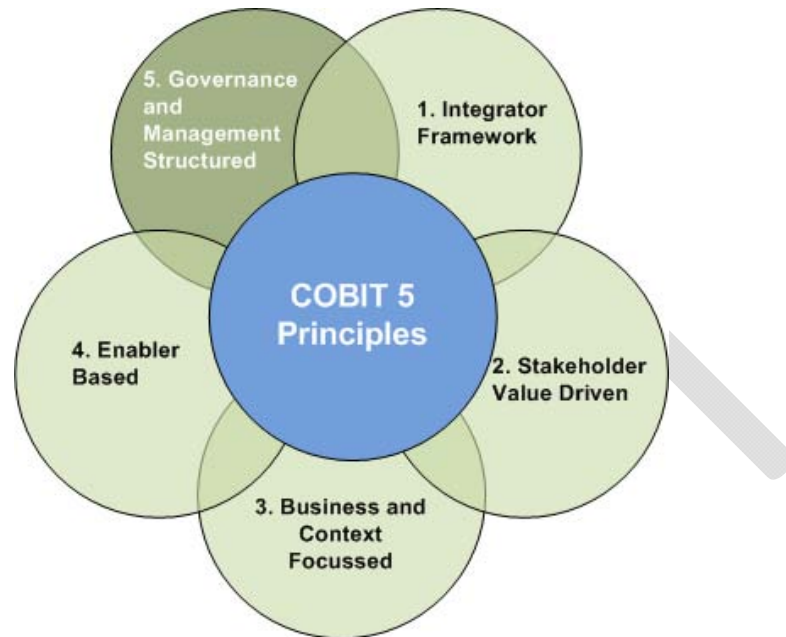
<sup>4</sup> This scale, with the names of the different levels, is taken from ISO/IEC 15504.

## 6. Principle 5: Governance- and Management-structured

### Purpose and Overview of This Section

In this section the last COBIT 5 principle—difference between management and governance (**figure 18**)—is further discussed, making a clear distinction between them.

Figure18—COBIT 5 Principles: Governance- and Management-structured



Governance and management are different types of activities and require different organisational structures. In this section, the definitions of governance and management are presented again, and an overview is included on how governance and management inter-relate and interact with each other.

The new COBIT 5 process reference model is included as an example, showing a clear distinction between governance and management processes for enterprise IT.

### Governance and Management

#### Governance and Management Defined

The COBIT 5 framework makes a clear distinction between governance and management. The two disciplines include different types of activities, require different organisational structures and serve different purposes. Since this distinction is key to COBIT 5, the following paragraphs explain the COBIT 5 view of governance and management.

#### Governance

'Governance' is derived from the Greek verb meaning 'to steer'. A governance system refers to all the means and mechanisms that enable multiple stakeholders in an enterprise to have an organised say in evaluating conditions and options; setting direction; and monitoring compliance, performance and progress against plans, to satisfy specific enterprise objectives. Means and mechanisms include frameworks, principles, policies, sponsorship, structures and decision mechanisms, roles and responsibilities, processes and practices, to set direction and monitor compliance and performance aligned with the overall objectives. In most enterprises, it is the responsibility of the board of directors under the leadership of the CEO and chairman.

## Management

Often differentiated from governance as the distinction between being ‘committed’ (governance) and ‘involved’ (management), management entails the judicious use of means (resources, people, processes, practices *et al*) to achieve an identified end. It is the means or instrument by which the governance body achieves a result or objective. Management is responsible for execution within the direction set by the guiding body or unit. Management is about planning, building, organising and controlling operational activities to align with the direction set by the governance body.

## Interactions between Governance and Management

From these definitions of governance and management, it is clear that they are different types of activities, with different responsibilities. However, given the role of governance—to evaluate, direct and monitor—a set of interactions is required between governance and management to result in an efficient and effective governance system. These interactions, using the enabler structure, include those shown in **figure 19**.

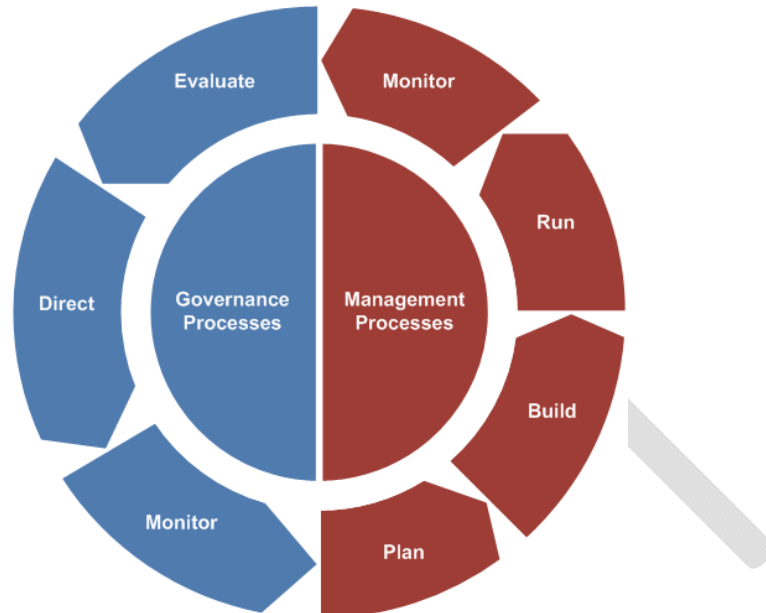
Figure 19—COBIT 5 Governance and Management Interactions

Enabler	Governance-Management Interaction
<b>Process</b>	In the illustrative COBIT 5 process model ( <i>COBIT 5: Process Reference Guide</i> ), a distinction is made between governance and management processes, including specific sets of practices and activities for each.  The process model also includes RACI charts, describing the responsibilities of different organisational structures and roles within the enterprise.
<b>Information</b>	The process model describes inputs to and outputs from the different process practices to other processes, including information exchanged between governance and management processes.
<b>Organisational Structures</b>	A number of organisational structures are defined in each organisation; structures can sit in the governance space or the management space, depending on their composition and scope of decisions. Because governance is about setting the direction, interaction takes place by the decisions taken by the governance structures, e.g., deciding about the investment portfolio and setting risk appetite.
<b>Principles and Policies</b>	Principles and policies are the vehicle by which governance decisions are institutionalised within the enterprise, and for that reason are an interaction between governance decisions (direction setting) and management (execution of decisions).
<b>Culture and Behaviour</b>	Behaviour is also a key enabler of good governance and management of the enterprise. It is set at the top—leading by example—and is therefore an important interaction between governance and management.

## COBIT 5 Process Reference Model

COBIT 5 is not prescriptive, but it is clear that it advocates that organisations implement governance and management processes such that the key areas are covered, as shown in **Figure 20**.

Figure 20—COBIT 5 Governance and Management Processes



In theory, an organisation can organise its processes as it sees fit, as long as the basic governance and management objectives are covered. Smaller organisations have fewer processes, while larger and more complex organisations may have many processes, all to cover the same objectives.

However, notwithstanding the previous paragraph, COBIT 5 includes a process reference model, which defines and describes in detail a number of governance and management processes. It represents all the processes normally found in an enterprise relating to IT activities, providing a common reference model understandable to operational IT and business managers. The proposed process model is a complete, comprehensive model, but it is not the only possible process model. Each enterprise must define its own process set, taking into account its specific situation.

Incorporating an operational model and a common language for all parts of the business involved in IT activities is one of the most important and critical steps toward good governance. It also provides a framework for measuring and monitoring IT performance, communicating with service providers, and integrating best management practices.

The COBIT 5 process reference model divides the governance and management processes of enterprise IT into two main process domains—governance and management:

- The GOVERNANCE domain, contains five governance processes; within each process, evaluate, direct and monitor practices are defined
- The four MANAGEMENT domains, in line with the responsibility areas of plan, build, run and monitor (PBRM—an evolution of the COBIT 4.1 domains), provides an end-to-end coverage of IT. Each domain contains a number of processes, as in COBIT 4.1 and in previous versions. Although—as described previously—most of the processes require ‘planning’, ‘implementation’, ‘execution’ and ‘monitoring’ activities within the process or within the specific issue being addressed (e.g., quality, security), they are placed in domains in line with what is generally the most relevant area of activity when looking at IT at the enterprise level.
- In COBIT 5, the processes also cover the full scope of business and IT activities related to the governance and management of enterprise IT, thus making the process model truly enterprisewide

## *COBIT 5: The Framework Exposure Draft*

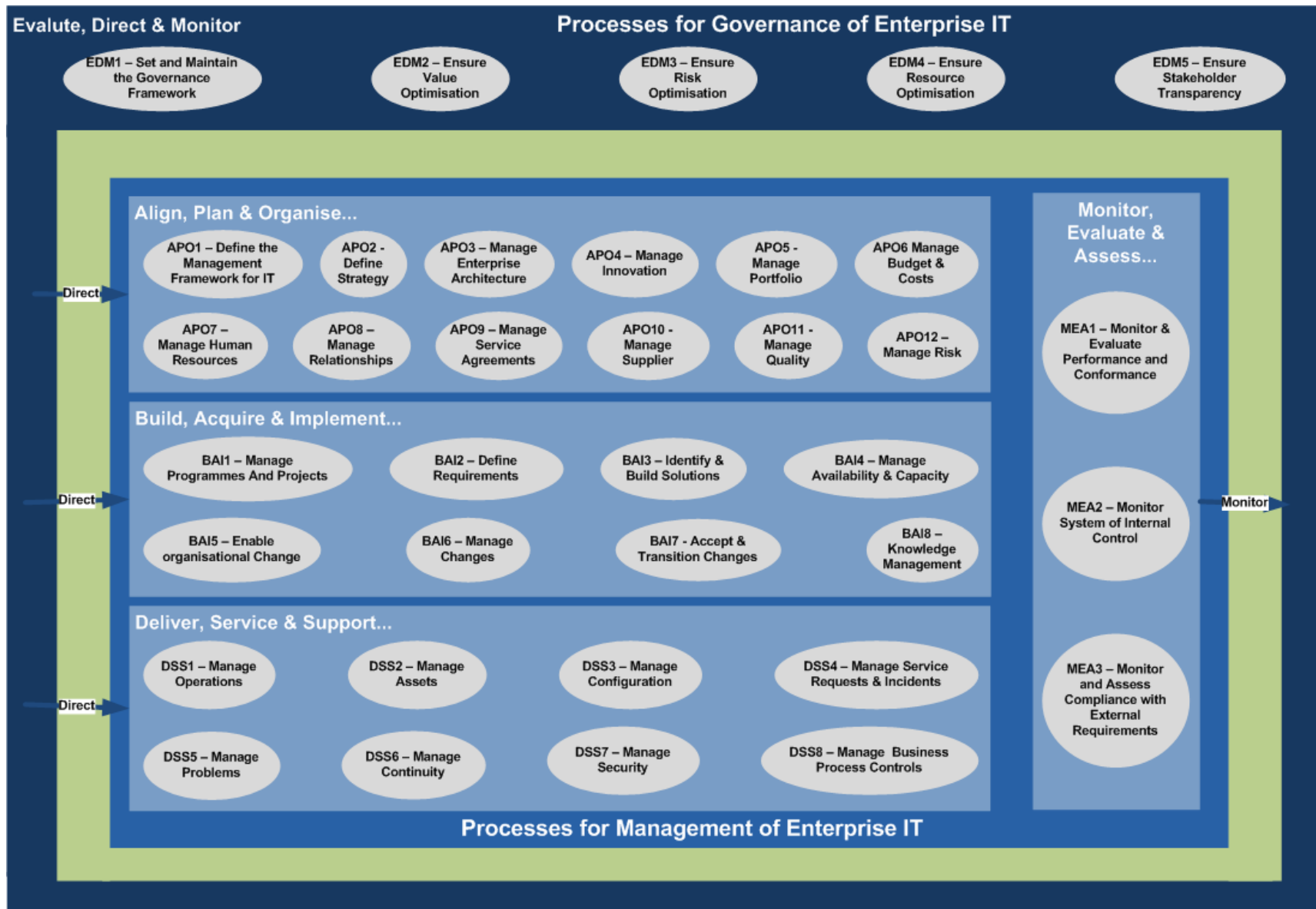
---

The COBIT 5 process reference model is the successor of the COBIT 4.1 process model, with the Risk IT and Val IT process models integrated as well. **Figure 21** shows the complete set of 36 governance and management processes within COBIT 5. The details of all processes, as per the process model described previously, are included in *COBIT 5: Process Reference Guide*.

DRAFT

# COBIT 5: The Framework *Exposure Draft*

Figure 21—COBIT 5 Illustrative Governance and Management Processes



## 7. Implementation Guidance

### Introduction

Optimal value can only be realised from leveraging COBIT if it is effectively adopted and adapted to suit each enterprise's unique environment. Each implementation approach will also need to address specific challenges including managing changes to culture and behaviour.

ISACA provides practical and extensive implementation guidance in its publication COBIT 5: *Implementation Guide*<sup>5</sup> which is based on a continual improvement life cycle. It is not intended to be a prescriptive approach nor a complete solution, but rather a guide to avoid commonly encountered pitfalls, leverage best practices and assist in the creation of successful outcomes. The guide is also supported by an implementation tool kit containing a variety of resources that will be continually enhanced. Its content includes:

- Self-assessment, measurement and diagnostic tools
- Presentations aimed at various audiences
- Related articles and further explanations

The purpose of this section is to introduce the implementation and continual improvement life cycle at a high level and to highlight a number of important topics from COBIT 5: *Implementation Guide*, such as:

- Making a business case for the implementation and improvement of the governance and management of IT
- Recognising typical pain points and trigger events
- The creation of the right environment for implementation
- Leveraging COBIT to identify gaps and guide the development of enablers such as policies, processes, principles, organisational structures and roles and responsibilities

### Considering the Enterprise Context

The governance and management of enterprise IT do not occur in a vacuum. Every enterprise needs to design its own implementation plan or road map, depending on factors in the enterprise's specific internal and external environment, such as the enterprise's:

- Ethics and culture
- Applicable laws, regulations and policies
- Mission, vision and values
- Governance policies and practices
- Business plan and strategic intentions
- Operating model and level of maturity
- Management style
- Risk appetite
- Capabilities and available resources
- Industry practices

It is equally important to leverage and build on any governance and management of IT enablers the enterprise already has in place.

The optimal approach for the governance and management of enterprise IT will be different for every enterprise, and the context needs to be understood and considered in order to adopt and adapt COBIT effectively in the implementation of governance and management of enterprise IT enablers. COBIT is often underpinned with other frameworks, best practices and standards and these too need to be adapted to suit specific requirements.

Key success factors for successful implementation include:

---

<sup>5</sup> Will provide link here when publication is available.

- Top management providing the direction and mandate for the initiative, as well as visible ongoing commitment and support
- All parties supporting the governance and management processes to understand the business and IT objectives
- Ensuring effective communication and enablement of the necessary changes
- Tailoring COBIT and other supporting best practices and standards to fit the unique context of the enterprise
- Focusing on quick wins and prioritising the most beneficial improvements that are easiest to implement

## Creating the Right Environment

It is important for implementation initiatives leveraging COBIT to be properly governed and adequately managed. Major IT-related initiatives often fail due to inadequate direction, support and oversight by the various required stakeholders, and the implementation of governance or management of IT enablers leveraging COBIT is no different. Support and direction from key stakeholders are critical so that improvements are adopted and sustained. In a weak enterprise environment (such as an unclear overall business operating model or lack of enterprise-level governance enablers), this support and participation are even more important.

Enablers leveraging COBIT should be a solution addressing real business needs and issues rather than an end in themselves. Requirements based on current pain points and drivers should be identified and accepted by management as areas that need to be addressed. High-level health checks, diagnostics or capability assessments based on COBIT are excellent tools to raise awareness, create consensus and generate a commitment to act. The commitment and buy-in of the relevant stakeholders need to be solicited from the beginning. To achieve this, implementation objectives and benefits need to be clearly expressed in business terms and summarised in an outline business case.

Once commitment has been obtained, adequate resources need to be provided to support the programme. Key programme roles and responsibilities should be defined and assigned. Care should be taken on an ongoing basis to maintain commitment from all impacted stakeholders.

Appropriate structures and processes for oversight and direction should be established and maintained. These structures and processes should also ensure ongoing alignment with enterprise-wide governance and risk management approaches.

Last, visible support and commitment should be provided by key stakeholders such as the board and executives to set the 'tone at the top' and ensure commitment for the programme at all levels.

## Recognising Pain Points and Trigger Events

There are a number of factors that may indicate a need for improved governance and management of enterprise IT.

By using pain points or trigger events as the launching point for implementation initiatives, the business case for governance or management of enterprise IT improvement can be related to practical, everyday issues being experienced. This will improve buy-in and create the sense of urgency within the organisation that is necessary to kick off the implementation. In addition, quick wins can be identified and value-add can be demonstrated in those 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.

Examples of some of the typical pain points for which new or revised governance or management of IT enablers can be a solution (or part of a solution), as identified in *COBIT 5: Implementing and Continuously Improving IT Governance*, are:

- Business frustration with failed initiatives, rising IT costs and a perception of low business value
- Significant incidents related to IT risk, such as data loss or project failure

- Outsourcing service delivery problems, such as consistent failure to meet agreed service levels
- Failure to meet regulatory or contractual requirements
- IT limiting the enterprise's innovation capabilities and business agility
- Regular audit findings about poor IT performance or reported IT quality of service problems
- Hidden and rogue IT spending
- Duplication or overlap between initiatives or wasting resources, such as premature project termination
- Insufficient IT resources, staff with inadequate skills or staff burn-out/dissatisfaction
- IT-enabled changes failing to meet business needs and delivered late or over budget
- Board members, executives or senior managers who are reluctant to engage with IT, or a lack of committed and satisfied business sponsors for IT
- Complex IT operating models

In addition to these pain points, other events in the enterprise's internal and external environment can signal or trigger a focus on the governance and management of IT. Examples of these from the guide are:

- Merger, acquisition or divestiture
- A shift in the market, economy or competitive position
- Change in business operating model or sourcing arrangements
- New regulatory or compliance requirements
- Significant technology change or paradigm shift
- An enterprise-wide governance focus or project
- A new CxO
- External audit or consultant assessments
- A new business strategy or priority

### Enabling Change

Successful implementation depends on implementing the right change (the right governance or management enablers) in the right way. In many enterprises, there is a significant focus on the first aspect—core governance or management of IT—but not enough emphasis on managing the human, behavioural and cultural aspects of the change and motivating stakeholders to buy into the change.

It should not be assumed that the various stakeholders involved in, or impacted by, new or revised enablers will 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 implementation 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.

Sustainable improvement can be achieved either by gaining the commitment of the stakeholders (investment in winning hearts and minds, in leaders' time, and in communicating and responding to the workforce) or, where still required, by enforcing compliance (investment in processes to administer, monitor and enforce). In other words, human, behavioural and cultural barriers need to be overcome so that there is a common interest to properly adopt a new way, instil a will to adopt a new way, and to ensure the ability to adopt a new way.

### A Life Cycle Approach

The implementation life cycle provides a way for enterprises to address the complexity and challenges typically encountered during implementations using COBIT. There are three inter-related components to the life cycle:

1. The core continual improvement life cycle—this is not a one-off project
2. The enablement of change (addressing the behavioural and cultural aspects)
3. The management of the programme

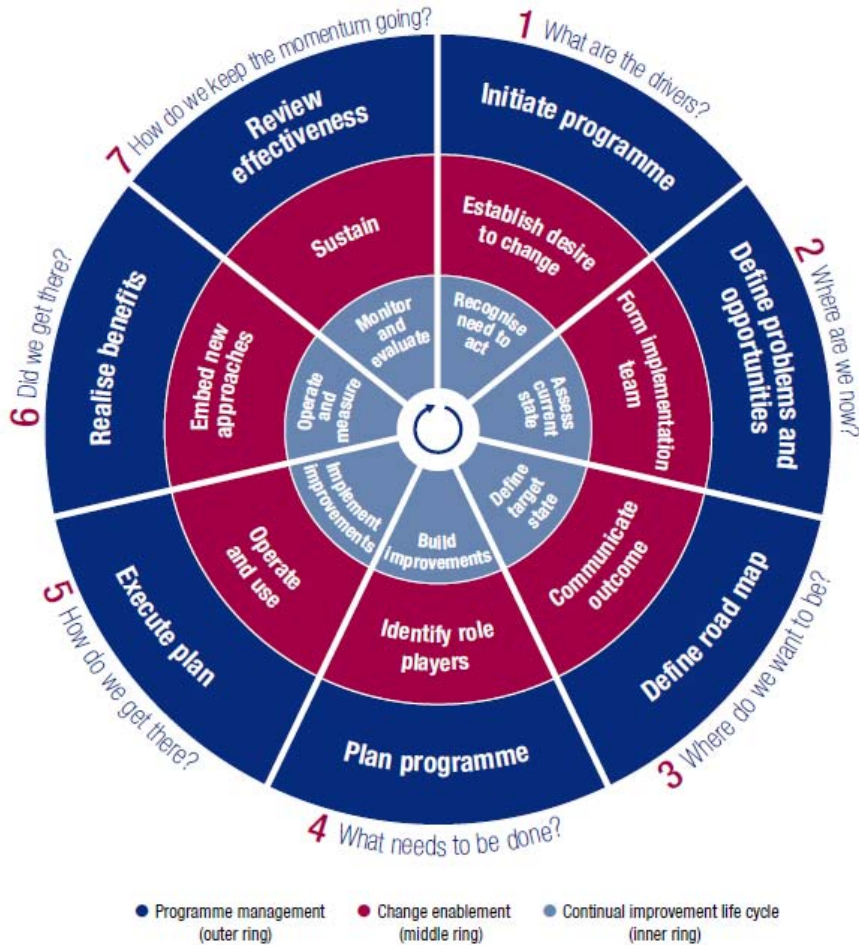
As discussed previously, the right environment needs to be created to ensure the success of the implementation or improvement initiative. The life cycle and its seven phases are illustrated in **figure 22**.

# COBIT 5: The Framework Exposure Draft

**Phase 1** starts with recognising and agreeing to the need for an implementation or improvement initiative. It identifies the current pain points and triggers and creates a desire to change at executive management levels.

**Phase 2** is focused on defining the scope of the implementation or improvement initiative using COBIT’s mapping of enterprise goals to IT-related goals to the associated IT processes. High-level diagnostics can also be useful for scoping and understanding high-priority areas on which to focus. An assessment of the current state is then performed, and issues or deficiencies are identified. This could, for example, be achieved through COBIT’s process capability assessments, as described in section 8 of this publication. Large-scale initiatives should be structured as multiple iterations of the life cycle—for any implementation initiative exceeding six months there is a risk of losing momentum, focus and buy-in from stakeholders.

Figure 22—The Seven Phases of the Implementation Life Cycle



During **phase 3**, an improvement target is set, followed by a more detailed analysis leveraging COBIT’s guidance to identify gaps and potential solutions. Some solutions may be quick wins and others more challenging and longer-term activities. Priority should be given to initiatives that are easier to achieve and those likely to yield the greatest benefits.

**Phase 4** plans practical solutions by defining projects supported by justifiable business cases. A change plan for implementation is also developed. A well-developed business case helps to ensure that the project’s benefits are identified and monitored.

The proposed solutions are implemented into day-to-day practices in **phase 5**. Measures can be defined and monitoring established, using COBIT’s goals and metrics to ensure that business alignment is achieved and maintained and performance can be measured. Success requires the engagement and demonstrated commitment of top management as well as ownership by the affected business and IT stakeholders.

**Phase 6** focuses on the sustainable operation of the new or improved enablers and the monitoring of the achievement of expected benefits.

During **phase 7**, the overall success of the initiative is reviewed, further requirements for the governance or management of enterprise IT are identified, and the need for continual improvement is reinforced.

Over time, the life cycle should be followed iteratively whilst building a sustainable approach to the governance and management of enterprise IT.

### Getting Started: Making the Business Case

To ensure the success of implementation initiatives leveraging COBIT, the need to act should be widely recognised and communicated within the enterprise. This can be in the form of a ‘wake-up call’ (where specific pain points are being experienced, as discussed previously) or an expression of the improvement opportunity to be pursued and, very important, the benefits that will be realised.

An appropriate level of urgency needs to be instilled and the key stakeholders should be aware of the risks of not taking action as well as the benefits of undertaking the programme. The initiative should be owned by a sponsor, involve all key stakeholders and be based on a business case. Initially this can be at a high level from a strategic perspective—from the top down—starting with a clear understanding of the desired business outcomes and progressing to a detailed description of critical tasks and milestones as well as key roles and responsibilities. The business case is a valuable tool available to management in guiding the creation of business value. At a minimum, the business case should include the following:

- The business benefits targeted, their alignment with business strategy and the associated benefit owners (who in the business will be responsible for securing them). This could be based on pain points and trigger events.
- The business changes needed to create the envisioned value. This could be based on health checks and capability gap analyses and should clearly state both what is in scope and what is out of scope.
- The investments needed to make the governance and management of enterprise IT changes (based on estimates of projects required)
- The ongoing IT and business costs
- The expected benefits of operating in the changed way
- The risks inherent in the previous bullets, including any constraints or dependencies (based on challenges and success factors)
- Roles, responsibilities and accountabilities related to the initiative
- How the investment and value creation will be monitored throughout the economic life cycle, and the metrics to be used (based on goals and metrics)

The business case is not a one-time static document but a dynamic operational tool that must be continually updated to reflect the current view of the future so that a view of the viability of the programme can be maintained.

It can be difficult to quantify the benefits of implementation or improvement initiatives, and care should be taken to commit only to benefits that are realistic and achievable. Studies conducted across a number of enterprises could provide useful information on benefits that have been achieved.

#### EXAMPLE 9

ITGI commissioned a market research project on the governance of IT<sup>6</sup> by PwC, with over 800 IT and business respondents in 21 countries. Thirty-eight percent of respondents cited lower IT costs as an outcome of governance of IT practices, 28.1 percent cited improved business competitiveness, and 27.1 percent indicated an improved return on IT investments. In addition, a number of less tangible benefits were reported, such as improved management of IT-related risk (42.2 percent of respondents), improved communication and relationships between business and IT (39.6 percent of respondents) and improved IT delivery of business

<sup>6</sup> ITGI, *Global Status Report on the Governance of Enterprise IT (GEIT)—2011*, USA, 2011, [www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Global-Status-Report-on-the-Governance-of-Enterprise-IT-GEIT-2011.aspx](http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Global-Status-Report-on-the-Governance-of-Enterprise-IT-GEIT-2011.aspx)

objectives (37.3 percent of respondents).

ISACA has also undertaken research that<sup>7</sup> explores and demonstrates the business value of COBIT. The dataset resulting from the research offers many analysis opportunities and clarifies the relationship between the enterprise governance of IT and business performance.

Another study conducted across 250 enterprises worldwide found that those enterprises with superior IT governance had at least 20 percent higher profitability than firms with poor governance, given the same objectives.<sup>8</sup> It argues that IT business value results directly from effective IT governance.

Finally, another case research in the airline industry concluded that the implementation and ongoing assurance of enterprise governance of IT restored trust between business and IT, and resulted in an increased alignment of investments to strategic goals. Also, more tangible benefits were reported in this case, including lowered IT continuity cost per business production unit, and the freeing up of funds for innovation. Other cross-case research in the financial sector demonstrated that organisations with better governance of IT approaches clearly obtained higher business/IT alignment maturity scores.<sup>9</sup>

DRAFT

<sup>7</sup> ISACA, *Building the Business Case for COBIT® and Val IT™ Executive Briefing*, USA, 2009, [www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Building-the-Business-Case-for-COBIT-and-Val-IT-Executive-Briefing.aspx](http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Building-the-Business-Case-for-COBIT-and-Val-IT-Executive-Briefing.aspx)

<sup>8</sup> Weill, P.; Jeanne W. Ross; *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, USA, 2004

<sup>9</sup> De Haes, Steven; Dirk Gemke; John Thorp; Wim Van Grembergen; 'Analyzing IT Value Management @ KLM Through the Lens of Val IT', *ISACA Journal*, vol. 4, USA, 2011. Van Grembergen, Wim; Steven De Haes; *Enterprise Governance of IT: Achieving Alignment and Value*; Springer, USA, 2009

## 8. The New COBIT 5 Process Capability Model

### Introduction

COBIT 4.1, Risk IT and Val IT users will be familiar with the process maturity models included in those frameworks. These models are used to measure the current or 'as-is' maturity of the enterprises' IT-related processes, to define a required 'to-be' state of maturity and to determine the gap between them and how to improve the process to achieve the desired maturity level.

The COBIT 5 product set includes a new process capability model, based on the internationally recognised ISO/IEC 15504 Software Engineering—Process Assessment standard. This model will achieve the same overall objectives of process assessment and process improvement support. However, the new model is different from the COBIT 4.1 maturity model in its design and use.

In this section, the following topics are discussed:

- Differences between the new COBIT 5 and the COBIT 4 models
- Benefits of the COBIT 5 model
- Summary of the differences COBIT 5 users will encounter in practice
- Performing a COBIT 5 capability assessment

Details of the new COBIT 5 capability assessment approach is contained in the separate document *COBIT Assessment Process (CAP): COBIT 4.1 Process Assessment Model*.<sup>10</sup>

Although this approach will provide valuable information about the state of processes, processes are one of the seven governance and management enablers. By consequence, process assessments will not provide the full picture on the state of governance of an enterprise. For that, the other enablers need to be assessed as well.

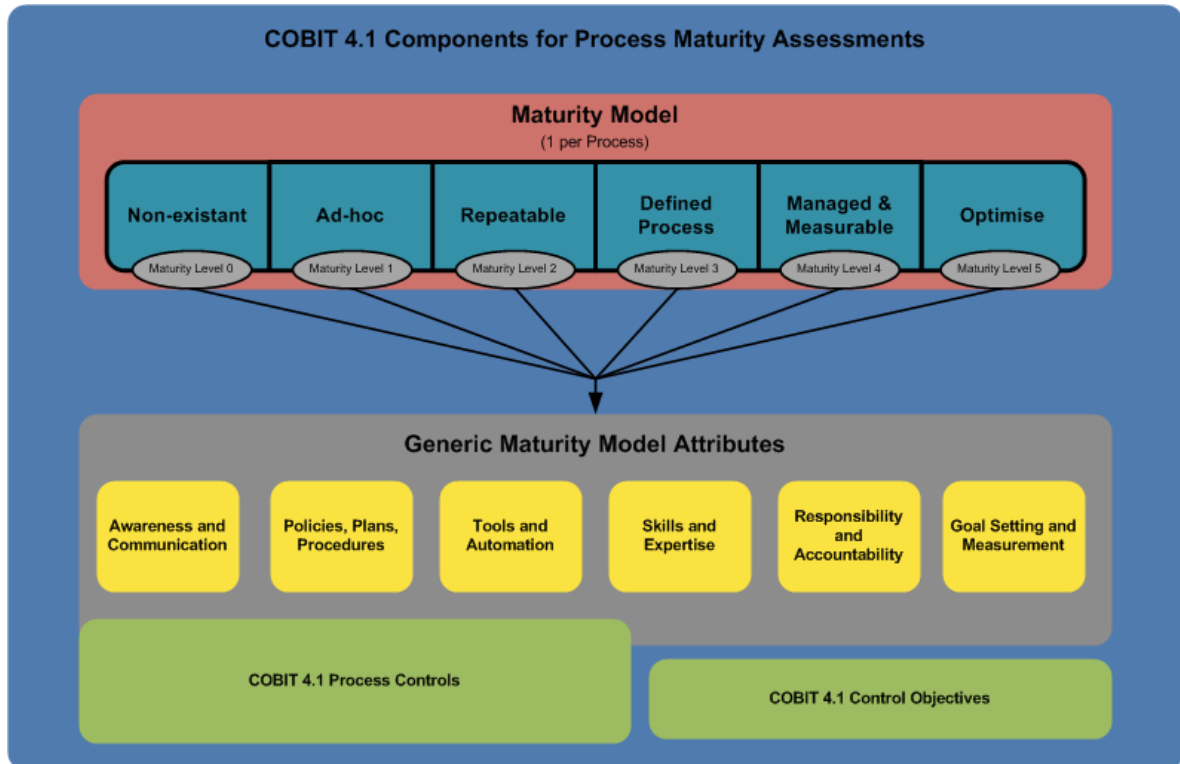
### Differences Between COBIT 4 Maturity Model and COBIT 5 Process Capability Model

The elements of the COBIT 4 maturity model approach are shown in **figure 23**. Figure contains some ampersands and some "ands." Several other errors as well.

---

<sup>10</sup> [www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Assessment-Process-CAP-COBIT-41-Process-Assessment-Model-Exposure-Draft.aspx](http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Assessment-Process-CAP-COBIT-41-Process-Assessment-Model-Exposure-Draft.aspx)

Figure 23—Summary of the COBIT 4.1 Process Maturity Model



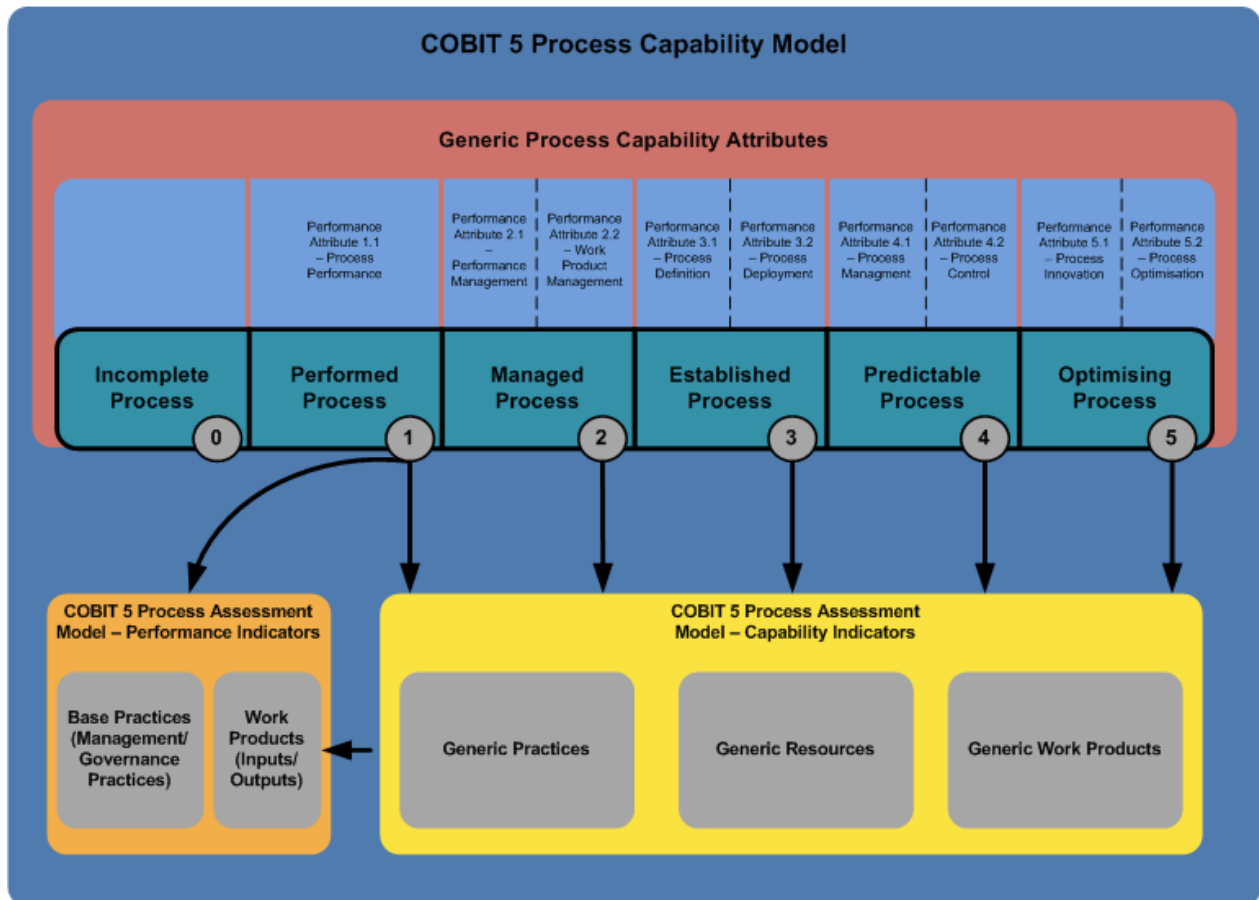
Using the COBIT 4.1 maturity model for process improvement purposes—assessing a process maturity, defining a target maturity level and identifying the gaps—required using the following COBIT 4.1 components:

- First, an assessment needed to be made whether control objectives for the process were met.
- Next, the maturity model included in the management guideline for each process could be used to obtain a maturity profile of the process.
- In addition, the generic maturity model in COBIT 4.1 provided six distinct attributes that were applicable for each process and that assisted in obtaining a more detailed view on the processes' maturity level.
- Process controls are generic control objectives—they also needed to be reviewed when a process assessment was made. Process controls partially overlap with the generic maturity model attributes.

# COBIT 5: The Framework *Exposure Draft*

The COBIT 5 process capability approach can be summarised as shown in **figure 24**.

Figure 24—Summary of the COBIT 5 Process Capability Model



The main COBIT 5 process capability model characteristics follow:

- There are six levels of capability a process can achieve, including an ‘incomplete process’ designation if the practices in it do not achieve the intended purpose of the process:
  - 0. Incomplete process**—The process is not implemented or fails to achieve its process purpose. At this level, there is little or no evidence of any systematic achievement of the process purpose.
  - 1. Performed process** (one attribute)—The implemented process achieves its process purpose.
  - 2. Managed process** (two attributes)—The previously described performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
  - 3. Established process** (two attributes)—The previously described managed process is now implemented using a defined process that is capable of achieving its process outcomes.
  - 4. Predictable process** (two attributes)—The previously described established process now operates within defined limits to achieve its process outcomes.
  - 5. Optimising process** (two attributes)—The previously described predictable process is continuously improved to meet relevant current and projected business goals.
- Each capability level can be achieved only when the level below has been fully achieved. For example, a process capability level three (established process) requires the process definition and process deployment attributes to be largely achieved, on top of full achievement of the attributes for a process capability level two (managed process).
- There is a **significant** distinction between process capability level 1 and the higher capability levels. Process capability level achievement 1 requires the process performance attribute to be largely achieved, which actually means that the process is being successfully performed and the required outcomes obtained by the enterprise. The higher capability levels then add different attributes to it. In this assessment scheme,

achieving a capability level 1, even on a scale to 5, is already an important achievement for an organisation.

The most important differences between an ISO/IEC 15504-based process capability assessment and the current COBIT 4.1 maturity model (or, for that matter, of the Val IT and Risk IT domain-based maturity models) can be summarised as follows:

- The naming and meaning of the ISO/IEC 15504-defined capability levels are quite different from the current COBIT 4.1 maturity levels for processes.
- In ISO/IEC 15504, capability levels are defined by a set of nine process attributes. These attributes cover some ground covered by the current COBIT 4 maturity attributes and/or process controls, but only to a certain extent and in a different way.
- Requirements for a ISO/IEC15504:2-compliant process reference model prescribe that in the description of any process that will be assessed (i.e., any COBIT 5 governance and/or management process):
  - The process is described in terms of its purpose and outcomes.
  - The process description shall not contain any aspects of the measurement framework beyond level 1, which means that any characteristic of a process attribute beyond level 1 cannot appear inside a process description. Whether a process is measured and monitored, or whether it is formally described, etc., cannot be part of a process description or any of the management practices/activities underneath. This means that the process descriptions—as included in *COBIT 5: Process Reference Guide*—contain only the necessary steps to achieve the actual process purpose and goals.
  - Following from the previous bullets, the common attributes applicable to all enterprise processes, which produced duplicative control objectives in COBIT 3<sup>rd</sup> Edition and were grouped into the process control objectives (PCs) in COBIT 4, are now defined in levels 2 to 5 of the assessment model.

### Differences in Practice<sup>11</sup>

From the previous descriptions, it is clear that there are some practical differences associated with the change in process assessment models. Users need to be aware of these changes and be prepared to take them into account in their action plans.

The main changes to be considered include:

- The assessment results, i.e., the numbers expressing a maturity level in COBIT 4 and a capability level in COBIT 5, **are not directly comparable and cannot be used interchangeably or mixed**. In general, scores will be lower with the COBIT 5 process capability model, as shown in **figure 25**. In the COBIT 4 maturity model, a process could achieve a level 2 or 3 without fully achieving all the process's objectives; in the new COBIT 5 process capability level, this will result in a much lower score of 0 or 1.

The COBIT 4 and COBIT 5 capability scales can be considered to 'map' approximately as shown in **figure 25**.

---

<sup>11</sup> More information on the new ISO/IEC 15504-based COBIT Assessment Program can be found at [www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Assessment-Process-CAP-COBIT-41-Process-Assessment-Model-Exposure-Draft.aspx](http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Assessment-Process-CAP-COBIT-41-Process-Assessment-Model-Exposure-Draft.aspx).

# COBIT 5: The Framework Exposure Draft

Figure 25—Comparison Table of Maturity Levels (COBIT 4.1) and Process Capability Levels (COBIT 5)

COBIT 4.1 Maturity Model Levels	COBIT 5 ISO/IEC 15504-based Capability Levels	Meaning of the COBIT 5 ISO/IEC 15504-based Capability Levels	Context
5. Optimised	5. Optimised	Continuously improved to meet relevant current and projected enterprise goals	Enterprise view/ corporate knowledge
4. Managed and measurable	4. Predictable	Operates within defined limits to achieve its process outcomes	
3. Defined	3. Established	Implemented using a defined process that is capable of achieving its process outcomes	
N/A	2. Managed	Implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained	Instance view/ individual knowledge
N/A	1. Performed	Process achieves its process purpose.	
2. Repeatable 1. Ad Hoc 0. Non-existent	0. Incomplete	Not implemented or little or no evidence of any systematic achievement of the process purpose	

- There is no longer a specific maturity model per process included with the detailed process contents in COBIT 5, because the ISO/IEC 15504 process capability assessment approach does not require this and even prohibits this approach. Instead, the approach defines the information required in the ‘process reference model’ (the process model to be used for the assessment), i.e.:
  - Process description, with the purpose statements
  - Base practices, which are the equivalent of process governance or management practices in COBIT 5 terms
  - Work products, which are the equivalent of the inputs and outputs in COBIT 5 terms
- The COBIT 4.1. maturity model produced a maturity profile of an organisation. The main purpose of this profile was to identify in which dimensions or for which attributes there were specific weaknesses that needed improvement. This approach was used by organisations when there was an improvement focus rather than a need to obtain ‘one maturity number’ for reporting purposes. In COBIT 5, the assessment model provides a measurement scale for each capability attribute and guidance on how to apply it, so for each process an assessment can be made for each of the nine capability attributes.
- The maturity attributes in COBIT 4.1 and the COBIT 5 process capability attributes are not identical. They overlap/map to a certain extent, as shown in **figure 26**. Organisations having used the maturity model attributes approach in COBIT 4.1 can re-use their existing assessment data and re-classify them under the COBIT 5 attribute assessments based on **figure 26**.

Figure 26—Comparison Table of Maturity Attributes (COBIT 4.1) and Process Attributes (COBIT 5)

COBIT 4 Maturity Attributes	COBIT 5 Process Capability Attributes									
	Process Performance	Performance Mgt.	Work Product Mgt.	Deployment	Definition	Controlled	Measured	Optimisation	Innovation	Performance
Awareness and Communication										
Policies, Processes and Procedures										
Tools and Automation										
Skills and Expertise										
Responsibility and Accountability										
Goals and Metrics										

## Benefits of the Changes

The benefits of the new COBIT 5 process capability model, compared to the COBIT 4.1 maturity models, include:

- Improved focus on the process being performed, to confirm that it is actually achieving its purpose and delivering its required outcomes as expected.
- Simplification through elimination of duplication of content, because the COBIT 4.1 maturity model assessment required the use of a number of specific components, including the generic maturity model, process maturity models, control objectives and process controls to support process assessment.
- Improved reliability and repeatability of process capability assessment activities and evaluations, reducing debates and disagreements between stakeholders on assessment results.
- Compliance with a generally accepted process assessment standard and therefore strong support for the process assessment approach in the market.
- Increased usability of process capability assessment results, as the new model establishes a basis for more formal, rigorous assessments to be performed, for both internal and potential external purposes.

## Performing Process Capability Assessments in COBIT 5

The ISO/IEC 15504 standard specifies that process capability assessments can be performed for various purposes and with varying degrees of rigour. Purposes can be internal, with a focus on comparisons between enterprise areas and/or process improvement for internal benefit, or they can be external, with a focus on formal assessment, reporting and certification.

The COBIT 5 ISO 15504-based assessment approach continues to facilitate the following objectives that have been a key COBIT management tools approach since 2000 to:

- Enable management to benchmark process capability.
- Enable high-level 'as-is' and 'to-be' health checks to support management investment decision making with regard to process improvement.
- Provide gap analysis and improvement planning information to support definition of justifiable improvement projects.
- Provide management with assessment ratings so they can measure and monitor current capabilities.

This section describes how a high-level assessment can be performed with the new COBIT 5 process capability model to achieve these objectives.

The assessment distinguishes between assessing capability level 1 and the higher levels. Indeed, as described previously, process capability level 1 describes whether a process achieves its intended purpose, and is therefore a very important level to achieve—as well as foundational in enabling higher capability levels to be reached.

Assessing whether the process achieves its goals—or, in other words, achieves capability level 1—can be done by:

1. Reviewing the process outcomes as they are described for each process in the detailed process descriptions, and using the ISO/IEC 15504 rating scale to assign a rating to which degree each objective is achieved. This scale consists of the following ratings:
  - **N** (Not achieved)—There is little or no evidence of achievement of the defined attribute in the assessed process. (0 to 15 percent achievement)
  - **P** (Partially achieved)—There is some evidence of an approach to, and some achievement of, the defined attribute in the assessed process. Some aspects of achievement of the attribute may be unpredictable. (15 to 50 percent achievement)
  - **L** (Largely achieved)—There is evidence of a systematic approach to, and significant achievement of, the defined attribute in the assessed process. Some weakness related to this attribute may exist in the assessed process. (50 to 85 percent achievement)
  - **F** (Fully achieved)—There is evidence of a complete and systematic approach to, and full achievement of, the defined attribute in the assessed process. No significant weaknesses related to this attribute exist in the assessed process. (85 to 100 percent achievement)

2. In addition, the process (governance or management) practices can be assessed using the same rating scale, expressing to which extent the base practices are applied.
3. To further refine the assessment, the work products may be taken into consideration as well to determine to which extent a specific assessment attribute has been achieved.

Although defining target capability levels is up to each enterprise to decide, many organisations will have the ambition to have all their processes achieve capability level 1 (otherwise, what would be the point of having these processes?). If this level is not achieved, the reasons for not achieving this level are immediately obvious from the approach explained above, and an improvement plan can be defined:

1. If a required process outcome is not consistently achieved, the process does not meet its objective and needs to be improved.
2. The assessment of the process practices will reveal which practices are lacking or failing, enabling implementation and/or improvement of those practices to take place and allowing all process outcomes to be achieved.

For higher process capability levels, the generic practices are used, taken from ISO/IEC 15504:2. They provide generic descriptions for each of the capability levels.

DRAFT

**Appendix A. References**

CONTENT TO BE SUPPLIED AFTER EXPOSURE.

DRAFT

## Appendix B. Detailed Mapping Enterprise Goals—IT-related Goals

The COBIT 5 goals cascade is explained in section 3. **Figure 27** contains:

- In the columns, all 17 generic enterprise goals defined in COBIT 5, grouped by BSC dimension
- In the rows, all 18 IT-related goals, also grouped in IT BSC dimensions
- A mapping on how each enterprise goal is supported by IT-related goals. This mapping is expressed using the following scale:
  - 'P' stands for primary, when there is an important relationship, i.e., the IT-related goal is a primary support for the enterprise goal.
  - 'S' stands for secondary, when there is still a strong, but less important, relationship, i.e., the IT-related goal is a secondary support for the enterprise goal.

### EXAMPLE 10

The mapping table suggests that one would normally expect that:

- Enterprise goal 7. Business service continuity and availability will:
  - Primarily depend on the achievement of the IT-related goals:
    - 4. Managed IT-related business risks
    - 10. Security of information and processing infrastructure and applications
    - 14. Availability of reliable and useful information
  - Also depend, but to a lesser degree, on the achievement of the IT-related goals:
    - 1. Alignment of IT and business strategy
    - 7. Delivery of IT services in line with business requirements
    - 8. Adequate use of applications, information and technology solutions
- Using the table in the opposite direction, achieving the IT-related goal 9. IT agility will contribute to the achievement of several enterprise goals:
  - Primarily, the enterprise goals:
    - 3. Portfolio of competitive products and services (this is #2 in fig 12)
    - 8. Agile responses to a changing business environment
    - 11. Optimisation of business process functionality
    - 17. Product and business innovation culture
  - To a lesser degree, the enterprise goals:
    - 2. Managed business risks (safeguarding of assets) (this is #3 in fig 12)
    - 4. Stakeholder value of business investments (this is #1 in fig 12)
    - 6. Customer-oriented service culture
    - 13. Managed business change programmes
    - 14. Operational and staff productivity
    - 16. Skilled and motivated people

The table was created based on the following inputs:

- Research by the University of Antwerp Management School (UAMS) IT Alignment and Governance Research Institute
- Additional reviews and expert opinions obtained during the development and review process of COBIT 5

When using this table, please keep in mind the remarks made in section 3 on how to use the COBIT 5 goals cascade.

# COBIT 5: The Framework Exposure Draft

Figure 27—Mapping COBIT 5 Enterprise Goals to IT-related Goals

			Enterprise Goals																
			Compliance with external laws and regulations	Managed business risks (safeguarding of assets)	Portfolio of competitive products and services	Stakeholder value of business investments	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
IT Related Goals			Financial				Customer				Internal				Learning & Growth				
Financial	1	Alignment of IT and business strategy		S	P	P		P	S	P	P	S	P	S	P			S	S
	2	IT compliance and support for business compliance with external laws and regulations	P	S													P		
	3	Commitment of executive management for making IT-related decisions		S	S	P				S	S		S		P			S	S
	4	Managed IT-related business risks	S	P					P	S		P			S		S	S	
	5	Realised benefits from IT-enabled investments and services portfolio			P	P		S		S		S	S	P		S			S
	6	Transparency of IT costs, benefits and risk		S		S	P				S	P		P					
Customer	7	Delivery of IT services in line with business requirements	S	S	P	P		P	S	P	S		P	S	S			S	S
	8	Adequate use of applications, information and technology solutions		S	S	S		S	S		S	S	P	S		P		S	S
Internal	9	IT agility		S	P	S		S		P			P		S	S		S	P
	10	Security of information and processing infrastructure and applications	P	P					P								P		
	11	Optimisation of IT assets, resources and capabilities			S	P				S		P	S	P	S	S			S
	12	Enablement and support of business processes by integrating applications and technology into business processes		S	P	S		S		S		S	P	S	S	S			S
	13	Delivery of programmes on time, on budget, and meeting requirements and quality standards		S	S	P		S				S		S	P	S			
	14	Availability of reliable and useful information	S	S	S	S			P		P		S						
Learning & Growth	15	IT compliance with internal policies	S	S													P		
	16	Competent and motivated IT personnel		P	S	S		S		S						P		P	S
	17	Knowledge, expertise and initiatives for business innovation			P	S		S		P	S		S		S			S	P

## Appendix C. Detailed Mapping IT-related Goals—IT-related Processes

Figure 28 contains:

- In the columns, all 18 generic IT-related goals defined in section 3, grouped in IT BSC dimensions
- In the rows, all 36 COBIT 5 processes, grouped by domain
- A mapping on how each IT-related goal is supported by a COBIT 5 IT-related process. This mapping is expressed using the following scale:
  - ‘P’ stands for primary, when there is an important relationship, i.e., the COBIT 5 process is a primary support for the achievement of an IT-related goal.
  - ‘S’ stands for secondary, when there is still a strong, but less important, relationship, i.e., the COBIT 5 process is a secondary support for the IT-related goal.

### EXAMPLE 11

The process DSS7 Manage security will contribute:

- Primarily, to the achievement of the IT-related goals:
  - 2. IT compliance and support for business compliance with external laws and regulations
  - 4. Managed IT-related business risks
  - 10. Security of information and processing infrastructure and applications
- To a lesser degree, to the achievement of the IT-related goals:
  - 1. Alignment of IT and business strategy
  - 7. Delivery of IT services in line with business requirements
  - 8. Adequate use of applications, information and technology solutions
  - 14. Availability of reliable and useful information
  - 15. IT compliance with internal policies

The table was created based on the following inputs:

- Research by the University of Antwerp Management School (UAMS) IT Alignment and Governance Research Institute
- Additional reviews and expert opinions obtained during the development and review process of COBIT 5

When using this table, please keep in mind the remarks made in section 3 on how to use the COBIT 5 goals cascade.

# COBIT 5: The Framework Exposure Draft

Figure 28—Mapping COBIT 5 IT-related Goals to COBIT 5 Processes

			IT-related Goals																
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			Alignment of IT and business strategy	IT compliance and support for business compliance with external laws and regulations	Commitment of executive management for making IT-related decisions	Managed IT-related business risks	Realised benefits from IT-enabled investments and services portfolio	Transparency of IT costs, benefits and risk	Delivery of IT services in line with business requirements	Adequate use of applications, information and technology solutions	IT agility	Security of information and processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of integrating applications and technology into business processes	Availability of reliable and useful information	IT compliance with internal policies	Competent and motivated IT personnel	Knowledge, expertise and initiatives for business innovation	
COBIT Processes			Corporate					Customer			Internal					Learning & Growth			
Evaluate, Direct & Monitor	EDM1	Set and Maintain the Governance Framework	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM2	Ensure Value Optimisation	P		S		P	P	P	S			S	S	S	S		S	P
	EDM3	Ensure Risk Optimisation	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM4	Ensure Resource Optimisation	S		S	S	S	S	S	S	P		P		S			P	S
	EDM5	Ensure Stakeholder Transparency	S	S	P			P	P						S	S	S		S
Align, Plan & Organise	APO1	Define the Management Framework for IT	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO2	Define Strategy	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO3	Manage Enterprise Architecture	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO4	Manage Innovation	P			S	P		S	P	P		P	S		S			P
	APO5	Manage Portfolio	S		S	S	P	S	S	S	S		S		P				S
	APO6	Manage Budget & Cost	S		S	S	P	P	S	S			S		S				
	APO7	Manage Human Resources	P	S	S	S			S		P	S	P		P		S	P	P
	APO8	Manage Relationships	P		S	S	S	S	P	S			S	S	S			S	S
	APO9	Manage Service Agreements	S			S	S	S	P	S	S	S	S		S	S	S		
	APO10	Manage Suppliers		S		P	S	S	S	S	S	S	S		S	S	S		S
	APO11	Manage Quality	S	S		S	S		S	S	S		S		P	S	S	S	S
	APO12	Manage Risk		P		P		P	S	S	S	P			P	S	S	S	S

# COBIT 5: The Framework Exposure Draft

Figure 28—Mapping COBIT 5 IT-related Goals to COBIT 5 Processes

			IT-related Goals																	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
COBIT Processes			Corporate					Customer			Internal						Learning & Growth			
Build, Acquire & Implement	BAI1	Manage Programmes and Projects	S		S	P	P	S	S	S			S		P			S	S	
	BAI2	Define Requirements	P	S	S	S	S		P	S	S	S	S	P	S	S			S	
	BAI3	Identify & Build Solutions	S			S	S		P	S			S	S	S	S			S	
	BAI4	Manage Availability and Capacity				S	S		S	S	S		P		S	S			S	
	BAI5	Enable Organisational Change	S		S		S		S	S	S		S	S	S			S	S	
	BAI6	Manage Changes			S	P	S		S	S	S	S	S	S	S	S	S		S	
	BAI7	Accept & Transition of Change				S	S		S	S	S			P	S	S	S		S	
	BAI8	Knowledge Management	S				S		S	S	P	S	S				S		S	P
	Deliver, Service & Support	DSS1	Manage Operations		S		P	S		S	S	S	S	P			S	S	S	S
DSS2		Manage Assets		S		S		P	S		S	S	P			S	S			
DSS3		Manage Configuration		S		S				S	S	S	S			S				
DSS4		Manage Service Requests and Incidents				P			S	S		S				S	S		S	
DSS5		Manage Problems		S		P	S		S	S	S		P	P	P	P	S		S	
DSS6		Manage Continuity	S	S		P	S		P	S	S	S	S			P	S	S	S	
DSS7		Manage Security	S	P		P			S	S		P				S	S			
DSS8		Manage Business Process Controls		S		P			P	S		S		S		S	S	S	S	
Monitor, Evaluate & Assess	MEA1	Monitor and Evaluate Performance and Conformance	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S	
	MEA2	Monitor System of Internal Control		P		P		S	S	S		S				S	P		S	
	MEA3	Monitor and Evaluate Compliance with External Requirements		P		P	S		P			S					S		S	

## Appendix D. Stakeholder Needs and Enterprise Goals

COBIT 5 defines a list of enterprise goals; these enterprise goals are a proxy for the stakeholder needs and, at the same time, are a next level of detail of the overall governance objectives shown in section 1. Section 3 showed the individual steps of the goals cascade, but from a stakeholder point of view it is also interesting to know how stakeholder needs relate to the enterprise goals and to the IT-related goals. For that reason the following tables are included:

- **Figure 29** shows how a (non-limitative) list of stakeholder needs can be linked to the enterprise goals.
- **Figure 30** shows how the same list of stakeholder needs can also be linked to the IT-related goals.

DRAFT

# COBIT 5: The Framework *Exposure Draft*

Figure 29—Mapping COBIT 5 Enterprise Goals to Typical Stakeholder Needs

	ENTERPRISE GOAL																
	Compliance with external laws and regulations	Managed business risks (safeguarding of assets)	Portfolio of competitive products and services	Stakeholder value of business investments	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
STAKEHOLDER CONCERN	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
How do I know whether I'm compliant with all applicable regulations?																	
How do I best build and structure my IT department?																	
What are (control) requirements for information?																	
Did I address IT-related risk?																	
Am I running an efficient and resilient IT operation?																	
How do I control the cost of IT?																	
How do I know I'm getting value from IT?																	
Do I have enough people for IT?																	
How do I develop and maintain skills?																	
How do I manage (people) performance?																	
How do I get assurance over IT?																	
Is the information I am processing well secured?																	
How do I improve business agility through a more flexible IT environment?																	
Is it clear what IT is doing?																	
How often do IT projects fail to deliver what they promised?																	
How critical is IT to sustaining the enterprise?																	
How do I know my business partner's operations are secure and reliable?																	
How do I know the organisation is compliant with applicable rules and regulations?																	
How do I know the enterprise is maintaining an effective system of internal control?																	

# COBIT 5: The Framework *Exposure Draft*

Figure 30—Mapping COBIT 5 IT-related Goals to Typical Stakeholder Needs

	IT-RELATED GOALS																
	Alignment of IT and business strategy	IT compliance with external laws and regulations	Commitment of executive management	Realisation of benefits across IT enabled investment portfolio	Managed IT related business risks	IT costs, benefits and risks transparency	Reliability and security of IT services	IT services in line with business requirements	Proper use of applications, information and technology solutions	Security of information and processing infrastructure	Delivery of programmes on time and on budget that meet quality standards	IT agility	Optimisation of IT infrastructure, resources and capabilities	Availability of reliable and useful information	Integration of applications and technology into business processes	Skilled and motivated IT people	Knowledge and expertise in emerging technologies for business innovation
STAKEHOLDER CONCERN	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
How do I know whether I'm compliant with all applicable regulations?																	
How do I best build and structure my IT department?																	
What are (control) requirements for information?																	
Did I address IT-related risk?																	
Am I running an efficient and resilient IT operation?																	
How do I control the cost of IT?																	
How do I know I'm getting value from IT?																	
Do I have enough people for IT?																	
How do I develop and maintain skills?																	
How do I manage (people) performance?																	
How do I get assurance over IT?																	
Is the information I am processing well secured?																	
How do I improve business agility through a more flexible IT environment?																	
Is it clear what IT is doing?																	
How often do IT projects fail to deliver what they promised?																	
How critical is IT to sustaining the enterprise?																	
How do I know my business partner's operations are secure and reliable?																	
How do I know the organisation is compliant with applicable rules and regulations?																	
How do I know the enterprise is maintaining an effective system of internal control?																	

**Appendix E. Mapping of COBIT 5 With Most Relevant Related Standards and Frameworks**

CONTENT TO BE SUPPLIED AFTER EXPOSURE

## Appendix F. Comparison Between COBIT 5 Information Model and the COBIT 4.1 Information Criteria.

How do the seven information criteria of COBIT 4.1—efficiency, effectiveness, integrity, reliability, availability, confidentiality, reliability—relate to the information quality categories and dimensions of the COBIT 5 IM?

This relationship can best be explored through the Product and Service Performance model for Information Quality (PSP/IQ). The PSP/IQ model uses the same quality dimensions as the IM, but organises them using a different 2 times 2 categorisation (on one dimension, product vs. service, and on the other dimension, conforming specifications vs. meeting/exceeding customer expectations) resulting in four information quality categories: soundness, dependability, usefulness, usability:

- Information as a product = focus on activities needed to put and maintain data in a database
- Information as a service = focus on activities needed to obtain and use information
- Conforming specifications = quality perspective that is taken mainly by information producers and custodians
- Meeting/exceeding customer expectations = quality perspective that is taken mainly by product/service designers and marketing professionals

The following table defines these information quality categories. Shouldn't this and the table below have figure numbers?

	<b>Conforms to Specifications</b>	<b>Meets or Exceeds Consumer Expectations</b>
<b>Product Quality</b>	<u>Sound Information</u> The characteristics of the information supplied meet IQ standards.	<u>Useful Information</u> The information supplied meets information consumer task needs.
<b>Service Quality</b>	<u>Dependable Information</u> The process of converting data into information meets standards.	<u>Usable Information</u> The process of converting data into information exceeds information consumer needs.

numbers?

The next table shows the PSP/IQ model and how the information quality criteria fit in each of the quadrants.

The PSP/IQ model

	Conforms to specifications	Meets or exceeds consumer expectations
Product Quality	Sound information IQ dimensions Free-of-error Concise representation Completeness Consistent representation	Useful information IQ dimensions Appropriate amount Relevancy Understandability Interpretability Objectivity
Service Quality	Dependable information IQ dimensions Timeliness Security	Usable information IQ dimensions Believability Accessibility Ease of operation Reputation

The COBIT information criteria can now be mapped to IM information quality:

- **Effectiveness**—Information is effective if it meets the needs of the information consumer who uses the information for a specific task. If the information consumer can perform the task with the information, then the information is effective. This corresponds to the information quality category usefulness in the PSP/IQ (i.e., effectiveness is usefulness).
- **Efficiency**—Whereas effectiveness considers the information as a product, efficiency relates more to the process of obtaining and using information, so it aligns to the 'information as a service' view. If information that meets the needs of the information consumer is obtained and used in an easy way (i.e., it takes few resources—physical effort,

cognitive effort, time, money), then the use of information is efficient. This matches the information quality category usability in the PSP/IQ (i.e., efficiency *is* usability), as well as the economical goals in COBIT 5.

- **Integrity**—If information has integrity, then it is free of error. Integrity is an attribute of the accuracy/free-of-error information quality dimension, which is in the PSP/IQ part of the soundness category (i.e., integrity *is part of* free-of-error).
- **Reliability**—Reliability is often seen as a synonym of accuracy; however, it can also be said that information is reliable if it is regarded as true and credible. Compared to integrity, reliability is more subjective, more related to perception, and not just factual. In the PSP/IQ, reliability is called believability, which is a dimension of the usability category (i.e., reliability *is* believability).
- **Availability**—Availability is an attribute of accessibility, which the PSP/IQ defines as the extent to which information is available or easily and quickly retrievable. Accessibility is another dimension of usability (i.e., availability *is part of* accessibility).
- **Confidentiality**—In one of the studies, confidentiality was one of the original data quality attributes but was not further considered, except for ‘access is restricted for competitors’, which is an attribute of security, part of the dependability category. Even if ‘access is restricted to competitors’ is too narrow a definition for confidentiality, it is clear that, in the spirit of the PSP/IQ, confidentiality is an attribute of security (i.e., confidentiality *is part of* security).
- **Compliance**—If the specifications that information must conform to include things such as laws and regulations (e.g., legal concerns for privacy of information), as well as professional standards, best practices, etc., then the information requirement of compliance matches well the ‘conforms to specifications’ column of the PSP/IQ. So, compliance covers the soundness and dependability categories (i.e., compliance *is* conforming specifications).

### Conclusion

The COBIT 4.1 information criteria are entirely covered by the IM information quality dimension (in the PSP/IQ view) and *vice versa*. Effectiveness is the usefulness category, efficiency is the usability category, and compliance is both the soundness and dependability category. The other COBIT 4.1 information criteria are information quality dimensions within these categories (i.e., reliability is the believability dimension) or are subsumed by information quality dimensions (i.e., integrity, availability and confidentiality are subsumed by, respectively, the free-of-error, accessibility and security dimensions).

## Appendix G. COBIT 5 Compared to ITGI Five Governance Focus Areas

In the *Board Briefing on IT Governance* and in COBIT 5, reference is made to the five IT governance focus areas, as shown in **figure 31**.

Figure 31—Legacy IT Governance Focus Areas



The concepts and ideas contained in these focus areas are maintained and built upon in COBIT 5, but the focus areas themselves have not been literally maintained. **Figure 32** provides a brief overview on how the governance aspects in each of the focus areas are covered in COBIT 5.

Figure 32—COBIT 5 Coverage of Governance Focus Areas

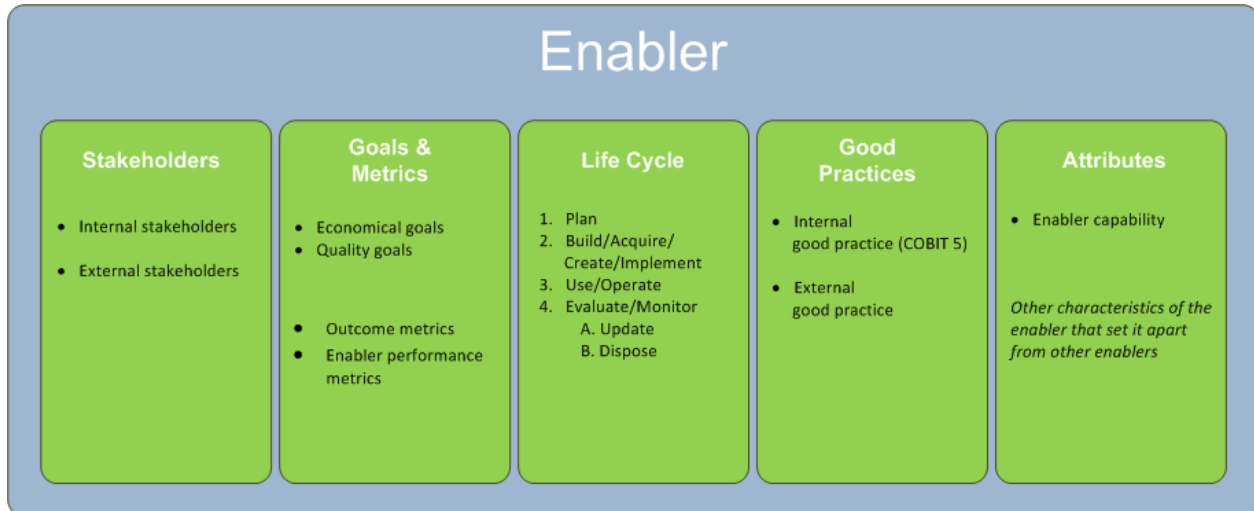
Focus Area	Coverage in COBIT 5
Value Delivery	Covered by the Ensure Value Delivery governance process
Risk Management	Covered by the Ensure Risk Management governance process
Strategic Alignment	Alignment is not a specific (process) activity, but is achieved through successful execution of the processes in the governance and management areas. The combination of the 'evaluate' and 'direct' governance practices in the governance area and the resulting direction given to management constitutes alignment.
Resource Management	Covered by the Ensure Resource Optimisation governance process
Performance Measurement	Covered by: <ul style="list-style-type: none"> <li>• Monitor governance practices in all governance processes</li> <li>• The Report to Stakeholders governance process</li> <li>• By the output(s) from the management processes in the Monitor, Assess and Inform domain</li> </ul>

## Appendix H. Detailed Description of COBIT 5 Enabler Models

### Overview of This Section

This section contains a more detailed description of the seven categories of enablers that are part of the COBIT 5 framework, which are initially described in section 4, as shown in **figure 33**.

Figure 33—COBIT 5 Generic Enabler Model (Repeat)



To start the description for each enabler, a similar drawing of the enabler model is shown. However, for all enablers, it will contain a number of additional or specific components. These are highlighted in another colour and are, thus, easily recognisable.

In addition to the specific enabler model for each enabler, a more detailed description is included for each enabler, discussing specific components and relationships with other enablers. Typically, only those components that encompass relevant or value-adding specific information over the generic information already included are discussed. In other words, not all detailed enabler models include discussions of all their components.

A number of small examples have been included as well.

## COBIT 5 Process Model

Figure 34—COBIT 5 Process Model

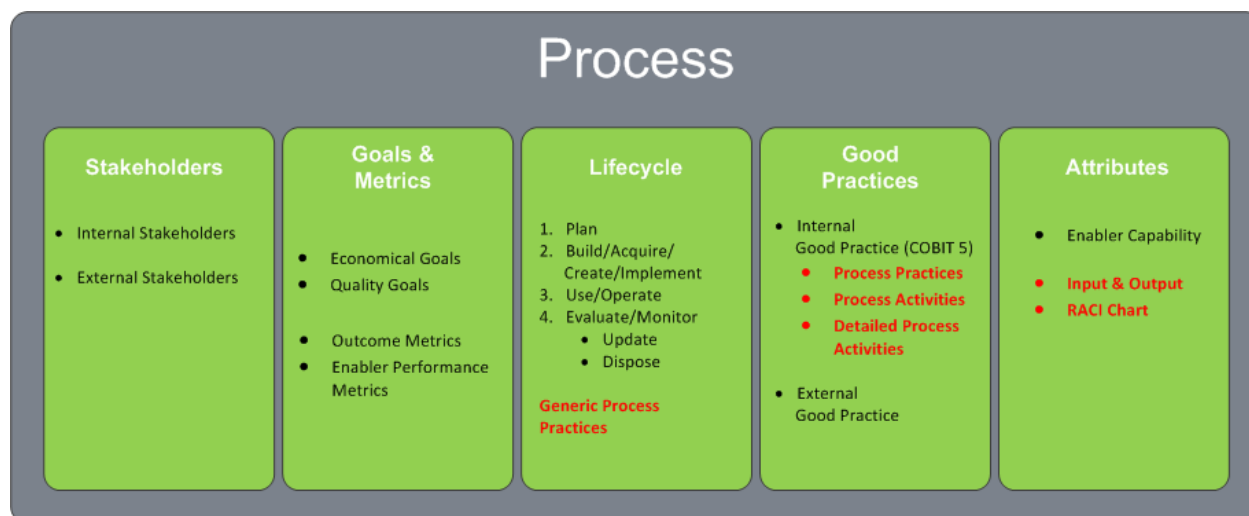


Figure 34 shows—at a high level—the different components of a process as it is defined within COBIT 5. This process model is an extension of the generic enabler model explained in section 4.

A process is defined as ‘a collection of activities that takes one or more kinds of input and creates an output that is of value to the organisation’.

The process model shows:

**Stakeholders**—Processes have internal and external stakeholders, each with their own roles; stakeholders and their responsibility levels are documented in RACI charts, which are an attribute of the process.

**Goals and metrics**—Process goals are defined as ‘a statement describing the desired outcome of a process. An outcome can be an artefact, a significant change of a state or a significant capability improvement of other processes’.

They are part of the goals cascade, i.e., process goals support IT-related goals, which in turn support enterprise goals. At each level, metrics are defined to measure the extent to which these goals are achieved. Metrics can be defined as ‘a quantifiable entity that allows the measurement of the achievement of a process goal. Metrics should be SMART—specific, measurable, actionable, relevant and timely’.

Goals can be classified in various ways. The generic classification distinguishes between ‘economical’ goals, which are more efficiency-oriented, and quality goals, which are more effectiveness-oriented.

Likewise, there are two types of process metrics: performance metrics, which have a predictive character, indicating the extent to which the process is performing in terms of activities, and outcome metrics, which indicate the extent to which the process really has achieved its goals and purpose.

Either type of metric can be associated to both types of goals.

**Life cycle**—Each process has a life cycle. It is defined, created, operated, monitored and adjusted/updated, or retired.

Generic process practices—e.g., as defined in the COBIT process assessment model based on ISO/IEC 15504—can assist with defining, running, monitoring and optimising processes.

**Good practices**—Process internal good practices are described in cascading levels of detail: practices, activities and detailed activities.<sup>12</sup>

a) **Practices:**

i) For each COBIT process, the management practices provide a complete set of high-level requirements for effective and practical management (governance) of enterprise IT. They:

<sup>12</sup> Only practices and activities are developed under the current project. The more detailed level(s) are subject to additional development(s), e.g., the various practitioner guides may provide more detailed guidance for their area.

- (1) Are statements of managerial actions to increase value, reduce risk and manage resources.
  - (2) Are aligned with relevant generally accepted standards and best practices.
  - (3) Are generic and applicable for any enterprise.
  - (4) Cover business and IT role players in the process (end to end).
- ii) Enterprise management needs to make choices relative to these management practices/governance practices by:
- (1) Selecting those that are applicable.
  - (2) Deciding upon those that will be implemented.
  - (3) Choosing how to implement them (frequency, span, automation, etc.).
  - (4) Accepting the risk of not implementing those that may apply.
- b) **Activities:**
- i. Are defined as 'guidance to achieve key management practices for successful governance and management of enterprise IT'. The COBIT 5 activities provide the how, why and what to implement for each governance practice or management practice to improve IT performance and/or address IT solution and service delivery risks. This material is of use to:
    - (1) Management, service providers, end users and IT professionals who need to justify and design or improve specific practices.
    - (2) Assurance professionals who may be asked for their opinions regarding proposed implementations or necessary improvements.
  - ii. A complete set of generic and specific activities provides one approach consisting of all the steps that are necessary and sufficient for achieving the key management practice/governance practice. They provide high-level guidance, at a level below the governance practice (GP)/management practice (MP), for assessing actual performance and for considering potential improvements. The activities:
    - (1) Describe a set of necessary and sufficient action-oriented implementation steps to achieve a MP/GP.
    - (2) Consider the inputs and outputs of the process.
    - (3) Are based on generally accepted standards and best practices.
    - (4) Support establishment of clear roles and responsibilities.
    - (5) Are non-prescriptive, and need to be adapted and developed into specific procedures appropriate for the enterprise.
- c) **Detailed activities** may not be at a sufficient level of detail for implementation and further guidance may need to be:
- i. Obtained from specific relevant standards and best practices such as ITIL, ISO/IEC 27000 series and PRINCE2.
  - ii. Developed as more detailed or specific activities in COBIT 5 itself.

External good practices can exist in any form or level of detail, and mostly refer to other standards and frameworks. Users can refer to these external good practice at all times, knowing that COBIT is aligned with these standards where relevant, and mapping information will be made available.

Successful completion of process activities and delivery of work products are the relevant process performance indicators for process capability achievement.

**Attributes**—There are a number of specific process attributes defined in the COBIT 5 process model. These include:

- a. **Inputs and outputs**—The COBIT 5 inputs and outputs are the process work products/artefacts considered necessary to support operation of the process. They enable key decisions, provide a record and audit trail of process activities, and enable follow-up in the event of an incident. They are defined at the key governance/management practice level, may include some work products used only within the process, and are often essential inputs to other processes.<sup>13</sup>
- b. **Process capability level**—COBIT 5 includes an ISO/IEC 15504-based process capability assessment scheme. The result of such an assessment is an attribute of a process.
- c. **RACI chart**, as described earlier

**Relationships with other enablers**—There are multiple relationships with other enablers, e.g.:

- a. Processes need information (as one of the types of inputs) and can produce information (as a work product).
- b. Processes need organisational structures and roles to operate, which is expressed through the RACI charts, e.g., IT steering committee, enterprise risk committee, board, audit, CIO, CEO, etc.
- c. Processes produce, and also require, service capabilities (infrastructure, applications, etc.).

<sup>13</sup> The illustrative COBIT 5 inputs and outputs should not be regarded as an exhaustive list since additional information flows could be defined depending on a particular enterprise's environment and process framework.

- d. Processes can and will depend on other processes.
- e. Processes will produce or will need policies and procedures to ensure consistent implementation and execution.
- f. Cultural and behavioural aspects will determine how well process are executed.

### COBIT 5 Process Reference Model

#### Governance and Management Processes

One of the guiding principles in COBIT is the distinction made between governance and management. In line with this principle, every organisation would be expected to implement a number of governance processes and a number of management processes in order to provide comprehensive governance and management of enterprise IT.

When considering processes for governance and management in the context of the enterprise, the difference between types of processes lies into the objectives of the processes:

- **Governance processes**—Governance processes will deal with the governance objectives—value delivery, risk management and resource balancing—and will include practices and activities aimed at evaluating strategic options, providing direction to IT and monitoring the outcome. (EDM—in line with the ISO/IEC 38500 standard concepts)
- **Management processes**—In line with the definition of management, practices and activities in management processes will cover the responsibility areas of plan, build, run and monitor (PBRM) enterprise IT, and they will have to provide end-to-end coverage of IT.

Although the outcome of both types of processes is different and intended for a different audience, internally (i.e., from the context of the process itself), all processes will also require ‘planning’, ‘building or implementation’, ‘execution’ and ‘monitoring’ activities within the process.

#### COBIT 5 Process Reference Model

COBIT 5 is not prescriptive, but from the previous text it is clear that it advocates that organisations implement governance and management processes such that the key areas are covered, as shown in **figure 35**.

In theory, an enterprise can organise its processes as it sees fit, as long as the basic governance and management objectives are covered. Smaller enterprises have fewer processes; larger and more complex enterprises may have many processes, all to cover the same objectives.

Figure 35—COBIT 5 Governance and Management Processes



However, notwithstanding the previous text, COBIT 5 includes a process reference model, defining and describing in detail a number of governance and management processes. It provides a process reference model that represents all the processes normally found in an enterprise relating to IT activities, offering a common reference model understandable to operational IT and business managers. The proposed process model is a complete, comprehensive model, but it is not the only possible process model. Each enterprise must define its own process set, taking into account the specific situation.

Incorporating an operational model and a common language for all parts of the business involved in IT activities is one of the most important and critical steps toward good governance. It also provides a framework for measuring and monitoring IT performance, communicating with service providers and integrating best management practices.

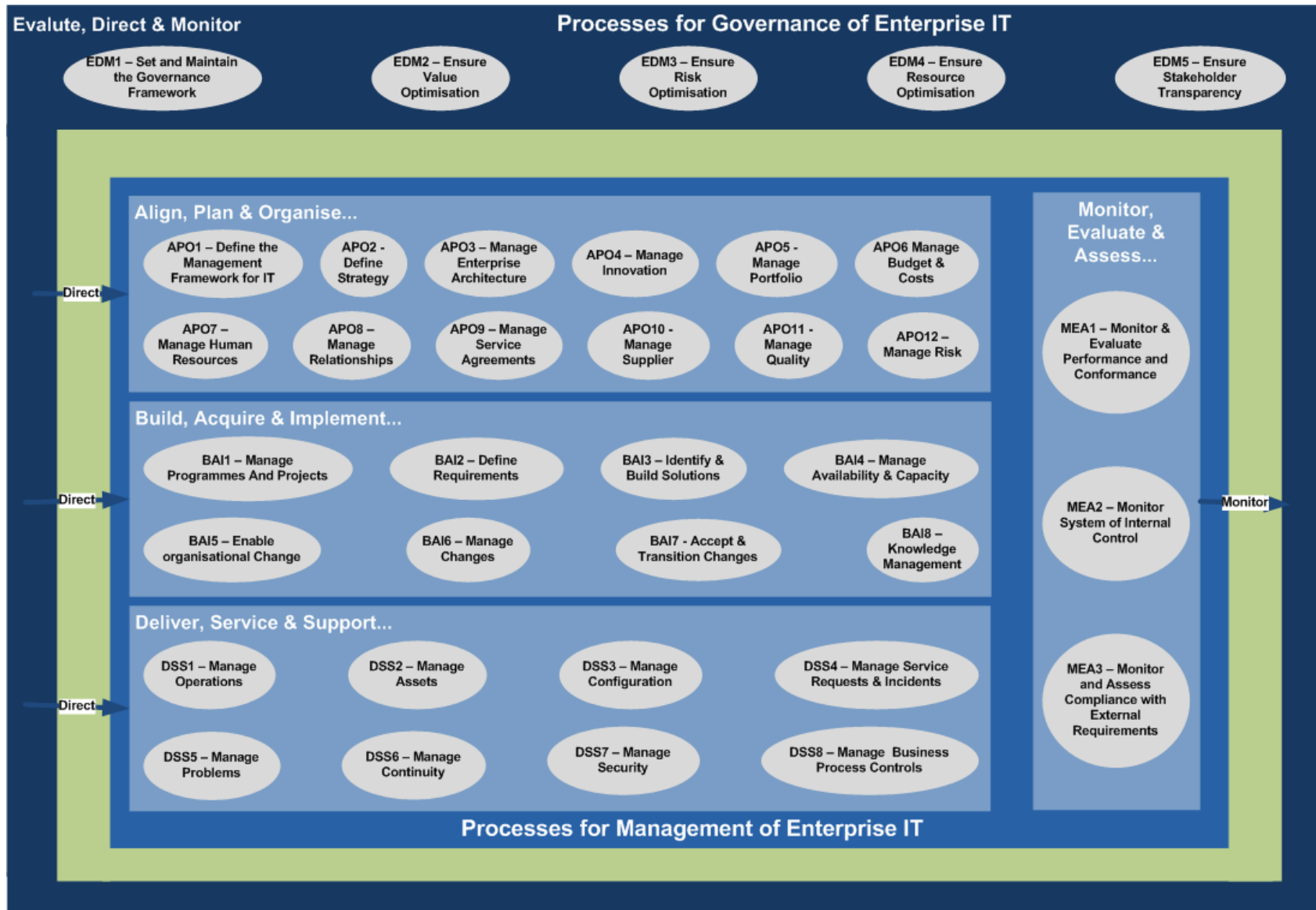
The COBIT 5 reference process model subdivides the governance and management processes of enterprise IT into two main areas of activity—governance and management—divided into domains of processes:

- The GOVERNANCE domain contains five governance processes; within each process, evaluate, direct and monitor practices are defined.
- The four MANAGEMENT domains, in line with the responsibility areas of plan, build, run and monitor (PBRM—an evolution of the COBIT 4.1 domains), provides end-to-end coverage of IT. Each domain contains a number of processes, as in COBIT 4.1 and in previous versions. Although—as described previously—most of the processes require ‘planning’, ‘implementation’, ‘execution’ and ‘monitoring’ activities within the process or within the specific issue being addressed (e.g., quality, security), they are placed in domains in line with what is generally the most relevant area of activity when regarding IT at the enterprise level.
- In COBIT 5, the processes also cover the full scope of business and IT activities related to the governance and management of enterprise IT, thus making the process model truly enterprise-wide.

The COBIT 5 process reference model is the successor of the COBIT 4.1 process model, with the Risk IT and Val IT process models integrated as well. **Figure 36** shows the complete set of 36 governance and management processes within COBIT 5. The details of all processes, as per the process model described previously, are included in *COBIT 5: Process Reference Guide*.

# COBIT 5: Framework Exposure Draft

Figure 36—COBIT 5 Illustrative Governance and Management Processes



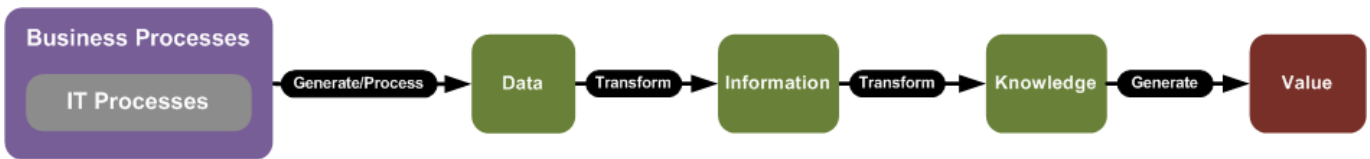
## COBIT 5 Information Model

### Introduction—The Information Cycle

The COBIT 5 information model (IM) is an extension of the generic enabler model (see section 4); it defines a number of specific dimensions of information, allowing all stakeholders who have to deal with information to consider all required aspects.

The information model deals with all information relevant for organisations, not only automated information. Information can be structured or ‘non-structured’ or not formalised. One can think of Information as being one stage in the ‘information cycle’ of an enterprise. In the information cycle (**figure 37**), business processes generate and process data, transforming it to information and knowledge, and ultimately generating value for the enterprise. The scope of the IM excludes the knowledge and value parts of the cycle.

Figure 37—COBIT 5 Metadata—Information Cycle



### COBIT 5 Information Model

Figure 38—COBIT 5 Information Model



**Figure 38** shows—at a high level—all components of the information model, with the specific components highlighted in red:

**Information stakeholders**—Can be internal or external to the enterprise. The generic model also suggests that, apart from identifying the stakeholders, their stakes need to be identified, i.e., why they care or are interested in the information.

With respect to which information stakeholders exist, different categorisations of roles in dealing with information are possible, ranging from fine-grained proposals (e.g., suggesting specific data or information roles like architect, owner, steward, trustee, supplier, beneficiary, modeller, quality manager, security manager) to more coarse-grained proposals, for instance, distinguishing amongst information producers, information custodians and information consumers:

- Information producer, responsible for creating the information

- Information custodian, responsible for storing and maintaining the information
- Information consumer, responsible for using the information

These categorisations refer to specific activities with regard to the information resource. Activities depend on the life cycle phase of the information. Therefore, to find a categorisation of roles that has an appropriate level of granularity for the IM, the information life cycle dimension of the IM can be used. This means that information stakeholder roles can be defined in terms of information life cycle phases, e.g., information planners, information ‘obtainers’, information users. At the same time, this means that the information stakeholder dimension is not an independent dimension; different life cycle phases have different stakeholders.

Whereas the relevant roles depend on the information life cycle phase, the stakes can be related to information goals.

### Information quality:

- A. **Quality goals**—The metrics are divided in two sub-dimensions: information quality and information benefits/cost/risk. *Information quality*, which is discussed here, is a very broad concept and comprises many different criteria. In the context of COBIT 5, this is modelled as a hierarchical structure of four information quality categories, which can be further decomposed into 15 information quality dimensions. The four categories are **Intrinsic** quality, which considers quality as an intrinsic property of information; **Contextual** quality, which recognises that information quality may depend on a context of use (i.e., the task to be performed by the information user); and **Representational** and **Accessibility** quality, which consider the quality of information in relation to the information technologies that are used to (re)present the information and make it accessible to users/not accessible to non-intended users, respectively.
- a. **Intrinsic quality**—The extent to which data values are in conformance with the actual or true values. It includes:
- Accuracy—The extent to which information is correct and reliable
  - Objectivity—The extent to which information is unbiased, unprejudiced and impartial
  - Believability—The extent to which information is regarded as true and credible
  - Reputation—The extent to which information is highly regarded in terms of its source or content
- b. **Contextual and representational quality**—The extent to which information is applicable to the task of the information user and is presented in an intelligible and clear manner. It includes:
- Relevancy—The extent to which information is applicable and helpful for the task at hand
  - Completeness—The extent to which information is not missing and is of sufficient depth and breadth for the task at hand
  - Timeliness—The extent to which information is sufficiently up to date for the task at hand
  - Appropriate amount of information—The extent to which the volume of information is appropriate for the task at hand
  - Concise representation—The extent to which information is compactly represented
  - Consistent representation—The extent to which information is presented in the same format
  - Interpretability—The extent to which information is in appropriate languages, symbols, and units, and the definitions are clear
  - Understandability—The extent to which information is easily comprehended
  - Ease of manipulation—The extent to which information is easy to manipulate and apply to different tasks
- c. **Accessibility quality**—The extent to which information is available or obtainable. It includes:
- Availability—The extent to which information is available when required, or easily and quickly retrievable
  - Confidentiality—The extent to which access to information is restricted appropriately to authorised parties

In the context of the IM, security can be seen as a subset of a number of the quality requirements. Indeed, availability and confidentiality are listed under accessibility, whereas information integrity is a combination of other, different intrinsic and contextual quality attributes, such as accuracy, completeness and, to some extent, reputation.

Appendix F provides a detailed description of how the COBIT 5 information quality criteria compare to the COBIT 4.1 information criteria.

- B. **Information economical goals**—A second sub-dimension of the information goals relates to information being economical and efficient. Investments in information technology are based on cost-benefit analysis, as costs and benefits refer not only to tangible, measurable factors but they also take into account intangible, more difficult to measure or even immeasurable factors such as competitive advantage, customer satisfaction and technology uncertainty. It is only when the information resource is applied or used that an enterprise receives value from it. Some considerations in this respect include:
- This value generated by information is generally hard or even impossible to quantify: what is the effect of information on decision making and on the outcome of effective decision making?
  - Sometimes value can be measured (i.e., a benefit). For example, information can be the end product that generates value for an organisation.
  - In any case, the value of information is determined solely through its use (internally or by selling it), so information has no intrinsic value. It is only through putting information into action that value can be generated.
  - On the other hand, all phases in the life cycle of information have a cost, as in all phases activities need to be performed, resources have to be used or consumed, etc. Since all these activities may fail (i.e., not be performed or not lead to the desired results), all life cycle phases also have an associated risk. For instance, if information is not properly stored, then it might get lost, which means that it needs to be obtained again, increasing its cost.
  - So, it can be argued that the information value/cost/risk IM sub-dimension is not independent from the life cycle dimension (see the following bullet). Costs and risk can be defined in relation to particular information life cycle phases and the value of information relates only to its use. The use phase includes amongst its risks the misuse of information (internally or externally), which can be considered as the 'negative value' of information.

**Information life cycle**—Like other resources, information has a life cycle. The full life cycle of information needs to be considered, and different approaches may be required for information in different phases of the life cycle. The COBIT 5 IM distinguishes the following phases:

- Plan**—The phase in which the creation and use of the information resource is prepared. Activities in this phase may refer to the identification of objectives, the planning of the information architecture, and the development of standards and definitions (e.g., data definitions, data collection procedures).
- Obtain**—The phase in which the information resource is acquired. Activities in this phase may refer to the creation of data records, the purchase of data and the loading of external files.
- Store**—The phase in which information is held electronically or in hard copy (or even just in human memory). Activities in this phase may refer to the storage of information in electronic form (e.g., electronic files, databases, data warehouses) or as hard copy (e.g., paper documents).
- Share**—The phase in which information is made available for use through a distribution method. Activities in this phase may refer to the processes involved in getting the information to places where it can be accessed and used (e.g., distributing documents by e-mail). For electronically held information, this life cycle phase may largely overlap with the store phase (e.g., sharing information through database access, file/document servers).
- Use**—The phase in which information is used to accomplish goals. Activities in this phase may refer to all kinds of information usage (e.g., managerial decision making, running automated processes), and also include activities such as information retrieval and converting information from one form to another.

According to the Taking Governance Forward view, information is an enabler for enterprise governance. Hence, information use as defined in the IM can be thought of as the purposes for which enterprise governance stakeholders need information when assuming their roles, fulfilling their activities and interacting with each other.

- These roles, activities, and relationships are captured in the lower part of **figure 3** in section 1. The interactions between stakeholders require information flows whose purposes are indicated in the schema: accountability, delegation, monitoring, direction setting, alignment, execution and control.
  - 'Maintain' is the phase in which it is ensured that the information resource continues to work properly (i.e., to be valuable). Activities in this phase may refer to keeping information up to date as well as other kinds of information management activities (e.g., enhancing, cleansing, merging, removing duplicate information data in data warehouses).
- F. **Dispose**—The phase in which the information resource is discarded when it is no longer of use. Activities in this phase may refer to information archiving or destroying.

**Information attributes**—The concept of information is understood differently in different disciplines such as economics, communication theory, information science, knowledge management and information systems.

Therefore, there is no universally agreed definition on what information is. The nature of information can, however, be clarified through its properties. An information attributes dimension can therefore answer the ‘what is information?’ question without imposing an artificial unifying definition.

To categorise and provide further structure to the different information attributes that can be used to characterise information, a generally recognised framework that considers six levels or layers to talk or reason about properties of information can be used. These six levels present a continuum of attributes, ranging from the physical world of information, where attributes are linked to information technologies and media for information capturing, storing, processing, distribution and presentation, to the social world of information use, sense-making and action.

The following descriptions can be given to the layers and information attributes:

- A. **Physical world layer**—The world where all phenomena that can be empirically observed take place
  - Information carrier/media—The attribute that identifies the physical carrier of the information (e.g., paper, electric signals, sound waves)
- B. **Empiric layer**—The empirical observation of the signs used to encode information and their distinction from each other and from background noise
  - Information access channel—The attribute that identifies the access channel of the information (e.g., user interfaces)
- C. **Syntactic layer**—The rules and principles for constructing sentences in natural or artificial languages. Syntax refers to the form of information.
  - Code/language—The attribute that identifies the representational language/format used for encoding the information
- D. **Semantic layer**—The rules and principles for constructing meaning out of syntactic structures. Semantics refers to the meaning of information.
  - Information type—The attribute that identifies the kind of information. Different categorisations are possible, e.g., financial vs. non-financial information, internal vs. external origin of the information, forecasted/predicted values vs. observed values, planned values vs. realised values.
  - Information currency—The attribute that identifies the time horizon referred to by the information, i.e., information on the past, the present or the future
  - Information level—The attribute that identifies the degree of detail of the information (e.g., sales per year, quarter, month)
- E. **Pragmatic layer**—The rules and structures for constructing larger language structures that fulfil specific purposes in human communication. Pragmatics refers to the use of information.
  - Retention period—The attribute that identifies how long information can be retained before it is destroyed
  - Information status—The attribute that identifies whether the information is operational or historical
  - Novelty—The attribute that identifies whether the information creates new knowledge or confirms existing knowledge (i.e., information vs. confirmation)
  - Contingency—The attribute that identifies the information that is required to precede this information (for it to be considered as information)
- F. **Social world layer**—The world that is socially constructed through the use of language structures at the pragmatic level of semiotics (e.g., contracts, law, culture)
  - Context—The attribute that identifies the context in which the information makes sense, is used, has value, etc. (e.g., cultural context, subject domain context)

The IM is a new model and is very rich in terms of different components. It will be further developed in a separate publication. In order to make it more tangible for the COBIT 5 user, and to make its relevance more clear in the context of the overall COBIT 5 framework, some examples of possible use of the IM follow.

### EXAMPLE 12

When developing a new application, the IM can be used to assist with the specifications of the application and the associated information or data models.

The Information attributes of the IM can be used to define specifications for the application and the business processes that will use the information.

For example, the design and specifications of the new system need to specify:

- Physical layer—Where will information be stored?
- Empirical layer—How can the information be accessed?
- Syntactical layer—How will the information be structured and coded?
- Semantic layer—What sort of information is it? What is the information level?
- Pragmatic layer—What are the retention requirements? Which other information is required for this information to be useful and useable?

Looking at the stakeholders dimension combined with the information life cycle, one can define who will need what type of access to the data during which phase of the information life cycle.

When the application is tested, testers can look at the information quality criteria to develop a comprehensive set of test cases.

### EXAMPLE 13

Security groups within the enterprise can benefit from the attributes dimension of the IM. Indeed, when charged with protection of information, they need to look at, e.g.:

- Physical layer—How and where is information physically stored?
- Empirical layer—What are the access channels to the information?
- Semantic layer—What type of information is it? Is the information current or relating to the past or to the future?
- Pragmatic layer—What are the retention requirements? Is information historic or operational?

Using these attributes will allow the user to determine the level of protection and the protection mechanisms required.

Looking at another dimension of the IM, security professionals can also consider the information life cycle stages, because information needs to be protected during all phases of the life cycle. Indeed, security starts at the information planning phase, and implies different protection mechanisms for storing, sharing and disposition of information. The IM ensures that information is protected during the full life cycle of the information.

### EXAMPLE 14

When performing a review of a business process (or an application), the IM can be used to assist with a general review of the information processed by and delivered by the process, and of the underlying information systems. The **quality criteria** can be used to assess the extent to which information is available, e.g., whether the information is complete, available on a timely basis, factually correct, relevant, available in the appropriate amount. One can also consider the accessibility criteria, i.e., whether the information is accessible when required and adequately protected.

The review can be even further extended to include representation criteria, e.g., the ease with which the information can be understood, interpreted, used and manipulated.

A review that uses the information quality criteria of the IM provides an enterprise with a comprehensive and complete view on the current information quality within a business process.

## COBIT 5 Organisational Structures Model

Figure 39—COBIT 5 Organisational Structures Model



The organisational structures model, based on the generic COBIT 5 enabler model, is shown in **Figure 39**:

**Stakeholders**—Organizational structures stakeholders can be internal and external to the enterprise, and they include the individual members of the structure, other structures, organizational entities, clients, suppliers, regulators etc. Their roles vary, and include decision making, influencing, advising. The stakes of each of the stakeholders also varies, i.e. what interest do they have by the decisions made by the structure?

**Goals and metrics**—Each organisational structure has a reason to exist, expressed by its mandate. The mandate of the structure describes the goals it has to achieve and how achievement of these goals will be measured.

**Life cycle**— An organisational structure has a life cycle. It is created, exists and is adjusted, and finally it can be disbanded. During its inception, a mandate has to be defined, i.e., a reason and purpose for its existence, hence a link to the goals and metrics.

**Good practices**—A number of good practices for organisational structures can be distinguished, e.g.:

- Operating principles—The practical arrangements how the structure will operate, such as frequency of meetings, documentation and housekeeping rules.
- Delegation of authority—The structure can delegate (a subset of) its decision rights to other structures reporting to it.
- Escalation procedures—The escalation path for a structure describes the required actions in case of problems in taking decisions.

**Attributes**—Some attributes of a decision structure include:

- Composition—Structures have members, which are internal or external stakeholders. They also have a role in the context of the organisational structures.
- Inputs and outputs—A structure requires inputs (typically information) before it can take informed decisions, and it produces outputs (typically, decisions or requests for additional inputs).
- RACI chart—A RACI chart is more an attribute of a process, although it is relevant for an organisational structure as well. It describes where and in which processes the structure intervenes.
- Span of control—The boundaries of the organisation structure’s decision rights
- Level of authority/decision rights—The decisions the structure is authorised to take

**Relationships with other enablers**—A link between organisational structures to other enablers in COBIT 5 is through the RACI charts, where structures are linked to process activities, and where people are linked to the structures. Relationships with other enablers include:

- Culture and behaviour determine the efficiency and effectiveness of organisation structures and their decisions.
- Composition of organisational structures should take into account the appropriate skill set of its members.
- The mandate and operating principles of organisational structures are guided by the policy framework in place.

# COBIT 5: Framework Exposure Draft

## Illustrative Organisational Structures in COBIT 5

As mentioned in the discussion on the COBIT 5 process model, an illustrative COBIT 5 process reference model has been created and is described in detail in *COBIT 5: Process Reference Guide*. The model includes RACI charts, which use a number of roles and structures. **Figure 40** describes these predefined roles and structures. Please note that:

- These do not necessarily have to correspond with actual functions organisations have implemented, but nonetheless they provide value in the sense that the purpose of the structure or the role remains valid for most organisations, and for that reason the responsibility should be assumed anyhow.
- The purpose of this table is not to prescribe a universal sort of organisation chart for every organisation. Rather, it should be seen as illustration.

**Figure 40—COBIT 5 Roles and Organisational Structures**

ROLE/STRUCTURE	DEFINITION/DESCRIPTION
BOARD	The group of the most senior executives and/or non-executives of the enterprise who are accountable for the governance of the enterprise and have overall control of its resources
CHIEF EXECUTIVE OFFICER (CEO)	The highest-ranking officer who is in charge of the total management of the enterprise
CHIEF FINANCIAL OFFICER (CFO)	The most senior official of the enterprise who is accountable for all aspects of financial management including financial risk and controls and reliable and accurate accounts
CHIEF OPERATING OFFICER (COO)	The most senior official of the enterprise who is accountable for the operation of the enterprise
CHIEF RISK OFFICER (CRO)	The most senior official of the enterprise who is accountable for all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk.
CHIEF INFORMATION OFFICER (CIO)	The most senior official of the enterprise who is responsible for aligning IT and business strategies and accountable for planning, resourcing and managing the delivery of IT services and solutions to support enterprise objectives
CHIEF INFORMATION SECURITY OFFICER (CISO)	The most senior official of the enterprise who is accountable for the security of enterprise information in all its forms
BUSINESS EXECUTIVE	A senior management individual accountable for the operation of a specific business unit or subsidiary
BUSINESS PROCESS OWNER	An individual accountable for the performance of a process in realising its objectives, driving process improvement and approving process changes.
STRATEGY (IT EXECUTIVE) COMMITTEE	A group of senior executives appointed by the board to ensure that the board is involved in and kept informed of major IT-related matters and decisions. The committee is accountable for managing the portfolios of IT-enabled investments, IT services and IT assets, ensuring that value is delivered and risks are managed. The committee is normally chaired by a board member, not the CIO.
(PROJECT AND PROGRAMME) STEERING COMMITTEES	A group of stakeholders and experts who are accountable for guidance of programmes and projects, including management and monitoring of plans, allocation of resources, delivery of benefits and value, and management of programme and project risks
ARCHITECTURE BOARD	A group of stakeholders and experts who are accountable for guidance on enterprise architecture-related matters and decisions, and for setting architectural policies and standards
ENTERPRISE RISK COMMITTEE	The group of executives of the enterprise who are accountable for the enterprise-level collaboration and consensus required to support enterprise risk management activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the Enterprise Risk Committee.
HEAD HUMAN RESOURCES	The most senior official of an enterprise who is accountable for planning and policies with respect to all human resources in that enterprise
COMPLIANCE	The function in the enterprise responsible for guidance on legal, regulatory and contractual compliance
AUDIT	The function in the enterprise responsible for provision of internal and external audits
HEAD ARCHITECT	A senior individual accountable for the enterprise architecture process
HEAD DEVELOPMENT	A senior individual accountable for IT-related solution development processes
HEAD IT OPERATIONS	A senior individual accountable for the IT operational environments and infrastructure
HEAD IT ADMINISTRATION	A senior individual accountable for IT-related records and responsible for supporting IT-

## COBIT 5: Framework Exposure Draft

Figure 40—COBIT 5 Roles and Organisational Structures

ROLE/STRUCTURE	DEFINITION/DESCRIPTION
	related administrative matters
PROGRAMME AND PROJECT MANAGEMENT OFFICE (PMO)	The function responsible for supporting programme and project managers, and gathering, assessing and reporting information about the conduct of their programmes and constituent projects
VALUE MANAGEMENT OFFICE (VMO)	The function that acts as the secretariat for managing investment and service portfolios, including assessing and advising on investment opportunities and business cases, recommending value governance/management methods and controls, and reporting on progress on sustaining and creating value from investments and services
SERVICE MANAGER	An individual who manages the development, implementation, evaluation and ongoing management of new and existing products and services for a specific customer (user) or group of customers (users)
INFORMATION SECURITY MANAGER	An individual who manages, designs, oversees and/or assesses an enterprise's information security
BUSINESS CONTINUITY MANAGER	An individual who manages, designs, oversees and/or assesses an enterprise's business continuity capability, to ensure that the enterprise's critical functions continue to operate following disruptive events
PRIVACY OFFICER	An individual who is responsible for monitoring the risks and business impacts of privacy laws and for guiding and co-ordinating the implementation of policies and activities that will ensure that the privacy directives are met

## COBIT 5 Skills and Competencies Model

The people and skills model, based on the generic COBIT 5 enabler model, is shown in **Figure 41**. The purpose of this model is to provide the necessary components to provide guidance on how people skills and behaviour can be influenced and structured.

Figure 41—COBIT 5 Skills and Competencies Model



**Stakeholders** – Skills and competencies stakeholders are internal and also external to the enterprise. Different stakeholders assume different roles – think e.g. business managers, project managers, partners, competitors, recruiters, trainers, developers, technical IT specialists, etc. – and each role requires a distinct skill set.

**Goals & Metrics** - goals and metrics for skills & competencies will relate to skill sets and skill levels to be achieved, and to all processes and activities required to achieve and maintain them.

### Life cycle:

- People and skills have a life cycle. An enterprise has to know what its current skill base is, and plan what it needs to be. This is influenced by (amongst other issues) the strategy and goals of the enterprise. Skills need to be developed (e.g., through training) or acquired (e.g., through recruitment) and deployed in the various roles within the organisation structure.
- Periodically, such as on an annual basis, the enterprise needs to assess the skill base to understand the evolution that has occurred, which will feed into the planning process for the next period.
- This assessment can also feed into the reward and recognition process for human resources.

### Good practices:

- Internal good practice—Good practice for people and skills includes the need for objective skill requirements for each role played by the various stakeholders. This can be described through different skill levels in different skill categories. For each appropriate skill level in each skill category, a skill definition should be available. The skill categories correspond with the IT related activities undertaken, e.g., information management, business analysis.
- External good practice:
  - There are external sources of good practice, such as the Skills Framework for the Information Age (SFIA),<sup>14</sup> which provides comprehensive skill definitions.
  - Within COBIT5, the roles responsible for various IT activities as captured in the process reference model can be defined. Some of these roles are already described as part of the RACI charts, as shown in **figure 39**.
  - Examples of potential skill categories, mapped to COBIT 5 process domains, are shown in **figure 42**.

<sup>14</sup> [www.sfia.org.uk/](http://www.sfia.org.uk/)

Figure 42—COBIT 5 Skills Categories

PROCESS DOMAIN	EXAMPLES OF SKILL CATEGORIES
EVALUATE, DIRECT AND MONITOR	<ul style="list-style-type: none"> <li>• Governance of enterprise IT</li> </ul>
ALIGN, PLAN AND ORGANISE	<ul style="list-style-type: none"> <li>• IT policy formulation</li> <li>• IT strategy</li> <li>• Enterprise architecture</li> <li>• Innovation</li> <li>• Financial management</li> <li>• Portfolio management</li> </ul>
BUILD, ACQUIRE AND IMPLEMENT	<ul style="list-style-type: none"> <li>• Business analysis</li> <li>• Project management</li> <li>• Usability evaluation</li> <li>• Requirements definition and management</li> <li>• Programming</li> <li>• System ergonomics</li> <li>• Software decommissioning</li> </ul>
DELIVER, SERVICE AND SUPPORT	<ul style="list-style-type: none"> <li>• Capacity management</li> <li>• Availability management</li> <li>• Problem management</li> <li>• Service desk and incident management</li> <li>• Security administration</li> <li>• IT operations</li> <li>• Database administration</li> </ul>
MONITOR, EVALUATE AND ASSESS	<ul style="list-style-type: none"> <li>• Compliance review</li> <li>• Performance monitoring</li> <li>• Controls audit</li> </ul>

**ATTRIBUTES**—Attributes of people and skills include experience, education and qualifications, knowledge, technical skills, and behavioural skills.

**Relationships with other enablers**—There are links between people and skills and other enablers in COBIT 5:

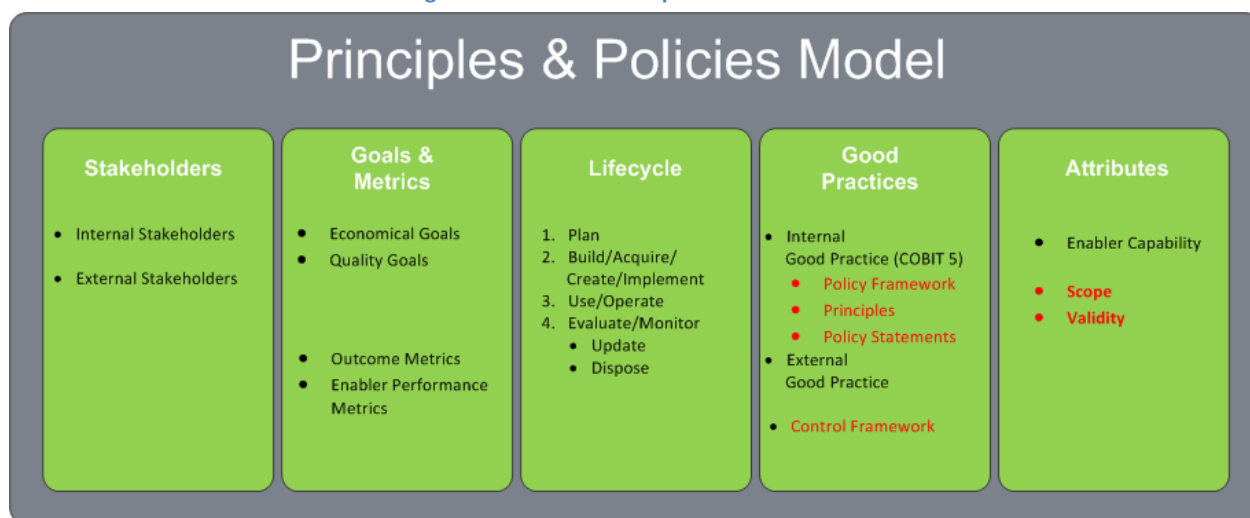
- Through RACI charts, people are linked to process and organisational structures.
- There is also a link to culture, ethics and behaviour through behavioural skills, which are influenced by individual ethics.

#

## COBIT 5 Principles and Policies Model

The principles and policies model, based on the generic COBIT 5 enabler model, is shown in **figure 43**.

Figure 43—COBIT 5 Principles and Policies Model



**Stakeholders**—Principles and policies stakeholders can be internal and external to the enterprise. They include board and executive management, compliance officers, risk managers, internal and external auditors, service providers and customers, regulatory agencies, etc. The stakes are twofold: some stakeholders define and set policies, others have to align to and comply with policies.

**Goals and metrics**—Policies and procedures are instruments to communicate the rules of the organisation in support of the governance objectives and enterprise values, as defined by the board and executive management. Principles need to be:

- Limited in number
- Put in simple language, expressing as clearly as possible the core values of the enterprise

Policies provide more detailed guidance on how to put principles into practice and they influence how decision making aligns with the principles. Good policies are:

- Effective—They achieve the stated purpose.
- Efficient—They ensure that principles are implemented in the most efficient way.
- Non-intrusive—They appear logical for those who have to comply with them, i.e., they do not create unnecessary resistance.

**Life cycle**—Policies have a life cycle, too. In that context, the policy framework is key. It provides the structure in which a consistent set of policies can be created and maintained, and it provides an easy point of navigation within and between individual policies.

Depending on the external environment in which the enterprise operates, there can be varying degrees of regulatory requirements for strong internal control and, as a consequence, a strong policy framework. Some key attention points to be taken into account include:

- Access to policies—Is there a mechanism in place that provides easy access to policies for all stakeholders? In other words, do stakeholders know where to find policies?
- Currency of policies—If and when policies are reviewed and updated, are there strong mechanisms in place to ensure that people are aware of these updates, that the newest version is easily accessible (see previous point), and that obsolete copies are disposed of?

**Good practices:**

1. Good practice requires that policies be part of an overall policy and control framework, providing a (hierarchical) structure into which all policies should fit and clearly making the link to the underlying principles.
2. As part of the policy framework, the following items need to be described:
  - a. The consequences of failing to comply with the policy

- b. The means for handling exceptions
  - c. The manner in which compliance with the policy will be checked and measured
3. Generally recognised control frameworks can provide valuable guidance on the actual policy statements to be included in policies.
  4. Policies should be aligned with the organisation's risk appetite. Policies are a key component of an enterprise's system of internal control, whose purpose it is to manage and contain risk. As part of risk governance activities, the enterprise's risk appetite is defined, and this risk appetite should be reflected in the policies. A risk-averse organisation has stricter policies than a risk-aggressive organisation.

**Attributes**—Principles and policies have some specific attributes, such as scope and validity, describing their applicability. Policies need to be re-validated and/or updated at regular intervals.

**Relationships with other enablers**—There are many links with the other enablers, e.g.:

- Policies should reflect the culture and ethical values of the enterprise, and they should encourage the desired behaviour, hence a strong link with the culture, ethics and behaviour enabler.
- Process practices and activities are the most important vehicle for executing policies.
- Organisational structures can define and implement policies within their span of control, and their activities are also defined by policies.

### EXAMPLE 15

An enterprise is considering how to deal with the fast-rising use of social media and pressure from its staff to have full access. Until now, the organisation has been conservative or restrictive in granting access to this kind of service, mainly for security reasons.

There is pressure from different sides to take another position with regard to social media. Staff wants similar levels of access as it has from home, but the organisation itself also wants to use and exploit the benefits of social media for marketing and public awareness-raising purposes.

The decision is taken to define a policy on the use of social media on the enterprise's networks and systems, including laptops provided by the enterprise to its staff members. The new policy fits in the existing policy framework under the category of 'acceptable use policies', and it is more relaxed than previous policies. As a consequence, communication is developed to explain the reasons for the new policy. At the same time, there is also impact on some other enablers:

- Staff needs to learn how to deal with the new media in order not to create embarrassing situations for the enterprise, i.e., learning the right behaviour in line with the new direction the enterprise is taking and developing the right skills
- A number of processes with regard to security need to be changed; access is opened up to these media, so security settings and configurations have to change and possibly some compensating measures need to be defined.

## COBIT 5 Culture, Ethics and Behaviour Model

Human behaviour is one of the key factors determining the success of any enterprise, and the COBIT 5 model for culture, ethics and behaviour (**figure 44**) provides a number of components that need to be taken into account.

Figure 44—COBIT 5 Culture, Ethics and Behaviour Model



**Stakeholders** - Culture, ethics and behaviour stakeholders can be internal and external to the enterprise. Internal stakeholders include the whole enterprise, external stakeholders include regulators, e.g. external auditors or supervisory bodies. Stakes are twofold: some stakeholders deal with defining, implementing and enforcing desired behaviours, e.g. legal officers, risk managers, HR managers, remuneration boards and officers, etc., others have to align with the defined rules and norms.

**Goals & Metrics** – goals and metrics can either relate to instances of desired/undesired behaviour (outcome metrics), or they can relate to the culture and behaviour changing techniques and measure put in place (performance measures).

**Lifecycle** – an organisational culture, individual behaviours, etc. all have their lifecycles. Starting from an existing culture, an organisation can identify required changes and work towards their implementation. Several tools – described in the good practices – can be used for that.

**Good practices**—Good practices for creating, encouraging and maintaining desired behaviour throughout the organisation include:

- Communication throughout the enterprise of desired behaviours and the underlying corporate values
- Awareness of desired behaviour, strengthened by the example behaviour exercised by senior management
- Incentives to encourage and deterrents to enforce desired behaviour. There is a clear link between individual behaviour and the HR reward scheme an enterprise puts in place.
- Rules and norms, which provide more guidance on desired organisational behaviour. This links very clearly to the principles and policies an organisation puts in place.

**5. Attributes**—Specific attributes for culture, ethics and behaviour include:

- Organisational ethics, determined by the values the enterprise wants to live by
- Individual ethics, determined by the personal values of each individual in the organisation and depending to a important extent on external factors such as religion, ethnicity, socio-economic background, geography and personal experiences
- Behaviours, which collectively determine the culture of an organisation. Many factors drive behaviours, e.g., the external factors mentioned above but also interpersonal relationships in enterprises, personal objectives and ambitions. Some types of behaviours that can be relevant in this context include:
  - Behaviour toward taking risk—How much risk does the enterprise feel it can absorb and which risks is it willing to take?
  - Behaviour toward following policy—To what extent will people embrace and/or comply with policy?

- Behaviour toward negative outcomes—How does the enterprise deal with negative outcomes, i.e., loss events or missed opportunities? Will it learn from them and try to adjust, or will blame be assigned without treating the root cause?

**Relationships with other enablers**—Culture is an important influencer or even critical success factor for a number of other enablers, e.g.:

- Processes can be designed to a level of perfection, but if the stakeholders of the process do not wish to execute the process activities as they should, i.e., if their behaviour is one of non-compliance, process outcomes will fall short.
- Likewise, organisational structures can be designed and built according to the textbook, but if their decisions are not implemented—for reasons of different personal agendas, lack of incentives, etc.—they will not result in decent governance and management of enterprise IT.
- Principles and policies are a very important communication mechanism for corporate values and the desired behaviour.

### EXAMPLE 16

An enterprise is facing repeatedly serious quality problems with new applications. Despite the fact that a sound software project development methodology is in place, all too often software problems cause operational problems in day-to-day business.

An investigation shows that the development team members and management are evaluated and rewarded based on the timely delivery, within budget, of their projects. They are not measured against quality criteria or business benefits criteria. As a consequence, they focus diligently on delivery time and cost cutting during development, e.g., on testing time. The investigation also shows that compliance with the established methodology and procedures is virtually non-existent, because it would take some more time from the development budget (in favour of quality). In addition, the organisational structure is such that the official involvement of development stops when the development has been handed over to the operations team. From then on, development's involvement is only indirect, through the established incident management and problem management processes.

The lesson learned is that better incentives must be used for the solutions development management and teams, in order to encourage quality in their work.

### EXAMPLE 17

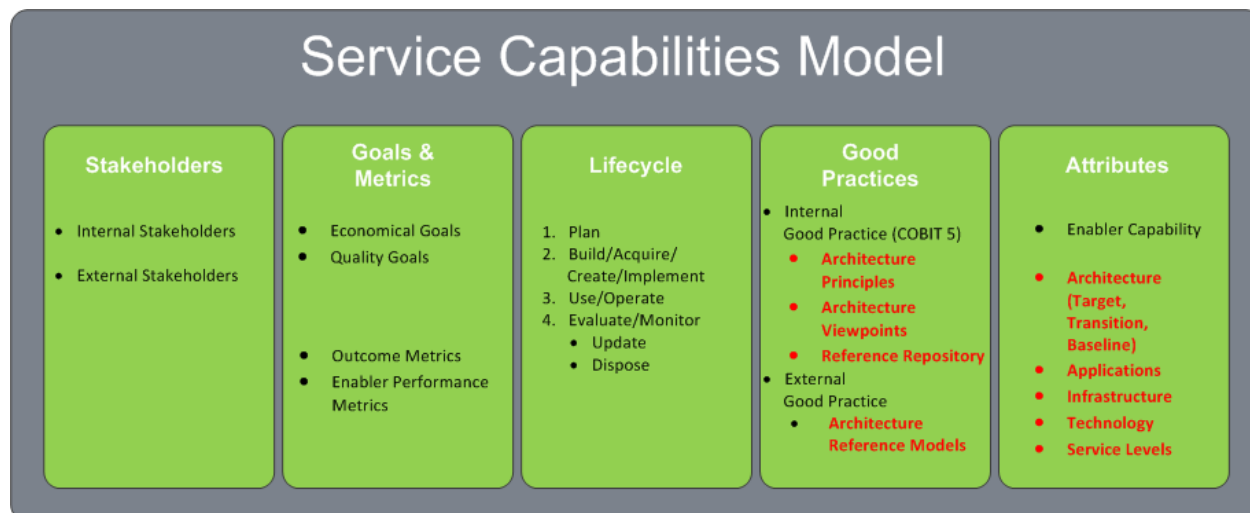
Some symptoms of an inadequate or problematic culture with regard to IT-related risk include:

- Misalignment between real risk appetite and translation into policies. Management's real values toward risk can be reasonably aggressive and risk-taking, whereas the policies that are created reflect a much more conservative attitude. Hence, there is a mismatch between values and the means to realise the values, inevitably leading to conflict. Conflicts may arise, for example, between the incentives set for management and the enforcement of misaligned policies.
- The existence of a 'blame culture'. This type of culture should by all means be avoided; it is the most effective inhibitor of relevant and efficient communication. In a blame culture, business units tend to point the finger at IT when projects are not delivered on time or do not meet expectations. In doing so, they fail to realise how the business unit's involvement up front affects project success. In extreme cases, the business unit may assign blame for a failure to meet the expectations that the unit never clearly communicated. The 'blame game' only detracts from effective communication across units, further fuelling delays. Executive leadership must identify and quickly control a blame culture if collaboration is to be fostered throughout the enterprise.

## COBIT 5 Service Capabilities Model

The service capabilities model, based on the generic COBIT 5 enabler model, is shown in **Figure 45**. Service capabilities refer to resources such as applications and infrastructures that are leveraged in the delivery of IT-related services.

Figure 45—COBIT 5 Service Capabilities Model



**Stakeholders** - Service capabilities stakeholders can be internal and external; services can be delivered by internal or external parties – think internal IT departments, operations managers, outsourcing providers; users of services can also be internal – think business users – and external to the organization, e.g. partners, clients, suppliers. The stakes of each of the stakeholders need to be identified and will either be focused on delivering adequate services, or on receiving required services from providers.

**Goals & Metrics** – Goals and metrics for service capabilities are linked to service levels, where both quality aspects and economical aspects will need to be defined.

**Life cycle**—Service capabilities have a life cycle. The future or planned service capabilities are typically described in a target architecture. It covers the building blocks, such as future applications and the target infrastructure model, and also describes the linkages and relationships amongst these building blocks.

The current service capabilities that are used or operated to deliver current IT services are described in a baseline architecture. Depending on the time frame of the target architecture, a transition architecture may also be defined, which shows the enterprise at incremental states between the target and baseline architectures.

**Good practices**—Good practice for service capabilities includes:

- Definition of architecture principles. Architecture principles are overall guidelines that govern the implementation and use of IT-related resources within the enterprise. Examples of potential architecture principles are:
  - **Re-use**—Common components of the architecture should be used when designing and implementing solutions as part of the target or transition architectures.
  - **Buy vs. build**—Solutions should be purchased unless there is an approved rationale for developing them internally.
  - **Simplicity**—The enterprise architecture should be designed and maintained to be as simple as possible while still meeting enterprise requirements.
  - **Agility**—The enterprise architecture should incorporate agility to meet changing business needs in an effective and efficient manner.
  - **Openness**—The enterprise architecture should leverage open industry standards.
- The enterprise’s definition of the most appropriate architecture viewpoints to meet the needs of different stakeholders. These are the models, catalogues and matrices used to describe the baseline, target or transition architectures. For example, an application architecture could be described through an application interface diagram, which shows the applications in use (or planned) and the interfaces amongst them.

- Having an architecture repository, which can be used to store different types of architectural outputs, including architecture principles and standards, architecture reference models, and other architecture deliverables

External good practice for architecture frameworks and service capabilities exist. These are guidelines, templates or standards that could be used to fast-track the creation of architecture deliverables. For example:

- The Open Group Architecture Framework (TOGAF)<sup>15</sup> provides a Technical Reference Model and an Integrated Information Infrastructure Reference Model.
- ITIL provides comprehensive guidance on how to design and operate services.

**Attributes**—Attributes specific for service capabilities include:

- The architecture viewpoints, as discussed previously
- Service levels that need to be defined and achieved by the service providers
- The building blocks of services, i.e.:
  - Applications, providing business functionality
  - Technology infrastructure, including hardware, system software, networking infrastructure, etc.
  - Physical infrastructure

**Relationships with other enablers**—There are links between service capabilities and other enablers in COBIT 5.

Information is one of the service capabilities, and service capabilities are leveraged through processes to deliver internal and external services.

Cultural and behavioural aspects are also relevant when a service-oriented culture needs to be built.

Within COBIT 5, the inputs and outputs of the management practices and activities could include service capabilities, which are required as inputs or delivered as outputs.

---

<sup>15</sup> [www.opengroup.org/togaf/](http://www.opengroup.org/togaf/)