ISACA®
Trust in, and value from, information systems

COBIT®

Enabling Processes

COBIT® 5
AN ISACA® FRAMEWORK

Personal Copy of: Dr. David Lanter

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

Disclaimer
ISACA has designed this publication, *COBIT® 5: Enabling Processes* (the 'Work'), primarily as an educational resource for governance of enterprise IT (GEIT), assurance, risk and security professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, readers should apply their own professional judgement to the specific GEIT, assurance, risk and security circumstances presented by the particular systems or information technology environment.

Copyright
© 2012 ISACA. All rights reserved. For usage guidelines, see *www.isaca.org/COBITuse*.

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

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

COBIT® 5: Enabling Processes
ISBN 978-1-60420-241-0
Print run 9

Personal Copy of: Dr. David Lanter

ACKNOWLEDGEMENTS

ISACA wishes to recognise:

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

Development Team
Floris Ampe, CISA, CGEIT, CIA, ISO 27000, PwC, Belgium
Gert du Preez, CGEIT, PwC, Canada
Stefanie Grijp, PwC, Belgium
Gary Hardy, CGEIT, IT Winners, South Africa
Bart Peeters, PwC, Belgium
Dirk Steuperaert, CISA, CGEIT, CRISC, IT In Balance BVBA, Belgium

Workshop Participants
Gary Baker, CGEIT, CA, Canada
Brian Barnier, CGEIT, CRISC, ValueBridge Advisors, USA
Johannes Hendrik Botha, MBCS-CITP, FSM, getITright Skills Development, South Africa
Ken Buechler, CGEIT, CRISC, PMP, Great-West Life, Canada
Don Caniglia, CISA, CISM, CGEIT, FLMI, USA
Mark Chaplin, UK
Roger Debreceny, Ph.D., CGEIT, FCPA, University of Hawaii at Manoa, USA
Mike Donahue, CISA, CISM, CGEIT, CFE, CGFM, CICA, Towson University, USA
Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Switzerland
Bob Frelinger, CISA, CGEIT, Oracle Corporation, USA
James Golden, CISM, CGEIT, CRISC, CISSP, IBM, USA
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, USA
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia
Nicole Lanza, CGEIT, IBM, USA
Philip Le Grand, PRINCE2, Ideagen Plc, UK
Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, USA
Stuart MacGregor, Real IRM Solutions (Pty) Ltd., South Africa
Christian Nissen, CISM, CGEIT, FSM, CFN People, Denmark
Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, UK
Eddy J. Schuermans, CGEIT, ESRAS bvba, Belgium
Michael Semrau, RWE Germany, Germany
Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Australia
Alan Simmonds, TOGAF9, TCSA, PreterLex, UK
Cathie Skoog, CISM, CGEIT, CRISC, IBM, USA
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Canada
Roger Southgate, CISA, CISM, UK
Nicky Tiesenga, CISA, CISM, CGEIT, CRISC, IBM, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Greet Volders, CGEIT, Voquals N.V., Belgium
Christopher Wilken, CISA, CGEIT, PwC, USA
Tim M. Wright, CISA, CRISC, CBCI, GSEC, QSA, Kingston Smith Consulting LLP, UK

Personal Copy of: Dr. David Lanter

Acknowledgements *(cont.)*

Expert Reviewers
Mark Adler, CISA, CISM, CGEIT, CRISC, Commercial Metals Company, USA
Wole Akpose, Ph.D., CGEIT, CISSP, Morgan State University, USA
Krzysztof Baczkiewicz, CSAM, CSOX, Eracent, Poland
Roland Bah, CISA, MTN Cameroon, Cameroon
Dave Barnett, CISSP, CSSLP, USA
Max Blecher, CGEIT, Virtual Alliance, South Africa
Ricardo Bria, CISA, CGEIT, CRISC, Meycor GRC, Argentina
Dirk Bruyndonckx, CISA, CISM, CGEIT, CRISC, MCA, KPMG Advisory, Belgium
Donna Cardall, UK
Debra Chiplin, Investors Group, Canada
Sara Cosentino, CA, Great-West Life, Canada
Kamal N. Dave, CISA, CISM, CGEIT, Hewlett Packard, USA
Philip de Picker, CISA, MCA, National Bank of Belgium, Belgium
Abe Deleon, CISA, IBM, USA
James Doss, ITIL Expert, TOGAF 9, PMP, SSGB, EMCCA, EMCISA, Oracle DBA, ITValueQuickStart.com, UK
Stephen Doyle, CISA, CGEIT, Department of Human Services, Australia
Heidi L. Erchinger, CISA, CRISC, CISSP, System Security Solutions, Inc., USA
Rafael Fabius, CISA, CRISC, Uruguay
Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Switzerland
Bob Frelinger, CISA, CGEIT, Oracle Corporation, USA
Kate Gentles, ITValueQuickStart.com, UK
Yalcin Gerek, CISA, CGEIT, CRISC, ITIL Expert, ITIL V3 Trainer, PRINCE2, ISO/IEC 20000 Consultant, Turkey
Edson Gin, CISA, CISM, CFE, CIPP, SSCP, USA
James Golden, CISM, CGEIT, CRISC, CISSP, IBM, USA
Marcelo Hector Gonzalez, CISA, CRISC, Banco Central Republic Argentina, Argentina
Erik Guldentops, University of Antwerp Management School, Belgium
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, USA
Angelica Haverblad, CGEIT, CRISC, ITIL, Verizon Business, Sweden
Kim Haverblad, CISM, CRISC, PCI QSA, Verizon Business, Sweden
J. Winston Hayden, CISA, CISM, CGEIT, CRISC, South Africa
Eduardo Hernandez, ITIL V3, HEME Consultores, Mexico
Jorge Hidalgo, CISA, CISM, CGEIT, ATC, Lic. Sistemas, 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 E. Jasinski, CISA, CGEIT, SSBB, ITIL Expert, USA
Masatoshi Kajimoto, CISA, CRISC, Japan
Joanna Karczewska, CISA, Poland
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia
Eddy Khoo S. K., Prudential Services Asia, Malaysia
Marty King, CISA, CGEIT, CPA, Blue Cross Blue Shield NC, USA
Alan S. Koch, ITIL Expert, PMP, ASK Process Inc., USA
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia
Jason D. Lannen, CISA, CISM, TurnKey IT Solutions, LLC, USA
Nicole Lanza, CGEIT, IBM, USA
Philip Le Grand, PRINCE2, Ideagen Plc, UK
Kenny Lee, CISA, CISM, CISSP, Bank of America, USA
Brian Lind, CISA, CISM, CRISC, Topdanmark Forsikring A/S, Denmark
Bjarne Lonberg, CISSP, ITIL, A.P. Moller - Maersk, Denmark
Stuart MacGregor, Real IRM Solutions (Pty) Ltd., South Africa
Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK
Cindy Marcello, CISA, CPA, FLMI, Great-West Life & Annuity, USA
Nancy McCuaig, CISSP, Great-West Life, Canada
John A. Mitchell, Ph.D., CISA, CGEIT, CEng, CFE, CITP, FBCS, FCIIA, QiCA, LHS Business Control, UK
Makoto Miyazaki, CISA, CPA, Bank of Tokyo-Mitsubishi, UFJ Ltd., Japan

Personal Copy of: Dr. David Lanter

Acknowledgements *(cont.)*

Expert Reviewers (cont.)
Lucio Augusto Molina Focazzio, CISA, CISM, CRISC, ITIL, Independent Consultant, Colombia
Christian Nissen, CISM, CGEIT, FSM, ITIL Expert, CFN People, Denmark
Tony Noblett, CISA, CISM, CGEIT, CISSP, USA
Ernest Pages, CISA, CGEIT, MCSE, ITIL, Sciens Consulting LLC, USA
Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, UK
Tom Patterson, CISA, CGEIT, CRISC, CPA, IBM, USA
Robert Payne, CGEIT, MBL, MCSSA, PrM, Lode Star Strategy Consulting, South Africa
Andy Piper, CISA, CISM, CRISC, PRINCE2, ITIL, Barclays Bank Plc, UK
Andre Pitkowski, CGEIT, CRISC, OCTAVE, ISO27000LA, ISO31000LA, APIT Consultoria de Informatica Ltd., Brazil
Geert Poels, Ghent University, Belgium
Dirk Reimers, Hewlett-Packard, Germany
Steve Reznik, CISA, ADP, Inc., USA
Robert Riley, CISSP, University of Notre Dame, USA
Martin Rosenberg, Ph.D., Cloud Governance Ltd., UK
Claus Rosenquist, CISA, CISSP, Nets Holding, Denmark
Jeffrey Roth, CISA, CGEIT, CISSP, L-3 Communications, USA
Cheryl Santor, CISSP, CNA, CNE, Metropolitan Water District, USA
Eddy J. Schuermans, CGEIT, ESRAS bvba, Belgium
Michael Semrau, RWE Germany, Germany
Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Australia
Alan Simmonds, TOGAF9, TCSA, PreterLex, UK
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Canada
Jennifer Smith, CISA, CIA, Salt River Pima Maricopa Indian Community, USA
Marcel Sorouni, CISA, CISM, CISSP, ITIL, CCNA, MCDBA, MCSE, Bupa Australia, Australia
Roger Southgate, CISA, CISM, UK
Mark Stacey, CISA, FCA, BG Group Plc, UK
Karen Stafford Gustin, MLIS, London Life Insurance Company, 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, CIA, Hitachi Consulting Co., Ltd., Japan
Rob van der Burg, Microsoft, The Netherlands
Johan van Grieken, CISA, CGEIT, CRISC, Deloitte, Belgium
Flip van Schalkwyk, Centre for e-Innovation, Western Cape Government, South Africa
Jinu Varghese, CISA, CISSP, ITIL, OCA, Ernst & Young, Canada
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, CISA, CRISC, CBCI, GSEC, QSA, 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
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, Inc., USA, Vice President
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vice President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (retired), USA, Past International President
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, UK, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Director

Personal Copy of: Dr. David Lanter

Acknowledgements *(cont.)*

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

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

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

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

Personal Copy of: Dr. David Lanter

Table of Contents

List of Figures 9

Chapter 1. Introduction 11

Chapter 2. The Goals Cascade and Metrics for Enterprise Goals and IT-related Goals 13
COBIT 5 Goals Cascade 13
Step 1. Stakeholder Drivers Influence Stakeholder Needs 13
Step 2. Stakeholder Needs Cascade to Enterprise Goals 13
Step 3. Enterprise Goals Cascade to IT-related Goals 15
Step 4. IT-related Goals Cascade to Enabler Goals 15
Using the COBIT 5 Goals Cascade 15
Benefits of the COBIT 5 Goals Cascade 15
Using the COBIT 5 Goals Cascade Carefully 16
Using the COBIT 5 Goals Cascade in Practice 16
Metrics 16
Enterprise Goal Metrics 16
IT-related Goal Metrics 17

Chapter 3. The COBIT 5 Process Model 19
Enabler Performance Management 21

Chapter 4. The COBIT 5 Process Reference Model 23
Governance and Management Processes 23
Model 23

Chapter 5. COBIT 5 Process Reference Guide Contents 25
Inputs and Outputs 25
Generic Guidance for Processes 27
Evaluate, Direct and Monitor (EDM) 29
Align, Plan and Organise (APO) 49
Build, Acquire and Implement (BAI) 117
Deliver, Service and Support (DSS) 171
Monitor, Evaluate and Assess (MEA) 201

Appendix A. Mapping Between COBIT 5 and Legacy ISACA Frameworks 217

Appendix B. Detailed Mapping Enterprise Goals—IT-related Goals 225

Appendix C. Detailed Mapping IT-related Goals—IT-related Processes 227

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

List of Figures

Figure 1—COBIT 5 Product Family....11
Figure 2—The Governance Objective: Value Creation....13
Figure 3—COBIT 5 Goals Cascade Overview....14
Figure 4—COBIT 5 Enterprise Goals....14
Figure 5—IT-related Goals....15
Figure 6—Enterprise Goal Sample Metrics....16
Figure 7—IT-related Goal Sample Metrics....17
Figure 8—COBIT 5 Enabler: Processes....19
Figure 9—COBIT 5 Governance and Management Key Areas....23
Figure 10—COBIT 5 Process Reference Model....24
Figure 11—Outputs....26
Figure 12—COBIT 4.1 Process Controls and Related ISO/IEC 15504 Process Capability Attributes....27
Figure 13—ISACA Frameworks Included in COBIT 5....217
Figure 14—COBIT 4.1 Control Objectives Mapped to COBIT 5....217
Figure 15—Val IT 2.0 Key Management Practices Covered by COBIT 5....222
Figure 16—Risk IT Key Management Practices Covered by COBIT 5....224
Figure 17—Mapping COBIT 5 Enterprise Goals to IT-related Goals....226
Figure 18—Mapping COBIT 5 IT-related Goals to Processes....227

Personal Copy of: Dr. David Lanter

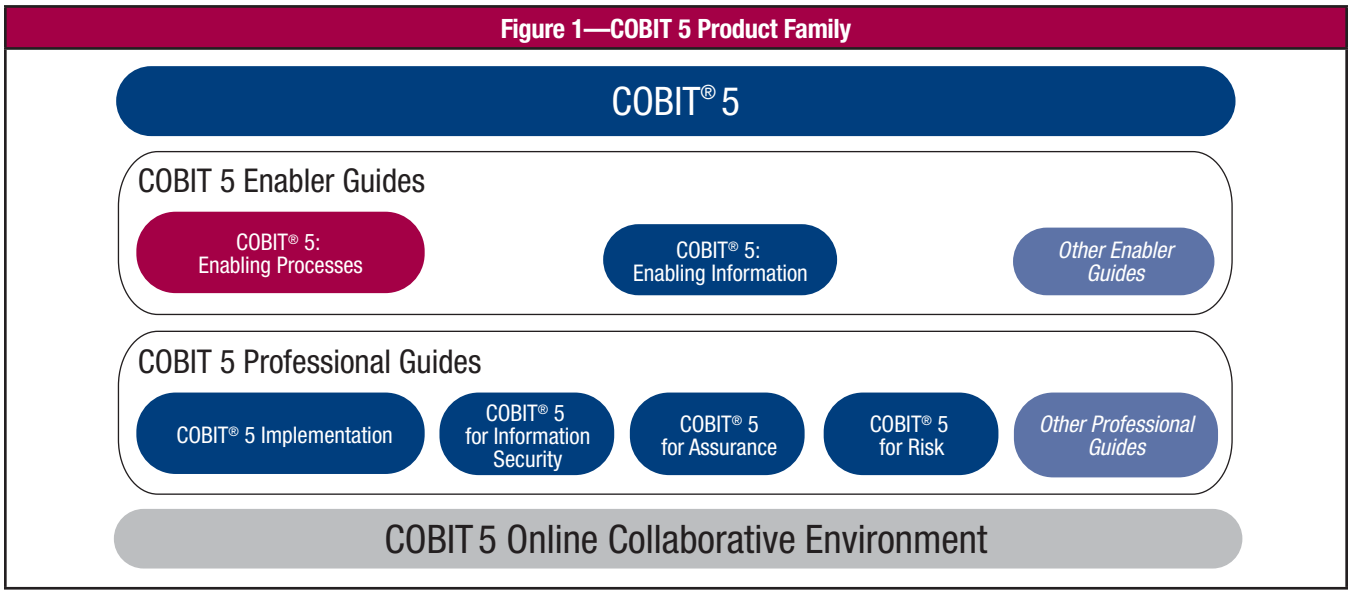
Page intentionally left blank

Personal Copy of: Dr. David Lanter

Chapter 1
Introduction

COBIT 5: Enabling Processes complements COBIT 5 (**figure 1**). This publication contains a detailed reference guide to the processes that are defined in the COBIT 5 process reference model.

Figure 1—COBIT 5 Product Family



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

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

This publication is structured as follows:
- In chapter 2, the COBIT 5 goals cascade—also explained in the COBIT 5 framework—is recapitulated and complemented with a set of example metrics for enterprise goals and IT-related goals.
- In chapter 3, the COBIT 5 process model is explained and its components defined. This chapter explains what information is included in the detailed process information section. The COBIT 5 process model includes 37 governance and management processes; this set of processes is the successor to the COBIT 4.1, Val IT and Risk IT processes, and includes all processes required for end-to-end treatment of governance and management of enterprise IT.
- Chapter 4 shows the diagram of the process reference model, which was developed based on good practices, standards and the opinion of experts. It is important to understand that the model and its contents are generic and not prescriptive, and it has to be adapted to suit the enterprise. Also, the guidance defines practices and activities at a relatively high level and does not describe how the process procedure is to be defined.
- Chapter 5—the main section in this publication—contains the detailed process information for all 37 COBIT 5 processes in the process reference model.
- A number of appendices are also included:
  - Appendix A contains a mapping between the COBIT 4.1, Val IT 2.0 and Risk IT processes (and their control objectives or management practices) and their COBIT 5 equivalents.
  - Appendices B and C contain the mapping tables from the goals cascade, i.e., mapping enterprise goals to IT-related goals and IT-related goals to processes.

Personal Copy of: Dr. David Lanter

Page intentionally left blank

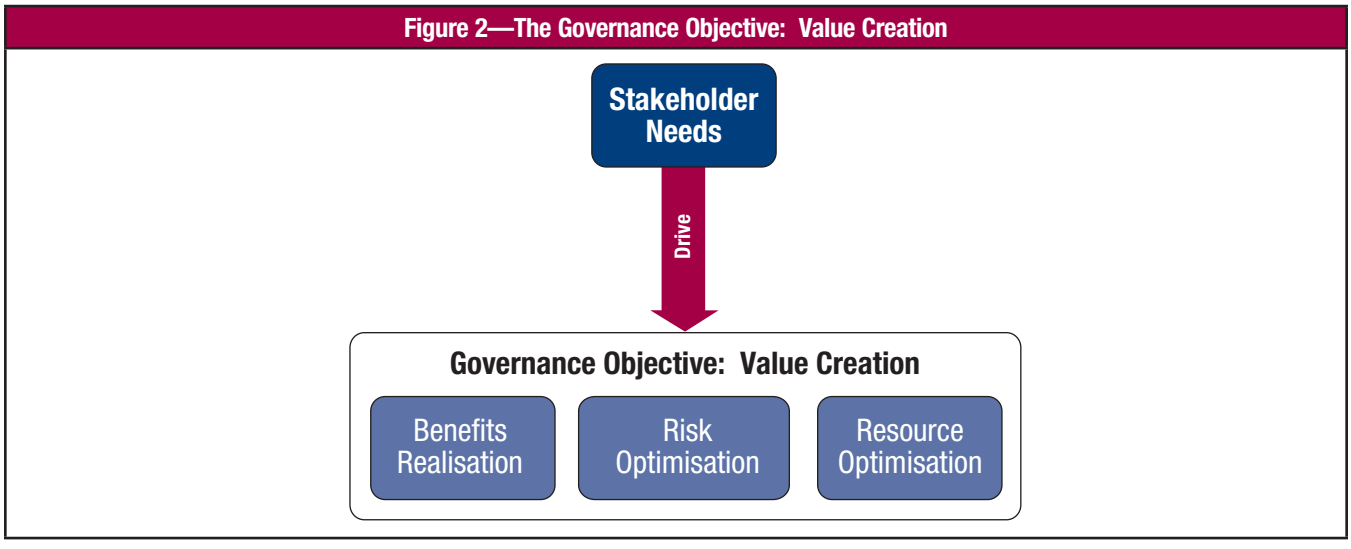
Personal Copy of: Dr. David Lanter

Chapter 2
The Goals Cascade and Metrics for Enterprise Goals and IT-related Goals

COBIT 5 Goals Cascade

Enterprises exist to create value for their stakeholders. Consequently, any enterprise—commercial or not—will have value creation as a governance objective. Value creation means realising benefits at an optimal resource cost while optimising risk. (See **figure 2**.) Benefits can take many forms, e.g., financial for commercial enterprises or public service for government entities.

Figure 2—The Governance Objective: Value Creation



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 should consider all stakeholders when making benefit, risk and resource assessment decisions. For each decision, the following questions can and should be asked: For whom are the benefits? Who bears the risk? What resources are required?

Stakeholder needs have to be transformed into an enterprise's actionable strategy. The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customised 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.

The COBIT 5 goals cascade is shown in **figure 3**.

Step 1. Stakeholder Drivers Influence Stakeholder Needs

Stakeholder needs are influenced by a number of drivers, e.g., strategy changes, a changing business and regulatory environment, and new technologies.

Step 2. Stakeholder Needs Cascade to Enterprise Goals

Stakeholder needs can be related to a set of generic enterprise goals. These enterprise goals have been developed using the balanced scorecard (BSC)[1] dimensions, and they represent a list of commonly used goals that an enterprise may define for itself. Although this list is not exhaustive, most enterprise-specific goals can be mapped easily onto one or more of the generic enterprise goals.

COBIT 5 defines 17 generic goals, as shown in **figure 4**, which includes the following information:
- The BSC dimension under which the enterprise goal fits
- Enterprise goals
- The relationship to the three main governance objectives—benefits realisation, risk optimisation and resource optimisation. ('P' stands for primary relationship and 'S' for secondary relationship, i.e., a less strong relationship.)

[1] Kaplan, Robert S.; David P. Norton; *The Balanced Scorecard: Translating Strategy into Action*, Harvard University Press, USA, 1996

Personal Copy of: Dr. David Lanter

Figure 3—COBIT 5 Goals Cascade Overview

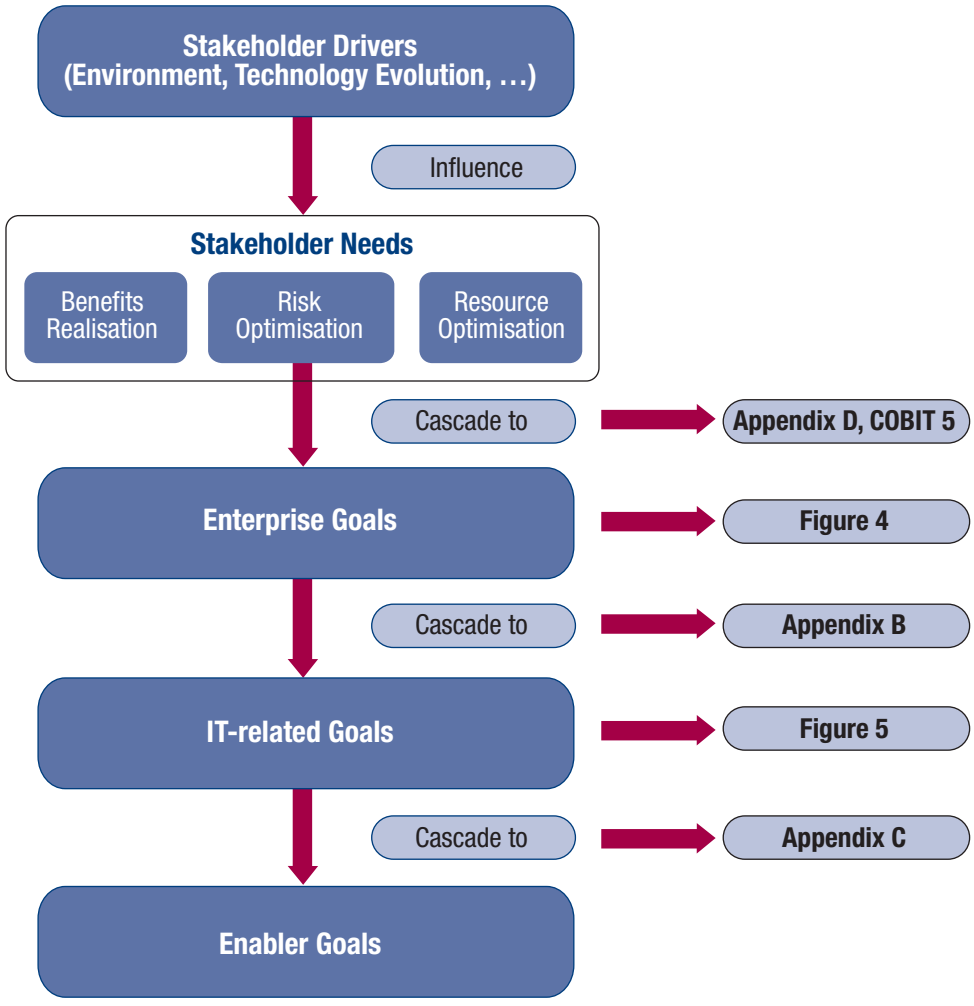


Figure 4—COBIT 5 Enterprise Goals

BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (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		P
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	P	P
	17. Product and business innovation culture	P		

Personal Copy of: Dr. David Lanter

Step 3. Enterprise Goals Cascade to IT-related Goals

Achievement of enterprise goals requires a number of IT-related outcomes,[2] which are represented by the IT-related goals. IT-related stands for information and related technology, and the IT-related goals are structured along the dimensions of the IT balanced scorecard (IT BSC). COBIT 5 defines 17 IT-related goals, listed in **figure 5**.

Figure 5—IT-related Goals

IT BSC Dimension	Information and Related Technology Goal	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
	06	Transparency of IT costs, benefits and risk
Customer	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
Internal	09	IT agility
	10	Security of information, 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 delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

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

Step 4. IT-related Goals Cascade to Enabler Goals

Achieving IT-related goals requires the successful application and use of a number of enablers. Enablers include:
- Principles, policies and frameworks
- Processes
- Organisational structures
- Culture, ethics and behaviour
- Information
- Services, infrastructure and applications
- People, skills and competencies

For each enabler a set of specific, relevant goals can be defined in support of the IT-related goals. In this document, process goals are provided in the detailed process descriptions. Processes are one of the enablers, and appendix C contains a mapping between IT-related goals and COBIT 5 processes.

Using the COBIT 5 Goals Cascade

Benefits of the COBIT 5 Goals Cascade

The goals cascade[3] is important, because it allows the definition of priorities for implementation, improvement and assurance of governance of enterprise IT based on (strategic) objectives of the enterprise and the related risk. 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

[2] IT-related outcomes obviously are 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.
[3] The goals cascade is based on research performed by the University of Antwerp Management School IT Alignment and Governance Institute in Belgium.

Personal Copy of: Dr. David Lanter

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 enablers (including 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 interrelated.
- 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 in Practice

From the previous 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. In other words, each enterprise should build its own goals cascade, compare it with COBIT and then refine it.

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.

Metrics

The following pages contain the enterprise goals and IT-related goals, with sample metrics that can be used to measure the achievement of each goal. These metrics are samples, and every enterprise should carefully review the list, decide on relevant and achievable metrics for its own environment, and design its own scorecard system. In addition to the metrics below, process goals and metrics are contained in the detailed process descriptions.

Enterprise Goal Metrics

Figure 6 contains all enterprise goals as identified in the framework publication, with sample metrics for each.

Figure 6—Enterprise Goal Sample Metrics

BSC Dimension	Enterprise Goal	Metric
Financial	1. Stakeholder value of business investments	• Percent of investments where value delivered meets stakeholder expectations • Percent of products and services where expected benefits are realised • Percent of investments where claimed benefits are met or exceeded
	2. Portfolio of competitive products and services	• Percent of products and services that meet or exceed targets in revenues and/or market share • Ratio of products and services per life cycle phase • Percent of products and services that meet or exceed customer satisfaction targets • Percent of products and services that provide competitive advantage
	3. Managed business risk (safeguarding of assets)	• Percent of critical business objectives and services covered by risk assessment • Ratio of significant incidents that were not identified in risk assessments vs. total incidents • Frequency of update of risk profile
	4. Compliance with external laws and regulations	• Cost of regulatory non-compliance, including settlements and fines • Number of regulatory non-compliance issues causing public comment or negative publicity • Number of regulatory non-compliance issues relating to contractual agreements with business partners
	5. Financial transparency	• Percent of investment business cases with clearly defined and approved expected costs and benefits • Percent of products and services with defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information • Percent of service cost that can be allocated to users

Personal Copy of: Dr. David Lanter

Figure 6—Enterprise Goal Sample Metrics *(cont.)*		
BSC Dimension	**Enterprise Goal**	**Metric**
Customer	6. Customer-oriented service culture	• Number of customer service disruptions due to IT service-related incidents (reliability) • Percent of business stakeholders satisfied that customer service delivery meets agreed-on levels • Number of customer complaints • Trend of customer satisfaction survey results
	7. Business service continuity and availability	• Number of customer service interruptions causing significant incidents • Business cost of incidents • Number of business processing hours lost due to unplanned service interruptions • Percent of complaints as a function of committed service availability targets
	8. Agile responses to a changing business environment	• Level of board satisfaction with enterprise responsiveness to new requirements • Number of critical products and services supported by up-to-date business processes • Average time to turn strategic enterprise objectives into an agreed-on and approved initiative
	9. Information-based strategic decision making	• Degree of board and executive management satisfaction with decision making • Number of incidents caused by incorrect business decisions based on inaccurate information • Time to provide supporting information to enable effective business decisions
	10. Optimisation of service delivery costs	• Frequency of service delivery cost optimisation assessments • Trend of cost assessment vs. service level results • Satisfaction levels of board and executive management with service delivery costs
Internal	11. Optimisation of business process functionality	• Frequency of business process capability maturity assessments • Trend of assessment results • Satisfaction levels of board and executives with business process capabilities
	12. Optimisation of business process costs	• Frequency of business process cost optimisation assessments • Trend of cost assessment vs. service level results • Satisfaction levels of board and executive management with business processing costs
	13. Managed business change programmes	• Number of programmes on time and within budget • Percent of stakeholders satisfied with programme delivery • Level of awareness of business change induced by IT-enabled business initiatives
	14. Operational and staff productivity	• Number of programmes/projects on time and within budget • Cost and staffing levels compared to benchmarks
	15. Compliance with internal policies	• Number of incidents related to non-compliance to policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices
Learning and Growth	16. Skilled and motivated people	• Level of stakeholder satisfaction with staff expertise and skills • Percent of staff whose skills are insufficient for the competency required for their role • Percent of satisfied staff
	17. Product and business innovation culture	• Level of awareness and understanding of business innovation opportunities • Stakeholder satisfaction with levels of product and innovation expertise and ideas • Number of approved product and service initiatives resulting from innovative ideas

IT-related Goal Metrics

Figure 7 contains all IT-related goals as defined in the goals cascade and includes sample metrics for each goal.

Figure 7—IT-related Goal Sample Metrics		
BSC Dimension	**IT-related Goal**	**Metric**
Financial	01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
	02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
	03 Commitment of executive management for making IT-related decisions	• Percent of executive management roles with clearly defined accountabilities for IT decisions • Number of times IT is on the board agenda in a proactive manner • Frequency of IT strategy (executive) committee meetings • Rate of execution of executive IT-related decisions

Personal Copy of: Dr. David Lanter

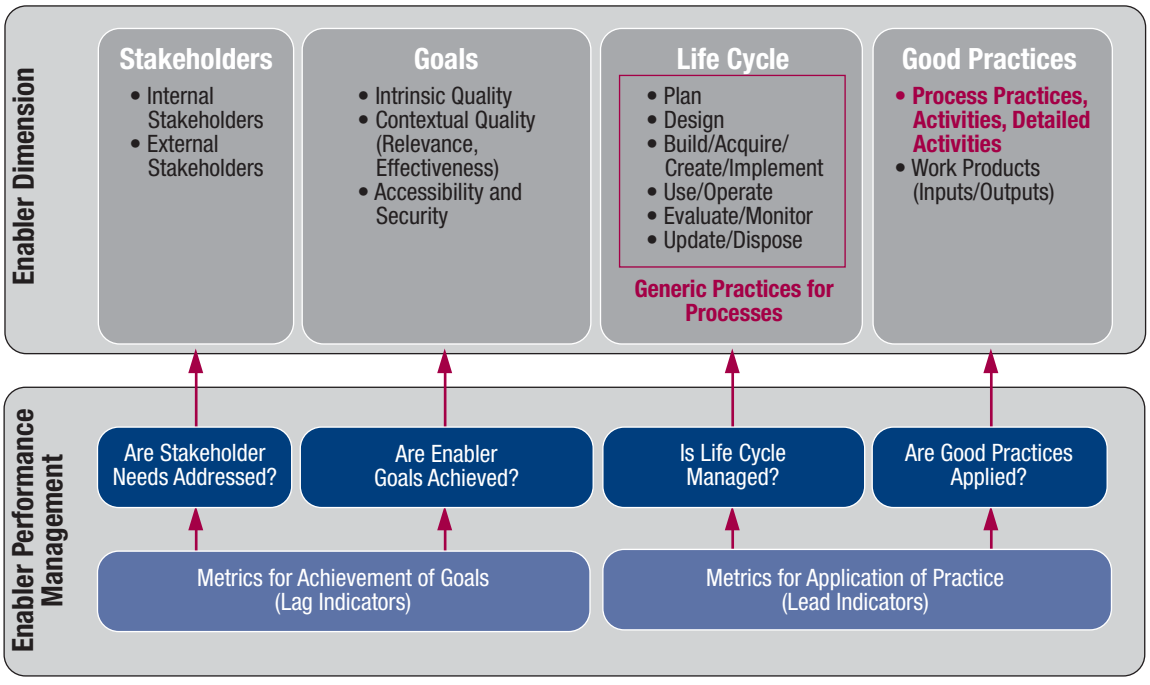
Figure 7—IT-related Goal Sample Metrics *(cont.)*		
BSC Dimension	**IT-related Goal**	**Metric**
Financial *(cont.)*	04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
	05 Realised benefits from IT-enabled investments and services portfolio	• Percent of IT-enabled investments where benefit realisation is monitored through the full economic life cycle • Percent of IT services where expected benefits are realised • Percent of IT-enabled investments where claimed benefits are met or exceeded
	06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information
Customer	07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
	08 Adequate use of applications, information and technology solutions	• Percent of business process owners satisfied with supporting IT products and services • Level of business user understanding of how technology solutions support their processes • Satisfaction level of business users with training and user manuals • Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions
Internal	09 IT agility	• Level of satisfaction of business executives with IT's responsiveness to new requirements • Number of critical business processes supported by up-to-date infrastructure and applications • Average time to turn strategic IT objectives into an agreed-on and approved initiative
	10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines
	11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
	12 Enablement and support of business processes by integrating applications and technology into business processes	• Number of business processing incidents caused by technology integration errors • Number of business process changes that need to be delayed or reworked because of technology integration issues • Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues • Number of applications or critical infrastructures operating in silos and not integrated
	13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	• Number of programmes/projects on time and within budget • Percent of stakeholders satisfied with programme/project quality • Number of programmes needing significant rework due to quality defects • Cost of application maintenance vs. overall IT cost
	14 Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor
	15 IT compliance with internal policies	• Number of incidents related to non-compliance to policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices • Frequency of policies review and update
Learning and Growth	16 Competent and motivated business and IT personnel	• Percent of staff whose IT-related skills are sufficient for the competency required for their role • Percent of staff satisfied with their IT-related roles • Number of learning/training hours per staff member
	17 Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of IT innovation possibilities • Level of stakeholder satisfaction with levels of IT innovation expertise and ideas • Number of approved initiatives resulting from innovative IT ideas

Personal Copy of: Dr. David Lanter

Chapter 3
The COBIT 5 Process Model

Processes are one of the seven enabler categories for governance and management of enterprise IT, as explained in COBIT 5, chapter 5. The specifics for the processes enabler compared to the generic enabler description are shown in **figure 8**.

Figure 8—COBIT 5 Enabler: Processes



A process is defined as **'a collection of practices influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs (e.g., products, services)'.**

The process model shows:

- **Stakeholders**—Processes have internal and external stakeholders, with their own roles; stakeholders and their responsibility levels are documented in charts that show who is responsible, accountable, consulted or informed (RACI). External stakeholders include customers, business partners, shareholders and regulators. Internal stakeholders include board, management, staff and volunteers.
- **Goals**—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.

  Process goals can be categorised as:
  - **Intrinsic goals**—Does the process have intrinsic quality? Is it accurate and in line with good practice? Is it compliant with internal and external rules?
  - **Contextual goals**—Is the process customised and adapted to the enterprise's specific situation? Is the process relevant, understandable, easy to apply?
  - **Accessibility and security goals**—The process remains confidential, when required, and is known and accessible to those who need it.

  At each level of the goals cascade, hence also for processes, metrics are defined to measure the extent to which 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'.

Personal Copy of: Dr. David Lanter

To manage the enabler effectively and efficiently, metrics need to be defined to measure the extent to which the expected outcomes are achieved. In addition, a second aspect of performance management of the enabler describes the extent to which good practice is applied. Here also, associated metrics can be defined to help with the management of the enabler.

- **Life cycle**—Each process has a life cycle. It is defined, created, operated, monitored, and adjusted/updated or retired. Generic process practices such as those defined in the COBIT process assessment model based on ISO/IEC 15504 can assist with defining, running, monitoring and optimising processes.
- **Good practices**—*COBIT 5: Enabling Processes* contains a process reference model, in which process internal good practices are described in growing levels of detail: practices, activities and detailed activities.[4]

Practices:

- For each COBIT 5 process, the governance/management practices provide a complete set of high-level requirements for effective and practical governance and management of enterprise IT. They are:
  - Statements of actions to deliver benefits, optimise the level of risk and optimise the use of resources
  - Aligned with relevant generally accepted standards and good practices
  - Generic and therefore needing to be adapted for each enterprise
  - Covering business and IT role players in the process (end to end)
- The enterprise governance body and management need to make choices relative to these governance and management practices by:
  - Selecting those that are applicable and deciding upon those that will be implemented
  - Adding and/or adapting practices where required
  - Defining and adding non-IT-related practices for integration in business processes
  - Choosing how to implement them (frequency, span, automation, etc.)
  - Accepting the risk of not implementing those that may apply

Activities—In COBIT the main actions to operate the process

- They are defined as 'guidance to achieve 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 or management practice to improve IT performance and/or address IT solution and service delivery risk. This material is of use to:
  - Management, service providers, end users and IT professionals who need to plan, build, run or monitor (PBRM) enterprise IT
  - Assurance professionals who may be asked for their opinions regarding current or proposed implementations or necessary improvements
- A complete set of generic and specific activities that provide one approach consisting of all the steps that are necessary and sufficient for achieving the key governance practice (GP)/management practice (MP). They provide high-level guidance, at a level below the GP/MP, for assessing actual performance and for considering potential improvements. The activities:
  - Describe a set of necessary and sufficient action-oriented implementation steps to achieve a GP/MP
  - Consider the inputs and outputs of the process
  - Are based on generally accepted standards and good practices
  - Support establishment of clear roles and responsibilities
  - Are non-prescriptive, and need to be adapted and developed into specific procedures appropriate for the enterprise

Detailed activities—The activities may not be at a sufficient level of detail for implementation, and further guidance may need to be:

- Obtained from specific relevant standards and good practices such as Information Technology Infrastructure Library (ITIL), the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 series and PRojects IN Controlled Environments 2 (PRINCE2)
- Developed as more detailed or specific activities as additional developments in the COBIT 5 product family itself

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.[5]

> *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 practices at all times, knowing that COBIT is aligned with these standards where relevant, and mapping information will be made available.*

[4] Only practices and activities are developed under the current project. The more detailed levels are subject to additional development(s), e.g., the various professional guides may provide more detailed guidance for their areas. Also, further guidance can be obtained through related standards and frameworks, as indicated in the detailed process descriptions.

[5] The illustrative COBIT 5 inputs and outputs should not be regarded as an exhaustive list because additional information flows could be defined, depending on a particular enterprise's environment and process framework.

Personal Copy of: Dr. David Lanter

Enabler Performance Management

Enterprises expect positive outcomes from the application and use of enablers. To manage performance of the enablers, the following questions will have to be monitored and answered—based on metrics—on a regular basis:
- Are stakeholder needs addressed?
- Are enabler goals achieved?
- Is the enabler life cycle managed?
- Are good practices applied?

In the case of the process enabler, the first two bullets deal with the actual outcome of the process. The metrics used to measure the extent to which the goals are achieved can be called 'lag indicators'. In *COBIT 5: Enabling Processes*, a number of metrics are defined per process goal.

The last two bullets deal with the actual functioning of the enabler itself, and metrics for this can be called 'lead indicators'.

Process capability level—COBIT 5 includes an ISO/IEC 15504-based process capability assessment scheme. This is discussed in chapter 8 of COBIT 5 and further guidance is available from separate ISACA publications. In brief, the process capability level measures both achievement of goals and application of good practice.

Relationships with other enablers—Links between processes and the other enabler categories exist through the following relationships:
- Processes need information (as one of the types of inputs) and can produce information (as a work product).
- Processes need organisational structures and roles to operate, as expressed through the RACI charts, e.g., IT steering committee, enterprise risk committee, board, audit, chief information officer (CIO), chief executive officer (CEO).
- Processes produce, and also require, service capabilities (infrastructure, applications, etc.).
- Processes can, and will, depend on other processes.
- Processes produce, or need, policies and procedures to ensure consistent implementation and execution.
- Cultural and behavioural aspects determine how well processes are executed.

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

Chapter 4
The 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 enterprise would be expected to implement a number of governance processes and a number of management processes 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 within the objectives of the processes:

- **Governance processes**—Governance processes deal with the stakeholder governance objectives—value delivery, risk optimisation and resource optimisation—and include practices and activities aimed at evaluating strategic options, providing direction to IT and monitoring the outcome (Evaluate, direct and monitor [EDM]—in line with the ISO/IEC 38500 standard concepts).
- **Management processes**—In line with the definition of management (see COBIT 5, Executive Summary), practices and activities in management processes cover the responsibility areas of PBRM enterprise IT, and they have to provide end-to-end coverage of IT.

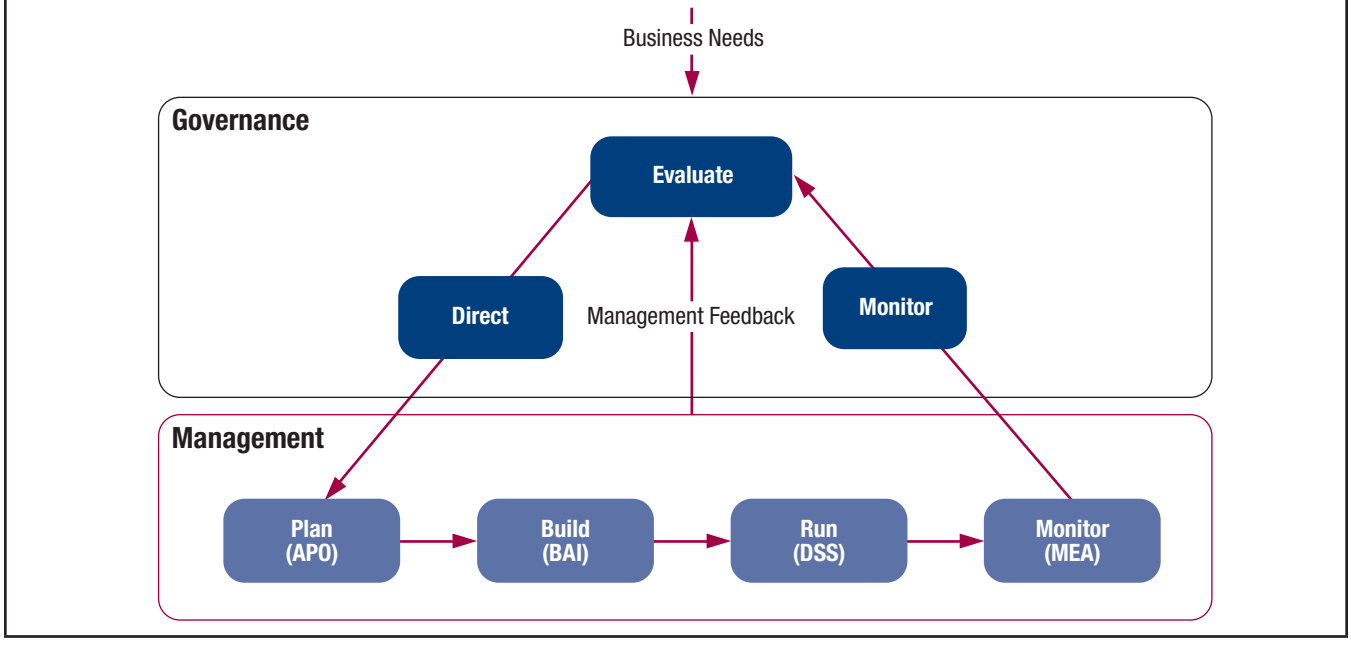
Although the outcome of both types of processes is different and intended for a different audience, internally, from the context of the process itself, all processes require 'planning', 'building or implementation', 'execution' and 'monitoring' activities within the process.

Model

COBIT 5 is not prescriptive, but from the previous text it is clear that it advocates that enterprises implement governance and management processes such that the key areas are covered, as shown in **figure 9**.

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 may have fewer processes; larger and more complex enterprises may have many processes, all to cover the same objectives.

Figure 9—COBIT 5 Governance and Management Key Areas



Personal Copy of: Dr. David Lanter

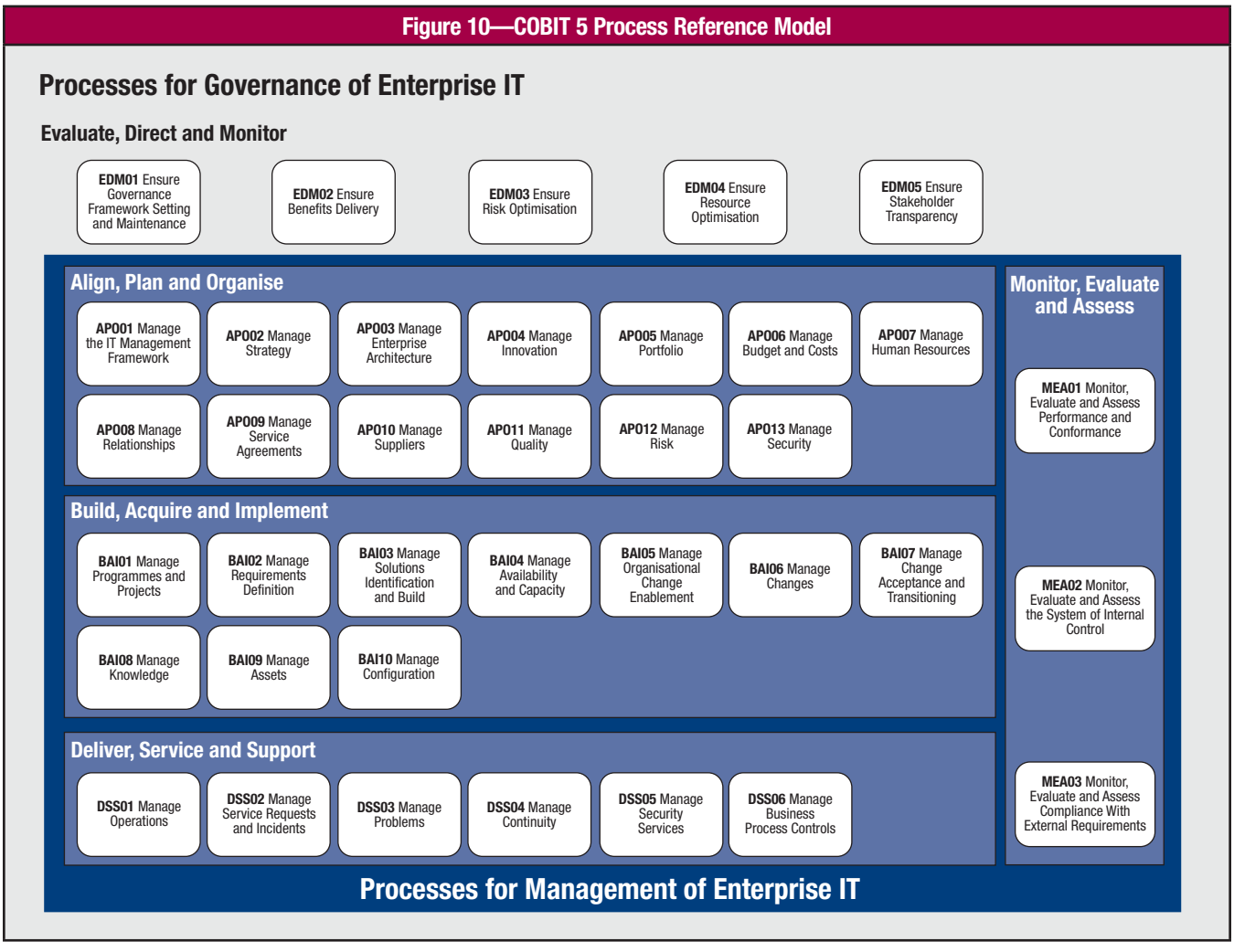
COBIT 5 includes a process reference model, defining and describing in detail a number of governance and management processes. It provides a process reference model that represents all of the processes normally found in an enterprise relating to IT activities, offering a common reference model understandable 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 enterprise involved in IT activities is one of the most important and critical steps towards 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 subdivides the governance and management processes of enterprise IT into two main areas of activity—governance and management—divided into domains of processes:
- **Governance**—This domain contains five governance processes; within each process, EDM practices are defined.
- **Management**—These four domains are in line with the responsibility areas of PBRM (an evolution of the COBIT 4.1 domains), and they provide end-to-end coverage of IT. Each domain contains a number of processes, as in COBIT 4.1 and 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.

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 10** shows the complete set of 37 governance and management processes within COBIT 5.

Figure 10—COBIT 5 Process Reference Model



Personal Copy of: Dr. David Lanter

Chapter 5
COBIT 5 Process Reference Guide Contents

This chapter describes the detailed process-related content for the COBIT 5 governance and management processes. For each process the following information is included, in line with the process model explained in the previous chapter:

- **Process identification**—On the first page:
  - Process label—The domain prefix (EDM, APO, BAI, DSS, MEA) and the process number
  - Process name—A short description, indicating the main subject of the process
  - Area of the process—Governance or management
  - Domain name
- **Process description**—An overview of what the process does and a high-level overview of how the process accomplishes its purpose
- **Process purpose statement**—A description of the overall purpose of the process
- **Goals cascade information**—Reference and description of the IT-related goals that are primarily supported by the process,[6] and metrics to measure the achievement of the IT-related goals
- **Process goals and metrics**—A set of process goals and a limited number of example metrics
- **RACI chart**—A suggested assignment of level of responsibility for process practices to different roles and structures. The enterprise roles listed are shaded darker than the IT roles. The different levels of involvement are:
  - R(esponsible)—**Who is getting the task done?** This refers to the roles taking the main operational stake in fulfilling the activity listed and creating the intended outcome
  - A(ccountable)—**Who accounts for the success of the task?** This assigns the overall accountability for getting the task done (Where does the buck stop?). Note that the role mentioned is the lowest appropriate level of accountability; there are, of course, higher levels that are accountable, too. To enable empowerment of the enterprise, accountability is broken down as far as possible. Accountability does not indicate that the role has no operational activities; it is very likely that the role gets involved in the task. As a principle, accountability cannot be shared.
  - C(onsulted)—**Who is providing input?** These are key roles that provide input. Note that it is up to the accountable and responsible role(s) to obtain information from other units or external partners, too. However, inputs from the roles listed are to be considered and, if required, appropriate action has to be taken for escalation, including the information of the process owner and/or the steering committee.
  - I(nformed)—**Who is receiving information?** These are roles who are informed of the achievements and/or deliverables of the task. The role in 'accountable', of course, should always receive appropriate information to oversee the task, as does the responsible roles for their area of interest.
- **Detailed description of the process practices**—For each practice:
  - Practice title and description
  - Practice inputs and outputs, with indication of origin and destination
  - Process activities, further detailing the practices
- **Related guidance**—References to other standards and direction to additional guidance

Inputs and Outputs

The detailed process descriptions contain—at the level of the governance and management practices—inputs and outputs. In general, each output is sent to one or a limited number of destinations, typically another COBIT process practice. That output then becomes an input to its destination. However, there are a number of outputs that have many destinations, e.g., all COBIT processes, or all processes within a domain. For readability reasons, these outputs are NOT listed as inputs in these processes. A complete list of such outputs is included in **figure 11**.

For some inputs/outputs, the destination 'internal' is mentioned. This means that the input/output is between activities within the same process.

[6] Only the IT-related goals with a 'P' in the mapping table between IT-related goals and processes (**figure 17**) are listed here.

Personal Copy of: Dr. David Lanter

Figure 11—Outputs		
Outputs to all Processes		
From Practice	**Output Description**	**Destination**
APO13.02	Information security risk treatment plan	All EDM; All APO; All BAI; All DSS; All MEA
Outputs to all Governance Processes		
From Practice	**Output Description**	**Destination**
EDM01.01	Enterprise governance guiding principles	All EDM
EDM01.01	Decision-making model	All EDM
EDM01.01	Authority levels	All EDM
EDM01.02	Enterprise governance communications	All EDM
EDM01.03	Feedback on governance effectiveness and performance	All EDM
Outputs to all Management Processes		
From Practice	**Output Description**	**Destination**
APO01.01	Communication ground rules	All APO; All BAI; All DSS; All MEA
APO01.03	IT-related policies	All APO; All BAI; All DSS; All MEA
APO01.04	Communication on IT objectives	All APO; All BAI; All DSS; All MEA
APO01.07	Process improvement opportunities	All APO; All BAI; All DSS; All MEA
APO02.06	Communication package	All APO; All BAI; All DSS; All MEA
APO11.02	Quality management standards	All APO; All BAI; All DSS; All MEA
APO11.04	Process quality of service goals and metrics	All APO; All BAI; All DSS; All MEA
APO11.06	Communications on continual improvement and good practices	All APO; All BAI; All DSS; All MEA
APO11.06	Examples of good practice to be shared	All APO; All BAI; All DSS; All MEA
APO11.06	Quality review benchmark results	All APO; All BAI; All DSS; All MEA
MEA01.02	Monitoring targets	All APO; All BAI; All DSS; All MEA
MEA01.04	Performance reports	All APO; All BAI; All DSS; All MEA
MEA01.05	Remedial actions and assignments	All APO; All BAI; All DSS; All MEA
MEA02.01	Results of internal control monitoring and reviews	All APO; All BAI; All DSS; All MEA
MEA02.01	Results of benchmarking and other evaluations	All APO; All BAI; All DSS; All MEA
MEA02.03	Self-assessment plans and criteria	All APO; All BAI; All DSS; All MEA
MEA02.03	Results of reviews of self-assessments	All APO; All BAI; All DSS; All MEA
MEA02.04	Control deficiencies	All APO; All BAI; All DSS; All MEA
MEA02.04	Remedial actions	All APO; All BAI; All DSS; All MEA
MEA02.06	Assurance plans	All APO; All BAI; All DSS; All MEA
MEA02.08	Refined scope	All APO; All BAI; All DSS; All MEA
MEA02.08	Assurance review results	All APO; All BAI; All DSS; All MEA
MEA02.08	Assurance review report	All APO; All BAI; All DSS; All MEA
MEA03.02	Communications of changed compliance requirements	All APO; All BAI; All DSS; All MEA

Personal Copy of: Dr. David Lanter

Generic Guidance for Processes

The activities in the detailed process descriptions describe the functional purpose of the process—what the process is supposed to deliver. These will be different for every process, because every process has different process goals.

There is also guidance on how the process will be executed, i.e., generic guidance on how to build, execute, monitor and improve the process itself. This guidance is generic—identical for each process.

In COBIT 4.1, the process controls contained good practices that were not specific to any process, but were generic and applicable to all processes. The process controls were similar to some of the generic maturity attributes in the COBIT 4.1 maturity model.

In COBIT 5, an ISO/IEC 15504-compliant process capability assessment scheme is used. In this scheme, the capability attributes belonging to the higher process capability levels describe how better and more capable processes can be built, thus effectively replacing the COBIT 4.1 process controls.

This is important process-related guidance, and for that reason **figure 12** contains a high-level overview of both COBIT 4.1 process controls and their equivalent ISO/IEC 15504-based process capability attributes that are foundational to good processes.

Figure 12—COBIT 4.1 Process Controls and Related ISO/IEC 15504 Process Capability Attributes

COBIT 4.1		Related ISO/IEC 15504 Process Capability Attributes	
PC1	Process Goals and Objectives	PA 2.1	Performance management attribute
PC2	Process Ownership	PA 2.1	Performance management attribute
PC3	Process Repeatability	PA 3.1	Process definition attribute
PC4	Roles and Responsibilities	PA 2.1 PA 3.2	Performance management attribute Process deployment attribute
PC5	Policy, Plans and Procedures	PA 2.1	Performance management attribute
PC6	Process Performance Improvement	PA 2.1 PA 5.2	Performance management attribute Process optimization attribute

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

Evaluate, Direct and Monitor (EDM)

01 Ensure governance framework setting and maintenance.

02 Ensure benefits delivery.

03 Ensure risk optimisation.

04 Ensure resource optimisation.

05 Ensure stakeholder transparency.

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

EDM01 Ensure Governance Framework Setting and Maintenance	Area: Governance Domain: Evaluate, Direct and Monitor
Process Description Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.	
Process Purpose Statement Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
03 Commitment of executive management for making IT-related decisions	• Percent of executive management roles with clearly defined accountabilities for IT decisions • Number of times IT is on the board agenda in a proactive manner • Frequency of IT strategy (executive) committee meetings • Rate of execution of executive IT-related decisions
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Strategic decision-making model for IT is effective and aligned with the enterprise's internal and external environment and stakeholder requirements.	• Actual vs. target cycle time for key decisions • Level of stakeholder satisfaction (measured through surveys)
2. The governance system for IT is embedded in the enterprise.	• Number of roles, responsibilities and authorities that are defined, assigned and accepted by appropriate business and IT management • Degree by which agreed-on governance principles for IT are evidenced in processes and practices (percentage of processes and practices with clear traceability to principles) • Number of instances of non-compliance with ethical and professional behaviour guidelines
3. Assurance is obtained that the governance system for IT is operating effectively.	• Frequency of independent reviews of governance of IT • Frequency of governance of IT reporting to the executive committee and board • Number of governance of IT issues reported

EDM01 RACI Chart

Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM01.01 Evaluate the governance system.	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C					
EDM01.02 Direct the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
EDM01.03 Monitor the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

EDM01 Process Practices, Inputs/Outputs and Activities				
Governance Practice	**Inputs**		**Outputs**	
EDM01.01 Evaluate the governance system. Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make a judgement on the current and future design of governance of enterprise IT.	**From**	**Description**	**Description**	**To**
	MEA03.02	Communications of changed compliance requirements	Enterprise governance guiding principles	All EDM APO01.01 APO01.03
	Outside COBIT	• Business environment trends • Regulations • Governance/decision-making model guidance • Constitution/bylaws/ statutes of organisation	Decision-making model	All EDM APO01.01
			Authority levels	All EDM APO01.02
Activities				
1. Analyse and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design.				
2. Determine the significance of IT and its role with respect to the business.				
3. Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise IT.				
4. Align the ethical use and processing of information and its impact on society, natural environment, and internal and external stakeholder interests with the enterprise's direction, goals and objectives.				
5. Determine the implications of the overall enterprise control environment with regard to IT.				
6. Articulate principles that will guide the design of governance and decision making of IT.				
7. Understand the enterprise's decision-making culture and determine the optimal decision-making model for IT.				
8. Determine the appropriate levels of authority delegation, including threshold rules, for IT decisions.				
Governance Practice	**Inputs**		**Outputs**	
EDM01.02 Direct the governance system. Inform leaders and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed-on governance design principles, decision-making models and authority levels. Define the information required for informed decision making.	**From**	**Description**	**Description**	**To**
			Enterprise governance communications	All EDM APO01.04
			Reward system approach	APO07.03 APO07.04
Activities				
1. Communicate governance of IT principles and agree with executive management on the way to establish informed and committed leadership.				
2. Establish or delegate the establishment of governance structures, processes and practices in line with agreed-on design principles.				
3. Allocate responsibility, authority and accountability in line with agreed-on governance design principles, decision-making models and delegation.				
4. Ensure that communication and reporting mechanisms provide those responsible for oversight and decision-making with appropriate information.				
5. Direct that staff follow relevant guidelines for ethical and professional behaviour and ensure that consequences of non-compliance are known and enforced.				
6. Direct the establishment of a reward system to promote desirable cultural change.				

Personal Copy of: Dr. David Lanter

EDM01 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Governance Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
EDM01.03 Monitor the governance system. Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.	MEA01.04	Performance reports	Feedback on governance effectiveness and performance	All EDM APO01.07
	MEA01.05	Status and results of actions		
	MEA02.01	• Results of benchmarking and other evaluations • Results of internal control monitoring and reviews		
	MEA02.03	Results of reviews of self-assessments		
	MEA02.06	Assurance plans		
	MEA03.03	Compliance confirmations		
	MEA03.04	• Reports of non-compliance issues and root causes • Compliance assurance reports		
	Outside COBIT	• Obligations • Audit reports		
Activities				
1. Assess the effectiveness and performance of those stakeholders given delegated responsibility and authority for governance of enterprise IT.				
2. Periodically assess whether agreed-on governance of IT mechanisms (structures, principles, processes, etc.) are established and operating effectively.				
3. Assess the effectiveness of the governance design and identify actions to rectify any deviations found.				
4. Maintain oversight of the extent to which IT satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines.				
5. Provide oversight of the effectiveness of, and compliance with, the enterprise's system of control.				
6. Monitor regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines.				

EDM01 Related Guidance	
Related Standard	**Detailed Reference**
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	
ISO/IEC 38500	
King III	• 5.1. The board should be responsible for information technology (IT) governance. • 5.3. The board should delegate to management the responsibility for the implementation of an IT governance framework.
Organisation for Economic Co-operation and Development (OECD)	Corporate Governance Principles

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

EDM02 Ensure Benefits Delivery	Area: Governance Domain: Evaluate, Direct and Monitor
Process Description Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs.	
Process Purpose Statement Secure optimal value from IT-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
05 Realised benefits from IT-enabled investments and services portfolio	• Percent of IT-enabled investments where benefit realisation is monitored through the full economic life cycle • Percent of IT services where expected benefits are realised • Percent of IT-enabled investments where claimed benefits are met or exceeded
06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
17 Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of IT innovation possibilities • Level of stakeholder satisfaction with levels of IT innovation expertise and ideas • Number of approved initiatives resulting from innovative IT ideas
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. The enterprise is securing optimal value from its portfolio of approved IT-enabled initiatives, services and assets.	• Level of executive management satisfaction with IT's value delivery and cost • Deviation between target and actual investment mix • Level of stakeholder satisfaction with the enterprise's ability to obtain value from IT-enabled initiatives
2. Optimal value is derived from IT investment through effective value management practices in the enterprise.	• Number of incidents that occur due to actual or attempted circumvention of established value management principles and practices • Percent of IT initiatives in the overall portfolio where value is being managed through the full life cycle
3. Individual IT-enabled investments contribute optimal value.	• Level of stakeholder satisfaction with progress towards identified goals, with value delivery based on surveys • Percent of expected value realised

Personal Copy of: Dr. David Lanter

EDM02 RACI Chart

Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM02.01 Evaluate value optimisation.	A	R	R	C	R		R			C	C		C	C	C	C	C	R	C	C	C					
EDM02.02 Direct value optimisation.	A	R	R	C	R	I	R	I	I	I	I	I	I	I	I	I	I	R	C	I	I	I	I	I	I	I
EDM02.03 Monitor value optimisation.	A	R	R	C	R		R			R	C	C	C	C	C	C	C	R	C	C	C					

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

EDM02 Process Practices, Inputs/Outputs and Activities

Governance Practice	Inputs		Outputs	
	From	Description	Description	To
EDM02.01 Evaluate value optimisation. Continually evaluate the portfolio of IT-enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgement on any changes in direction that need to be given to management to optimise value creation.	APO02.05	Strategic road map	Evaluation of strategic alignment	APO02.04 APO05.03
	APO05.02	Investment return expectations	Evaluation of investment and services portfolios	APO05.03 APO05.04 APO06.02
	APO05.03	Selected programmes with return on investment (ROI) milestones		
	APO05.06	Benefit results and related communication		
	BAI01.06	Stage-gate review results		

Activities

1. Understand stakeholder requirements; strategic IT issues, such as dependence on IT; and technology insights and capabilities regarding the actual and potential significance of IT for the enterprise's strategy.
2. Understand the key elements of governance required for the reliable, secure and cost-effective delivery of optimal value from the use of existing and new IT services, assets and resources.
3. Understand and regularly discuss the opportunities that could arise from enterprise change enabled by current, new or emerging technologies, and optimise the value created from those opportunities.
4. Understand what constitutes value for the enterprise, and consider how well it is communicated, understood and applied throughout the enterprise's processes.
5. Evaluate how effectively the enterprise and IT strategies have been integrated and aligned within the enterprise and with enterprise goals for delivering value.
6. Understand and consider how effective current roles, responsibilities, accountabilities and decision-making bodies are in ensuring value creation from IT-enabled investments, services and assets.
7. Consider how well the management of IT-enabled investments, services and assets aligns with enterprise value management and financial management practices.
8. Evaluate the portfolio of investments, services and assets for alignment with the enterprise's strategic objectives; enterprise worth, both financial and non-financial; risk, both delivery risk and benefits risk; business process alignment; effectiveness in terms of usability, availability and responsiveness; and efficiency in terms of cost, redundancy and technical health.

Personal Copy of: Dr. David Lanter

EDM02 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Governance Practice	**Inputs**		**Outputs**	
EDM02.02 Direct value optimisation. Direct value management principles and practices to enable optimal value realisation from IT-enabled investments throughout their full economic life cycle.	**From**	**Description**	**Description**	**To**
			Investment types and criteria	APO05.01 APO05.03
			Requirements for stage-gate reviews	BAI01.01
Activities				
1. Define and communicate portfolio and investment types, categories, criteria and relative weightings to the criteria to allow for overall relative value scores.				
2. Define requirements for stage-gates and other reviews for significance of the investment to the enterprise and associated risk, programme schedules, funding plans, and the delivery of key capabilities and benefits and ongoing contribution to value.				
3. Direct management to consider potential innovative uses of IT that enable the enterprise to respond to new opportunities or challenges, undertake new business, increase competitiveness, or improve processes.				
4. Direct any required changes in assignment of accountabilities and responsibilities for executing the investment portfolio and delivering value from business processes and services.				
5. Define and communicate enterprise-level value delivery goals and outcome measures to enable effective monitoring.				
6. Direct any required changes to the portfolio of investments and services to realign with current and expected enterprise objectives and/or constraints.				
7. Recommend consideration of potential innovations, organisational changes or operational improvements that could drive increased value for the enterprise from IT-enabled initiatives.				
Governance Practice	**Inputs**		**Outputs**	
EDM02.03 Monitor value optimisation. Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions.	**From**	**Description**	**Description**	**To**
	APO05.04	Investment portfolio performance reports	Feedback on portfolio and programme performance	APO05.04 APO06.05 BAI01.06
			Actions to improve value delivery	EDM05.01 APO05.04 APO06.02 BAI01.01
Activities				
1. Define a balanced set of performance objectives, metrics, targets and benchmarks. Metrics should cover activity and outcome measures, including lead and lag indicators for outcomes, as well as an appropriate balance of financial and non-financial measures. Review and agree on them with the IT and other business functions, and other relevant stakeholders.				
2. Collect relevant, timely, complete, credible and accurate data to report on progress in delivering value against targets. Obtain a succinct, high-level, all-around view of portfolio, programme and IT (technical and operational capabilities) performance that supports decision making, and ensure that expected results are being achieved.				
3. Obtain regular and relevant portfolio, programme and IT (technological and functional) performance reports. Review the enterprise's progress towards identified goals and the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risk mitigated.				
4. Upon review of reports, take appropriate management action as required to ensure that value is optimised.				
5. Upon review of reports, ensure that appropriate management corrective action is initiated and controlled.				

EDM02 Related Guidance	
Related Standard	**Detailed Reference**
COSO	
ISO/IEC 38500	
King III	• 5.2. IT should be aligned with the performance and sustainability objectives of the company. • 5.4. The board should monitor and evaluate significant IT investments and expenditure.

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

EDM03 Ensure Risk Optimisation	Area: Governance Domain: Evaluate, Direct and Monitor
Process Description Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.	
Process Purpose Statement Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update or risk profile
06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines
15 IT compliance with internal policies	• Number of incidents related to non-compliance to policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices • Frequency of policies review and update
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Risk thresholds are defined and communicated and key IT-related risk is known.	• Level of alignment between IT risk and enterprise risk • Number of potential IT risks identified and managed • Refreshment rate of risk factor evaluation
2. The enterprise is managing critical IT-related enterprise risk effectively and efficiently.	• Percent of enterprise projects that consider IT risk • Percent of IT risk action plans executed on time • Percent of critical risk that has been effectively mitigated
3. IT-related enterprise risk does not exceed risk appetite and the impact of IT risk to enterprise value is identified and managed.	• Level of unexpected enterprise impact • Percent of IT risk that exceeds enterprise risk tolerance

EDM03 RACI Chart

Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM03.01 Evaluate risk management.	A	R	C	C	R	C	R			I	R	C		I	C	C	C	R	C							C
EDM03.02 Direct risk management.	A	R	C	C	R	C	R	I	I	I	R	I	I	I	C	C	C	R	C	I	I	I	I	I	I	I
EDM03.03 Monitor risk management.	A	R	C	C	R	C	R	I	I	I	R	R	I	I	C	C	C	R	C	I	I	I	I	I	I	C

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

EDM03 Process Practices, Inputs/Outputs and Activities				
Governance Practice	**Inputs**		**Outputs**	
EDM03.01 Evaluate risk management. Continually examine and make judgement on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risk to enterprise value related to the use of IT is identified and managed.	**From**	**Description**	**Description**	**To**
	APO12.01	Emerging risk issues and factors	Risk appetite guidance	APO12.03
			Approved risk tolerance levels	APO12.03
	Outside COBIT	Enterprise risk management principles	Evaluation of risk management activities	APO12.01
Activities				
1. Determine the level of IT-related risk that the enterprise is willing to take to meet its objectives (risk appetite).				
2. Evaluate and approve proposed IT risk tolerance thresholds against the enterprise's acceptable risk and opportunity levels.				
3. Determine the extent of alignment of the IT risk strategy to enterprise risk strategy.				
4. Proactively evaluate IT risk factors in advance of pending strategic enterprise decisions and ensure that risk-aware enterprise decisions are made.				
5. Determine that IT use is subject to appropriate risk assessment and evaluation, as described in relevant international and national standards.				
6. Evaluate risk management activities to ensure alignment with the enterprise's capacity for IT-related loss and leadership's tolerance of it.				
Governance Practice	**Inputs**		**Outputs**	
EDM03.02 Direct risk management. Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite.	**From**	**Description**	**Description**	**To**
	APO12.03	Aggregated risk profile, including status of risk management actions	Risk management policies	APO12.01
			Key objectives to be monitored for risk management	APO12.01
	Outside COBIT	Enterprise risk management (ERM) profiles and mitigation plans	Approved process for measuring risk management	APO12.01
Activities				
1. Promote an IT risk-aware culture and empower the enterprise to proactively identify IT risk, opportunity and potential business impacts.				
2. Direct the integration of the IT risk strategy and operations with the enterprise strategic risk decisions and operations.				
3. Direct the development of risk communication plans (covering all levels of the enterprise) as well as risk action plans.				
4. Direct implementation of the appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed-on principles of escalation (what to report, when, where and how).				
5. Direct that risk, opportunities, issues and concerns may be identified and reported by anyone at any time. Risk should be managed in accordance with published policies and procedures and escalated to the relevant decision makers.				
6. Identify key goals and metrics of risk governance and management processes to be monitored, and approve the approaches, methods, techniques and processes for capturing and reporting the measurement information.				

Personal Copy of: Dr. David Lanter

EDM03 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Governance Practice	**Inputs**		**Outputs**	
EDM03.03 Monitor risk management. Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported for remediation.	**From**	**Description**	**Description**	**To**
	AP012.02	Risk analysis results	Remedial actions to address risk management deviations	AP012.06
	AP012.04	• Opportunities for acceptance of greater risk • Results of third-party risk assessments • Risk analysis and risk profile reports for stakeholders	Risk management issues for the board	EDM05.01
Activities				
1. Monitor the extent to which the risk profile is managed within the risk appetite thresholds.				
2. Monitor key goals and metrics of risk governance and management processes against targets, analyse the cause of any deviations, and initiate remedial actions to address the underlying causes.				
3. Enable key stakeholders' review of the enterprise's progress towards identified goals.				
4. Report any risk management issues to the board or executive committee.				

EDM03 Related Guidance	
Related Standard	**Detailed Reference**
COSO/ERM	
ISO/IEC 31000	Framework for Risk Management
ISO/IEC 38500	
King III	• 5.5. IT should form an integral part of the company's risk management. • 5.7. A risk committee and audit committee should assist the board in carrying out its IT responsibilities.

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

EDM04 Ensure Resource Optimisation	Area: Governance Domain: Evaluate, Direct and Monitor
Process Description Ensure that adequate and sufficient IT-related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost.	
Process Purpose Statement Ensure that the resource needs of the enterprise are met in the optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realisation and readiness for future change.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
09 IT agility	• Level of satisfaction of business executives with IT's responsiveness to new requirements • Number of critical business processes supported by up-to-date infrastructure and applications • Average time to turn strategic IT objectives into an agreed-on and approved initiative
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
16 Competent and motivated business and IT personnel	• Percent of staff whose IT-related skills are sufficient for the competency required for their role • Percent of staff satisfied with their IT-related roles • Number of learning/training hours per staff member
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. The resource needs of the enterprise are met with optimal capabilities.	• Level of stakeholder feedback on resource optimisation • Number of benefits (e.g., cost savings) achieved through optimal utilisation of resources • Number of deviations from the resource plan and enterprise architecture strategies
2. Resources are allocated to best meet enterprise priorities within budget constraints.	• Number of deviations from, and exceptions to, resource management principles • Percent of projects with appropriate resource allocations
3. Optimal use of resources is achieved throughout their full economic life cycles.	• Percent of re-use of architecture components • Percent of projects and programmes with a medium- or high-risk status due to resource management issues • Number of resource management performance targets realised

EDM04 RACI Chart

Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM04.01 Evaluate resource management.	A	R	C	C	R		R			I	C	C	C	C	C	C	C	R	C	C	C					
EDM04.02 Direct resource management.	A	R	C	C	R	I	R	I	I	I	I	I	I	I	I	I	I	R	C	I	I	I	I	I	I	I
EDM04.03 Monitor resource management.	A	R	C	C	R	I	R	I	I	I	C	C	C	C	C	C	C	R	C	C	C	I	I	I	I	I

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

EDM04 Process Practices, Inputs/Outputs and Activities				
Governance Practice	**Inputs**		**Outputs**	
EDM04.01 Evaluate resource management. Continually examine and make judgement on the current and future need for IT-related resources, options for resourcing (including sourcing strategies), and allocation and management principles to meet the needs of the enterprise in the optimal manner.	**From**	**Description**	**Description**	**To**
	AP002.04	Gaps and changes required to realise target capability	Guiding principles for allocation of resources and capabilities	AP002.01 AP007.01 BAI03.11
	AP007.03	Skill development plans	Guiding principles for enterprise architecture	AP003.01
	AP010.02	Decision results of supplier evaluations	Approved resources plan	AP002.05 AP007.01 AP009.02
Activities				
1. Examine and make judgement on the current and future strategy, options for providing IT resources, and developing capabilities to meet current needs and future needs (including sourcing options).				
2. Define the principles for guiding the allocation and management of resources and capabilities so that IT can meet the needs of the enterprise, with the required capability and capacity according to the agreed-on priorities and budgetary constraints.				
3. Review and approve the resource plan and enterprise architecture strategies for delivering value and mitigating risk with the allocated resources.				
4. Understand requirements for aligning resource management with enterprise financial and human resources (HR) planning.				
5. Define principles for the management and control of the enterprise architecture.				
Governance Practice	**Inputs**		**Outputs**	
EDM04.02 Direct resource management. Ensure the adoption of resource management principles to enable optimal use of IT resources throughout their full economic life cycle.	**From**	**Description**	**Description**	**To**
			Communication of resourcing strategies	AP002.06 AP007.05 AP009.02
			Assigned responsibilities for resource management	AP001.02 DSS06.03
			Principles for safeguarding resources	AP001.04
Activities				
1. Communicate and drive the adoption of the resource management strategies, principles, and agreed-on resource plan and enterprise architecture strategies.				
2. Assign responsibilities for executing resource management.				
3. Define key goals, measures and metrics for resource management.				
4. Establish principles related to safeguarding resources.				
5. Align resource management with enterprise financial and HR planning.				
Governance Practice	**Inputs**		**Outputs**	
EDM04.03 Monitor resource management. Monitor the key goals and metrics of the resource management processes and establish how deviations or problems will be identified, tracked and reported for remediation.	**From**	**Description**	**Description**	**To**
			Feedback on allocation and effectiveness of resources and capabilities	EDM05.01 AP002.05 AP007.05 AP009.05
			Remedial actions to address resource management deviations	AP002.05 AP007.01 AP007.03 AP009.04
Activities				
1. Monitor the allocation and optimisation of resources in accordance with enterprise objectives and priorities using agreed-on goals and metrics.				
2. Monitor IT sourcing strategies, enterprise architecture strategies, IT resources and capabilities to ensure that current and future needs of the enterprise can be met.				
3. Monitor resource performance against targets, analyse the cause of deviations, and initiate remedial action to address the underlying causes.				

Personal Copy of: Dr. David Lanter

EDM04 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 38500	
King III	5.6. The board should ensure that information assets are managed effectively.
The Open Group Architecture Forum (TOGAF) 9	The TOGAF components of an Architecture Board, Architecture Governance and Architecture Maturity Models map to resource optimisation.

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

EDM05 Ensure Stakeholder Transparency	Area: Governance Domain: Evaluate, Direct and Monitor
Process Description Ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions.	
Process Purpose Statement Make sure that the communication to stakeholders is effective and timely and the basis for reporting is established to increase performance, identify areas for improvement, and confirm that IT-related objectives and strategies are in line with the enterprise's strategy.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
03 Commitment of executive management for making IT-related decisions	• Percent of executive management roles with clearly defined accountabilities for IT decisions • Number of times IT is on the board agenda in a proactive manner • Frequency of IT strategy (executive) committee meetings • Rate of execution of executive IT-related decisions
06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Stakeholder reporting is in line with stakeholder requirements.	• Date of last revision to reporting requirements • Percent of stakeholders covered in reporting requirements
2. Reporting is complete, timely and accurate.	• Percent of reports that are not delivered on time • Percent of reports containing inaccuracies
3. Communication is effective and stakeholders are satisfied.	• Level of stakeholder satisfaction with reporting • Number of breaches of mandatory reporting requirements

EDM05 RACI Chart

Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM05.01 Evaluate stakeholder reporting requirements.	A	R	C	C	C	I										C	C	R	I			I				
EDM05.02 Direct stakeholder communication and reporting.	A	R	C	C	C	I										C	C	R	I			I				
EDM05.03 Monitor stakeholder communication.	A	R	C	C	C	I										C	C	R	I			I				

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

EDM05 Process Practices, Inputs/Outputs and Activities				
Governance Practice	**Inputs**		**Outputs**	
EDM05.01 Evaluate stakeholder reporting requirements. Continually examine and make judgement on the current and future requirements for stakeholder communication and reporting, including both mandatory reporting requirements (e.g., regulatory) and communication to other stakeholders. Establish the principles for communication.	**From**	**Description**	**Description**	**To**
	EDM02.03	Actions to improve value delivery	Evaluation of enterprise reporting requirements	MEA01.01
	EDM03.03	Risk management issues for the board	Reporting and communication principles	MEA01.01
	EDM04.03	Feedback on allocation and effectiveness of resources and capabilities		
	MEA02.08	Refined scope		
Activities				
1. Examine and make a judgement on the current and future mandatory reporting requirements relating to the use of IT within the enterprise (regulation, legislation, common law, contractual), including extent and frequency.				
2. Examine and make a judgement on the current and future reporting requirements for other stakeholders relating to the use of IT within the enterprise, including extent and conditions.				
3. Maintain principles for communication with external and internal stakeholders, including communication formats and communication channels, and for stakeholder acceptance and sign-off of reporting.				
Governance Practice	**Inputs**		**Outputs**	
EDM05.02 Direct stakeholder communication and reporting. Ensure the establishment of effective stakeholder communication and reporting, including mechanisms for ensuring the quality and completeness of information, oversight of mandatory reporting, and creating a communication strategy for stakeholders.	**From**	**Description**	**Description**	**To**
	APO12.04	Risk analysis and risk profile reports for stakeholders	Rules for validating and approving mandatory reports	MEA01.01 MEA03.04
			Escalation guidelines	MEA01.05
Activities				
1. Direct the establishment of the communication strategy for external and internal stakeholders.				
2. Direct the implementation of mechanisms to ensure that information meets all criteria for mandatory IT reporting requirements for the enterprise.				
3. Establish mechanisms for validation and approval of mandatory reporting.				
4. Establish reporting escalation mechanisms.				
Governance Practice	**Inputs**		**Outputs**	
EDM05.03 Monitor stakeholder communication. Monitor the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders are met.	**From**	**Description**	**Description**	**To**
	MEA02.08	• Assurance review report • Assurance review results	Assessment of reporting effectiveness	MEA01.01 MEA03.04
Activities				
1. Periodically assess the effectiveness of the mechanisms for ensuring the accuracy and reliability of mandatory reporting.				
2. Periodically assess the effectiveness of the mechanisms for, and outcomes from, communication with external and internal stakeholders.				
3. Determine whether the requirements of different stakeholders are met.				

EDM05 Related Guidance	
Related Standard	**Detailed Reference**
COSO	
ISO/IEC 38500	
King III	

Personal Copy of: Dr. David Lanter

Align, Plan and Organise (APO)

01 Manage the IT management framework.

02 Manage strategy.

03 Manage enterprise architecture.

04 Manage innovation.

05 Manage portfolio.

06 Manage budget and costs.

07 Manage human resources.

08 Manage relationships.

09 Manage service agreements.

10 Manage suppliers.

11 Manage quality.

12 Manage risk.

13 Manage security.

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

APO01 Manage the IT Management Framework	Area: Management Domain: Align, Plan and Organise
Process Description Clarify and maintain the governance of enterprise IT mission and vision. Implement and maintain mechanisms and authorities to manage information and the use of IT in the enterprise in support of governance objectives in line with guiding principles and policies.	
Process Purpose Statement Provide a consistent management approach to enable the enterprise governance requirements to be met, covering management processes, organisational structures, roles and responsibilities, reliable and repeatable activities, and skills and competencies.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
09 IT agility	• Level of satisfaction of business executives with IT's responsiveness to new requirements • Number of critical business processes supported by up-to-date infrastructure and applications • Average time to turn strategic IT objectives into an agreed-on and approved initiative
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
15 IT compliance with internal policies	• Number of incidents related to non-compliance to policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices • Frequency of policies review and update
16 Competent and motivated business and IT personnel	• Percent of staff whose IT-related skills are sufficient for the competency required for their role • Percent of staff satisfied with their IT-related roles • Number of learning/training hours per staff member
17 Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of IT innovation possibilities • Level of stakeholder satisfaction with levels of IT innovation expertise and ideas • Number of approved initiatives resulting from innovative IT ideas
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. An effective set of policies is defined and maintained.	• Percent of active policies, standards and other enablers documented and up to date • Date of last updates to the framework and enablers • Number of risk exposures due to inadequacies in the design of the control environment
2. Everyone is aware of the policies and how they should be implemented.	• Number of staff who attended training or awareness sessions • Percent of third-party suppliers who have contracts defining control requirements

Personal Copy of: Dr. David Lanter

AP001 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP001.01 Define the organisational structure.		C	C	C	C		I		C						R	I	I	A	C	C	C	R	C	C	C	
AP001.02 Establish roles and responsibilities.					I	C			C						C	C	C	A	C	C	C	R	C	C	C	C
AP001.03 Maintain the enablers of the management system.	C	A	C	R	C	C	I				C	C	C	C		C	C	R				R				
AP001.04 Communicate management objectives and direction.		A	R	R	R	I	R	I	I	I	R	R	I	I	I	I	I	R	I	I	I	I	I	I	I	I
AP001.05 Optimise the placement of the IT function.		C	C	C	C		A		C						C	C	C	R	C	C	C	R	C	C	C	
AP001.06 Define information (data) and system ownership.		I	I	C	A	R									C	C	C	C	C						C	C
AP001.07 Manage continual improvement of processes.				A		R			R				C		I	C	C	R	R	R	R	R	R	R	R	
AP001.08 Maintain compliance with policies and procedures.		A				R			R				R		R	C	I	R	R	R	R	R	R	R	R	

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

AP001 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
	From	Description	Description	To
AP001.01 Define the organisational structure. Establish an internal and extended organisational structure that reflects business needs and IT priorities. Put in place the required management structures (e.g., committees) that enable management decision making to take place in the most effective and efficient manner.	EDM01.01	• Decision-making model • Enterprise governance guiding principles	Definition of organisational structure and functions	AP003.02
	AP003.02	Process architecture model	Enterprise operational guidelines	AP003.02
			Communication ground rules	All APO All BAI All DSS All MEA

Personal Copy of: Dr. David Lanter

AP001 Process Practices, Inputs/Outputs and Activities *(cont.)*

AP001.01 Activities

1. Define the scope, internal and external functions, internal and external roles, and capabilities and decision rights required, including those IT activities performed by third parties.
2. Identify decisions required for the achievement of enterprise outcomes and the IT strategy, and for the management and execution of IT services.
3. Establish the involvement of stakeholders who are critical to decision making (accountable, responsible, consulted or informed).
4. Align the IT-related organisation with enterprise architecture organisational models.
5. Define the focus, roles and responsibilities of each function within the IT-related organisational structure.
6. Define the management structures and relationships to support the functions and roles of management and execution, in alignment with the governance direction set.
7. Establish an IT strategy committee (or equivalent) at the board level. This committee should ensure that governance of IT, as part of enterprise governance, is adequately addressed; advise on strategic direction; and review major investments on behalf of the full board.
8. Establish an IT steering committee (or equivalent) composed of executive, business and IT management to determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities; track status of projects and resolve resource conflicts; and monitor service levels and service improvements.
9. Provide guidelines for each management structure (including mandate, objectives, meeting attendees, timing, tracking, supervision and oversight) as well as required inputs for and expected outcomes of meetings.
10. Define ground rules for communication by identifying communication needs, and implementing plans based on those needs, considering top-down, bottom-up and horizontal communication.
11. Establish and maintain an optimal co-ordination, communication and liaison structure between the business and IT functions within the enterprise and with entities outside the enterprise.
12. Regularly verify the adequacy and effectiveness of the organisational structure.

Management Practice	Inputs		Outputs	
	From	Description	Description	To
AP001.02 Establish roles and responsibilities. Establish, agree on and communicate roles and responsibilities of IT personnel, as well as other stakeholders with responsibilities for enterprise IT, that clearly reflect overall business needs and IT objectives and relevant personnel's authority, responsibilities and accountability.	EDM01.01	Authority levels	Definition of IT-related roles and responsibilities	DSS05.04
	EDM04.02	Assigned responsibilities for resource management	Definition of supervisory practices	AP007.01
	AP007.03	• Skill development plans • Skills and competencies matrix		
	AP011.01	Quality management system (QMS) roles, responsibilities and decision rights		
	AP013.01	Information security management system (ISMS) scope statement		
	DSS06.03	• Allocated levels of authority • Allocated roles and responsibilities		

Activities

1. Establish, agree on and communicate IT-related roles and responsibilities for all personnel in the enterprise, in alignment with business needs and objectives. Clearly delineate responsibilities and accountabilities, especially for decision making and approvals.
2. Consider requirements from enterprise and IT service continuity when defining roles, including staff back-up and cross-training requirements.
3. Provide input to the IT service continuity process by maintaining up-to-date contact information and role descriptions in the enterprise.
4. Include in role and responsibility descriptions adherence to management policies and procedures, the code of ethics, and professional practices.
5. Implement adequate supervisory practices to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review performance. The level of supervision should be in line with the sensitivity of the position and extent of responsibilities assigned.
6. Ensure that accountability is defined through roles and responsibilities.
7. Structure roles and responsibilities to reduce the possibility for a single role to compromise a critical process.

Personal Copy of: Dr. David Lanter

AP001 Process Practices, Inputs/Outputs and Activities *(cont.)*

Management Practice	Inputs		Outputs	
	From	Description	Description	To
AP001.03 Maintain the enablers of the management system. Maintain the enablers of the management system and control environment for enterprise IT, and ensure that they are integrated and aligned with the enterprise's governance and management philosophy and operating style. These enablers include the clear communication of expectations/requirements. The management system should encourage cross-divisional co-operation and teamwork, promote compliance and continuous improvement, and handle process deviations (including failure).	EDM01.01	Enterprise governance guiding principles	IT-related policies	All APO All BAI All DSS All MEA
	AP002.05	Strategic road map		
	AP012.01	Emerging risk issues and factors		
	AP012.02	Risk analysis results		

Activities
1. Obtain an understanding of the enterprise vision, direction and strategy.
2. Consider the enterprise's internal environment, including management culture and philosophy, risk tolerance, security, ethical values, code of conduct, accountability, and requirements for management integrity.
3. Derive and integrate IT principles with business principles.
4. Align the IT control environment with the overall IT policy environment, IT governance and IT process frameworks, and existing enterprise-level risk and control frameworks. Assess industry-specific good practices or requirements (e.g., industry-specific regulations) and integrate them where appropriate.
5. Align with any applicable national and international governance and management standards and codes of practice, and evaluate available good practices such as COSO's *Internal Control—Integrated Framework* and COSO's *Enterprise Risk Management—Integrated Framework*.
6. Create a set of policies to drive the IT control expectations on relevant key topics such as quality, security, confidentiality, internal controls, usage of IT assets, ethics and intellectual property rights.
7. Evaluate and update the policies at least yearly to accommodate changing operating or business environments.
8. Roll out and enforce IT policies to all relevant staff, so they are built into, and are an integral part of, enterprise operations.
9. Ensure that procedures are in place to track compliance with policies and define the consequences of non-compliance.

Management Practice	Inputs		Outputs	
	From	Description	Description	To
AP001.04 Communicate management objectives and direction. Communicate awareness and understanding of IT objectives and direction to appropriate stakeholders and users throughout the enterprise.	EDM01.02	Enterprise governance communication	Communication on IT objectives	All APO All BAI All DSS All MEA
	EDM04.02	Principles for safeguarding resources		
	AP012.06	Risk impact communication		
	BAI08.01	Communication on value of knowledge		
	DSS04.01	Policy and objectives for business continuity		
	DSS05.01	Malicious software prevention policy		
	DSS05.02	Connectivity security policy		
	DSS05.03	Security policies for endpoint devices		

Activities
1. Continuously communicate IT objectives and direction. Ensure that communications are supported by executive management in action and words, using all available channels.
2. Ensure that the information communicated encompasses a clearly articulated mission, service objectives, security, internal controls, quality, code of ethics/conduct, policies and procedures, roles and responsibilities, etc. Communicate the information at the appropriate level of detail for the respective audiences within the enterprise.
3. Provide sufficient and skilled resources to support the communication process.

Personal Copy of: Dr. David Lanter

APO01 Process Practices, Inputs/Outputs and Activities *(cont.)*

Management Practice	Inputs		Outputs	
APO01.05 Optimise the placement of the IT function. Position the IT capability in the overall organisational structure to reflect an enterprise model relevant to the importance of IT within the enterprise, specifically its criticality to enterprise strategy and the level of operational dependence on IT. The reporting line of the CIO should be commensurate with the importance of IT within the enterprise.	**From**	**Description**	**Description**	**To**
	Outside COBIT	• Enterprise operating model • Enterprise strategy	Evaluation of options for IT organisation	APO03.02
			Defined operational placement of IT function	APO03.02
Activities				
1. Understand the context for the placement of the IT function, including an assessment of the enterprise strategy and operating model (centralised, federated, decentralised, hybrid), importance of IT, and sourcing situation and options.				
2. Identify, evaluate and prioritise options for organisational placement, sourcing and operating models.				
3. Define placement of the IT function and obtain agreement.				

Management Practice	Inputs		Outputs	
APO01.06 Define information (data) and system ownership. Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that owners make decisions about classifying information and systems and protecting them in line with this classification.	**From**	**Description**	**Description**	**To**
			Data classification guidelines	APO03.02 BAI02.01 DSS05.02 DSS06.01
			Data security and control guidelines	BAI02.01
			Data integrity procedures	BAI02.01 DSS06.01
Activities				
1. Provide policies and guidelines to ensure appropriate and consistent enterprisewide classification of information (data).				
2. Define, maintain and provide appropriate tools, techniques and guidelines to provide effective security and controls over information and information systems in collaboration with the owner.				
3. Create and maintain an inventory of information (systems and data) that includes a listing of owners, custodians and classifications. Include systems that are outsourced and those for which ownership should stay within the enterprise.				
4. Define and implement procedures to ensure the integrity and consistency of all information stored in electronic form such as databases, data warehouses and data archives.				

Management Practice	Inputs		Outputs	
APO01.07 Manage continual improvement of processes. Assess, plan and execute the continual improvement of processes and their maturity to ensure that they are capable of delivering against enterprise, governance, management and control objectives. Consider COBIT process implementation guidance, emerging standards, compliance requirements, automation opportunities, and the feedback of process users, the process team and other stakeholders. Update the process and consider impacts on process enablers.	**From**	**Description**	**Description**	**To**
	EDM01.03	Feedback on governance effectiveness and performance	Process capability assessments	MEA01.03
	MEA03.02	Updated policies, principles, procedures and standards	Process improvement opportunities	All APO All BAI All DSS All MEA
			Performance goals and metrics for process improvement tracking	MEA01.02
Activities				
1. Identify business-critical processes based on performance and conformance drivers and related risk. Assess process capability and identify improvement targets. Analyse gaps in process capability and control. Identify options for improvement and redesign of the process. Prioritise initiatives for process improvement based on potential benefits and costs.				
2. Implement agreed-on improvements, operate as normal business practice, and set performance goals and metrics to enable monitoring of process improvements.				
3. Consider ways to improve efficiency and effectiveness (e.g., through training, documentation, standardisation and automation of the process).				
4. Apply quality management practices to update the process.				
5. Retire outdated processes, process components or enablers.				

Personal Copy of: Dr. David Lanter

AP001 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
AP001.08 Maintain compliance with policies and procedures. Put in place procedures to maintain compliance with and performance measurement of policies and other enablers of the control framework, and enforce the consequences of non-compliance or inadequate performance. Track trends and performance and consider these in the future design and improvement of the control framework.	**From**	**Description**	**Description**	**To**
	DSS01.04	Environmental policies	Non-compliance remedial actions	MEA01.05
	MEA03.02	Updated policies, principles, procedures and standards		
Activities				
1. Track compliance with policies and procedures.				
2. Analyse non-compliance and take appropriate action (this could include changing requirements).				
3. Integrate performance and compliance into individual staff members' performance objectives.				
4. Regularly assess the performance of the framework's enablers and take appropriate action.				
5. Analyse trends in performance and compliance and take appropriate action.				

AP001 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	• 3.1 Management responsibility • 4.4 Continual improvement
ISO/IEC 27002	6. Organisation of Information Security
ITIL V3 2011	Continual Service Improvement, 4.1 The 7-Step Improvement Process

Personal Copy of: Dr. David Lanter

APO02 Manage Strategy	Area: Management Domain: Align, Plan and Organise
Process Description Provide a holistic view of the current business and IT environment, the future direction, and the initiatives required to migrate to the desired future environment. Leverage enterprise architecture building blocks and components, including externally provided services and related capabilities to enable nimble, reliable and efficient response to strategic objectives.	
Process Purpose Statement Align strategic IT plans with business objectives. Clearly communicate the objectives and associated accountabilities so they are understood by all, with the IT strategic options identified, structured and integrated with the business plans.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
17 Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of IT innovation possibilities • Level of stakeholder satisfaction with levels of IT innovation expertise and ideas • Number of approved initiatives resulting from innovative IT ideas
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. All aspects of the IT strategy are aligned with the enterprise strategy.	• Percent of objectives in the IT strategy that support the enterprise strategy • Percent of enterprise objectives addressed in the IT strategy
2. The IT strategy is cost-effective, appropriate, realistic, achievable, enterprise-focussed and balanced.	• Percent of initiatives in the IT strategy that are self-funding (financial benefits in excess of costs) • Trends in ROI of initiatives included in the IT strategy • Level of enterprise stakeholder satisfaction survey feedback on the IT strategy
3. Clear and concrete short-term goals can be derived from, and traced back to, specific long-term initiatives, and can then be translated into operational plans.	• Percent of projects in the IT project portfolio that can be directly traced back to the IT strategy
4. IT is a value driver for the enterprise.	• Percent of strategic enterprise objectives obtained as a result of strategic IT initiatives • Number of new enterprise opportunities realised as a direct result of IT developments • Percent of IT initiatives/projects championed by business owners
5. There is awareness of the IT strategy and a clear assignment of accountability for delivery.	• Achievement of measurable IT strategy outcomes part of staff performance goals • Frequency of updates to the IT strategy communication plan • Percent of strategic initiatives with accountability assigned

Personal Copy of: Dr. David Lanter

AP002 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP002.01 Understand enterprise direction.		C	C	C	A	C	C				C	C		C				R	C	R	R		R	R	R	
AP002.02 Assess the current environment, capabilities and performance.		C	C	C	R	C	C				C					C	C	A	R	R	R	C	C	C	C	
AP002.03 Define the target IT capabilities.		A	C	C	C	I	R		I		C		C			C	C	R	C	C	C	C	C	C	C	
AP002.04 Conduct a gap analysis.					R	R	C				C				C	R	R	A	R	R	R	R	R	R	C	
AP002.05 Define the strategic plan and road map.		C	I	C	C		C		R		C	C				C	C	A	C	C	C	C	C	C	C	
AP002.06 Communicate the IT strategy and direction.	I	R	I	I	R	I	A	I	I	I	I	I	I	I	I	I	I	R	I	I	I	I	I	I	I	I

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

AP002 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
	From	Description	Description	To
AP002.01 Understand enterprise direction. Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).	EDM04.01	Guiding principles for allocation of resources and capabilities	Sources and priorities for changes	Internal
	AP004.02	Innovation opportunities linked to business drivers		
	Outside COBIT	Enterprise strategy and enterprise strengths, weaknesses, opportunities, threats (SWOT) analysis		

Activities
1. Develop and maintain an understanding of enterprise strategy and objectives, as well as the current enterprise operational environment and challenges.
2. Develop and maintain an understanding of the external environment of the enterprise.
3. Identify key stakeholders and obtain insight on their requirements.
4. Identify and analyse sources of change in the enterprise and external environments.
5. Ascertain priorities for strategic change.
6. Understand the current enterprise architecture and work with the enterprise architecture process to determine any potential architectural gaps.

Personal Copy of: Dr. David Lanter

APO02 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
APO02.02 Assess the current environment, capabilities and performance. Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.	APO06.05	Cost optimisation opportunities	Baseline of current capabilities	Internal
	APO08.05	Definition of potential improvement projects	Gaps and risk related to current capabilities	APO12.01
	APO09.01	Identified gaps in IT services to the business	Capability SWOT analysis	Internal
	APO09.04	Improvement action plans and remediations		
	APO12.01	Emerging risk issues and factors		
	APO12.02	Risk analysis results		
	APO12.03	Aggregated risk profile, including status of risk management actions		
	APO12.05	Project proposals for reducing risk		
	BAI04.03	• Performance and capacity plans • Prioritised improvements		
	BAI04.05	Corrective actions		
	BAI09.01	Results of fit-for-purpose reviews		
	BAI09.04	• Opportunities to reduce asset costs or increase value • Results of cost optimisation reviews		

Activities
1. Develop a baseline of the current business and IT environment, capabilities and services against which future requirements can be compared. Include the relevant high-level detail of the current enterprise architecture (business, information, data, applications and technology domains), business processes, IT processes and procedures, the IT organisation structure, external service provision, governance of IT, and enterprisewide IT related skills and competencies.
2. Identify risk from current, potential and declining technologies.
3. Identify gaps between current business and IT capabilities and services and reference standards and good practices, competitor business and IT capabilities, and comparative benchmarks of good practice and emerging IT service provision.
4. Identify issues, strengths, opportunities and threats in the current environment, capabilities and services to understand current performance. Identify areas for improvement in terms of IT's contribution to enterprise objectives.

Personal Copy of: Dr. David Lanter

APO02 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO02.03 Define the target IT capabilities. Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, good practices and validated emerging technologies or innovation proposals.	**From**	**Description**	**Description**	**To**
	APO04.05	• Analysis of rejected initiatives • Results and recommendations from proof-of-concept initiatives	High-level IT-related goals	Internal
			Required business and IT capabilities	Internal
			Proposed enterprise architecture changes	APO03.03
Activities				
1. Consider validated emerging technology or innovation ideas.				
2. Identify threats from declining, current and newly acquired technologies.				
3. Define high-level IT objectives/goals and how they will contribute to the enterprise's business objectives.				
4. Define required and desired business process and IT capabilities and IT services and describe the high-level changes in the enterprise architecture (business, information, data, applications and technology domains), business and IT processes and procedures, the IT organisation structure, IT service providers, governance of IT, and IT skills and competencies.				
5. Align and agree with the enterprise architect on proposed enterprise architecture changes.				
6. Demonstrate traceability to the enterprise strategy and requirements.				
Management Practice	**Inputs**		**Outputs**	
APO02.04 Conduct a gap analysis. Identify the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimise investment in and utilisation of the internal and external asset base. Consider the critical success factors to support strategy execution.	**From**	**Description**	**Description**	**To**
	EDM02.01	Evaluation of strategic alignment	Gaps and changes required to realise target capability	EDM04.01 APO13.02 BAI03.11
	APO04.06	Assessments of using innovative approaches	Value benefit statement for target environment	BAI03.11
	APO05.02	Investment return expectations		
	BAI01.05	Results of programme goal achievement monitoring		
	BAI01.06	Stage-gate review results		
	BAI01.13	Post-implementation review results		
Activities				
1. Identify all gaps and changes required to realise the target environment.				
2. Consider the high-level implications of all gaps. Consider the value of potential changes to business and IT capabilities, IT services and enterprise architecture, and the implications if no changes are realised.				
3. Assess the impact of potential changes on the business and IT operating models, IT research and development capabilities, and IT investment programmes.				
4. Refine the target environment definition and prepare a value statement with the benefits of the target environment.				

Personal Copy of: Dr. David Lanter

APO02 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO02.05 Define the strategic plan and road map. Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT-related goals will contribute to the enterprise's strategic goals. Include how IT will support IT-enabled investment programmes, business processes, IT services and IT assets. Direct IT to define the initiatives that will be required to close the gaps, the sourcing strategy and the measurements to be used to monitor achievement of goals, then prioritise the initiatives and combine them in a high-level road map.	**From**	**Description**	**Description**	**To**
	EDM04.01	Approved resources plan	Definition of strategic initiatives	APO05.01
	EDM04.03	• Feedback on allocation and effectiveness of resources and capabilities • Remedial actions to address resource management deviations	Risk assessment initiatives	APO05.01 APO12.01
	APO03.01	• Defined scope of architecture • Architecture concept business case and value proposition	Strategic road map	EDM02.01 APO01.03 APO03.01 APO05.01 APO08.01
	APO03.02	Information architecture model		
	APO03.03	• Transition architectures • High-level implementation and migration strategy		
	APO05.01	Feedback on strategy and goals		
	APO05.02	Funding options		
	APO06.02	Budget allocations		
	APO06.03	• IT budget and plan • Budget communications		
	APO13.02	Information security business cases		
	BAI09.05	Action plan to adjust licence numbers and allocations		
	DSS04.02	Approved strategic options		
Activities				
1. Define the initiatives required to close gaps and migrate from the current to the target environment, including investment/operational budget, funding sources, sourcing strategy and acquisition strategy.				
2. Identify and adequately address risk, costs and implications of organisational changes, technology evolution, regulatory requirements, business process re-engineering, staffing, insourcing and outsourcing opportunities, etc., in the planning process.				
3. Determine dependencies, overlaps, synergies and impacts amongst initiatives, and prioritise the initiatives.				
4. Identify resource requirements, schedule and investment/operational budgets for each of the initiatives.				
5. Create a road map indicating the relative scheduling and interdependencies of the initiatives.				
6. Translate the objectives into outcome measures represented by metrics (what) and targets (how much) that can be related to enterprise benefits.				
7. Formally obtain support from stakeholders and obtain approval for the plan.				

Personal Copy of: Dr. David Lanter

AP002 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
AP002.06 Communicate the IT strategy and direction. Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.	**From**	**Description**	**Description**	**To**
	EDM04.02	Communication of resourcing strategies	Communication plan	Internal
			Communication package	All APO All BAI All DSS All MEA
Activities				
1. Develop and maintain a network for endorsing, supporting and driving the IT strategy.				
2. Develop a communication plan covering the required messages, target audiences, communication mechanisms/channels and schedules.				
3. Prepare a communication package that delivers the plan effectively using available media and technologies.				
4. Obtain feedback and update the communication plan and delivery as required.				

AP002 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	• 4.0 Planning and implementing service management • 5.0 Planning and implementing new or changed services
ITIL V3 2011	Service Strategy, 4.1 Strategy Management for IT Services

Personal Copy of: Dr. David Lanter

APO03 Manage Enterprise Architecture	Area: Management Domain: Align, Plan and Organise
Process Description Establish a common architecture consisting of business process, information, data, application and technology architecture layers for effectively and efficiently realising enterprise and IT strategies by creating key models and practices that describe the baseline and target architectures. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as re-use of building block components.	
Process Purpose Statement Represent the different building blocks that make up the enterprise and their inter-relationships as well as the principles guiding their design and evolution over time, enabling a standard, responsive and efficient delivery of operational and strategic objectives.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
09 IT agility	• Level of satisfaction of business executives with IT's responsiveness to new requirements • Number of critical business processes supported by up-to-date infrastructure and applications • Average time to turn strategic IT objectives into an agreed-on and approved initiative
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. The architecture and standards are effective in supporting the enterprise.	• Number of exceptions to architecture standards and baselines applied for and granted • Level of architecture customer feedback • Project benefits realised that can be traced back to architecture involvement (e.g., cost reduction through re-use)
2. A portfolio of enterprise architecture services supports agile enterprise change.	• Percent of projects using enterprise architecture services • Level of architecture customer feedback
3. Appropriate and up-to-date domain and/or federated architectures exist that provide reliable architecture information.	• Date of last update to domain and/or federated architectures • Number of identified gaps in models across enterprise, information, data, application and technology architecture domains • Level of architecture customer feedback regarding quality of information provided
4. A common enterprise architecture framework and methodology as well as an integrated architecture repository are used to enable re-use efficiencies across the enterprise.	• Percent of projects that utilise the framework and methodology to re-use defined components • Number of people trained in the methodology and tool set • Number of exceptions to architecture standards and baselines applied for and granted

Personal Copy of: Dr. David Lanter

AP003 RACI Chart																										
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP003.01 Develop the enterprise architecture vision.		A	C	C	R	C	R					C	R	C	C	C	C	R	R	C	C	C		C		
AP003.02 Define reference architecture.		C	C	C	R	C	R					C	A	C	C	C	C	R	R	C	C	C		C		
AP003.03 Select opportunities and solutions.		A	C	C	R	C	R					C	R	C	C	C	C	R	R	C	C	C		C		
AP003.04 Define architecture implementation.		A	C	R	C	C	R					C	R	C	C	C	C	R	R	C	C	C		C		
AP003.05 Provide enterprise architecture services.		A	C	R	C	C	R					C	R	C	C	C	C	R	R	C	C	C		C		

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

AP003 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
AP003.01 Develop the enterprise architecture vision. The architecture vision provides a first-cut, high-level description of the baseline and target architectures, covering the business, information, data, application and technology domains. The architecture vision provides the sponsor with a key tool to sell the benefits of the proposed capability to stakeholders within the enterprise. The architecture vision describes how the new capability will meet enterprise goals and strategic objectives and address stakeholder concerns when implemented.	EDM04.01	Guiding principles for enterprise architecture	Defined scope of architecture	AP002.05
	AP002.05	Strategic road map	Architecture principles	BAI02.01 BAI03.01 BAI03.02
	Outside COBIT	Enterprise strategy	Architecture concept business case and value proposition	AP002.05 AP005.03

Personal Copy of: Dr. David Lanter

APO03 Process Practices, Inputs/Outputs and Activities *(cont.)*				
APO03.01 Activities				
1. Identify the key stakeholders and their concerns/objectives, and define the key enterprise requirements to be addressed as well as the architecture views to be developed to satisfy the various stakeholder requirements.				
2. Identify the enterprise goals and strategic drivers of the enterprise and define the constraints that must be dealt with, including enterprisewide constraints and project-specific constraints (time, schedule, resources, etc.).				
3. Align architecture objectives with strategic programme priorities.				
4. Understand the capabilities and desires of the business, then identify options to realise those capabilities.				
5. Assess the enterprise's readiness for change.				
6. Define what is inside and what is outside the scope of the baseline architecture and target architecture efforts, understanding that the baseline and target need not be described at the same level of detail.				
7. Confirm and elaborate architecture principles, including enterprise principles. Ensure that any existing definitions are current and clarify any areas of ambiguity.				
8. Understand the current enterprise strategic goals and objectives and work with the strategic planning process to ensure that IT-related enterprise architecture opportunities are leveraged in the development of the strategic plan.				
9. Based on stakeholder concerns, business capability requirements, scope, constraints and principles, create the architecture vision: a high-level view of the baseline and target architectures.				
10. Define the target architecture value propositions, goals and metrics.				
11. Identify the enterprise change risk associated with the architecture vision, assess the initial level of risk (e.g., critical, marginal or negligible) and develop a mitigation strategy for each significant risk.				
12. Develop an enterprise architecture concept business case, outline plans and statement of architecture work, and secure approval to initiate a project aligned and integrated with the enterprise strategy.				
Management Practice	**Inputs**		**Outputs**	
APO03.02 Define reference architecture. The reference architecture describes the current and target architectures for the business, information, data, application and technology domains.	**From**	**Description**	**Description**	**To**
	APO01.01	• Enterprise operational guidelines • Definition of organisational structure and functions	Baseline domain descriptions and architecture definition	APO13.02 BAI02.01 BAI03.01 BAI03.02
	APO01.05	• Defined operational placement of IT function • Evaluation of options for IT organisation	Process architecture model	APO01.01
	APO01.06	Data classification guidelines	Information architecture model	APO02.05 BAI02.01 BAI03.02 DSS05.03 DSS05.04 DSS05.06
	Outside COBIT	Enterprise strategy		

Personal Copy of: Dr. David Lanter

AP003 Process Practices, Inputs/Outputs and Activities *(cont.)*

AP003.02 Activities

1. Maintain an architecture repository containing standards, reusable components, modelling artefacts, relationships, dependencies and views to enable uniformity of architectural organisation and maintenance.
2. Select reference viewpoints from the architecture repository that will enable the architect to demonstrate how stakeholder concerns are being addressed in the architecture.
3. For each viewpoint, select the models needed to support the specific view required, using selected tools or methods and the appropriate level of decomposition.
4. Develop baseline architectural domain descriptions, using the scope and level of detail necessary to support the target architecture and, to the extent possible, identifying relevant architecture building blocks from the architecture repository.
5. Maintain a process architecture model as part of the baseline and target domain descriptions. Standardise the descriptions and documentation of processes. Define the roles and responsibilities of the process decision makers, process owner, process users, process team and any other process stakeholders who should be involved.
6. Maintain an information architecture model as part of the baseline and target domain descriptions, consistent with the enterprise's strategy to enable optimal use of information for decision making. Maintain an enterprise data dictionary that promotes a common understanding and a classification scheme that includes details about data ownership, definition of appropriate security levels, and data retention and destruction requirements.
7. Verify the architecture models for internal consistency and accuracy and perform a gap analysis between the baseline and target. Prioritise gaps and define new or modified components that must be developed for the target architecture. Resolve potential impacts such as incompatibilities, inconsistencies or conflicts within the envisioned architecture.
8. Conduct a formal stakeholder review by checking the proposed architecture against the original motivation for the architecture project and the statement of architecture work.
9. Finalise business, information, data, applications and technology domain architectures, and create an architecture definition document.

Management Practice	Inputs		Outputs	
	From	Description	Description	To
AP003.03 Select opportunities and solutions. Rationalise the gaps between baseline and target architectures, taking both business and technical perspectives, and logically group them into project work packages. Integrate the project with any related IT-enabled investment programmes to ensure that the architectural initiatives are aligned with and enable these initiatives as part of overall enterprise change. Make this a collaborative effort with key enterprise stakeholders from business and IT to assess the enterprise's transformation readiness, and identify opportunities, solutions and all implementation constraints.	AP002.03	Proposed enterprise architecture changes	High-level implementation and migration strategy	AP002.05
	Outside COBIT	• Enterprise strategies • Enterprise drivers	Transition architectures	AP002.05

Activities

1. Determine and confirm key enterprise change attributes, including the enterprise's culture and how this will impact enterprise architecture implementation, as well as the enterprise's transition capabilities.
2. Identify any enterprise drivers that would constrain the sequence of implementation, including a review of the enterprise and line of business strategic and business plans, and consideration of the current enterprise architecture maturity.
3. Review and consolidate the gap analysis results between the baseline and target architectures and assess their implications with respect to potential solutions/opportunities, interdependencies and alignment with current IT-enabled programmes.
4. Assess the requirements, gaps, solutions and factors to identify a minimal set of functional requirements whose integration into work packages would lead to a more efficient and effective implementation of the target architecture.
5. Reconcile the consolidated requirements with potential solutions.
6. Refine the initial dependencies, ensuring that any constraints on the implementation and migration plans are identified, and consolidate them into a dependency analysis report.
7. Confirm the enterprise's readiness for, and the risk associated with, enterprise transformation.
8. Formulate a high-level implementation and migration strategy that will guide the target architecture implementation and structure the transition architectures in alignment with enterprise strategic objectives and time scales.
9. Identify and group major work packages into a coherent set of programmes and projects, respecting the enterprise strategic implementation direction and approach.
10. Develop a series of transition architectures as necessary where the scope of change required to realise the target architecture requires an incremental approach.

Personal Copy of: Dr. David Lanter

APO03 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO03.04 Define architecture implementation. Create a viable implementation and migration plan in alignment with the programme and project portfolios. Ensure that the plan is closely co-ordinated to ensure that value is delivered and the required resources are available to complete the necessary work.	**From**	**Description**	**Description**	**To**
			Resource requirements	BAI01.02
			Implementation phase descriptions	BAI01.01 BAI01.02
			Architecture governance requirements	BAI01.01
Activities				
1. Establish what the implementation and migration plan should include as part of programme and project planning and ensure that it is aligned with the requirements of applicable decision makers.				
2. Confirm transition architecture increments and phases and update the architecture definition document.				
3. Define architecture implementation governance requirements.				
Management Practice	**Inputs**		**Outputs**	
APO03.05 Provide enterprise architecture services. The provision of enterprise architecture services within the enterprise includes guidance to and monitoring of implementation projects, formalising ways of working through architecture contracts, and measuring and communicating architecture's value-add and compliance monitoring.	**From**	**Description**	**Description**	**To**
			Solution development guidance	BAI02.01 BAI02.02 BAI03.02
Activities				
1. Confirm scope and priorities and provide guidance for solution development and deployment.				
2. Manage the portfolio of enterprise architecture services to ensure alignment with strategic objectives and solution development.				
3. Manage enterprise architecture requirements and support with architectural principles, models and building blocks.				
4. Identify and align enterprise architecture priorities to value drivers. Define and collect value metrics and measure and communicate enterprise architecture value.				
5. Establish a technology forum to provide architectural guidelines, advice on projects and guidance on the selection of technology. Measure compliance with these standards and guidelines, including compliance with external requirements and their business relevance.				

APO03 Related Guidance	
Related Standard	**Detailed Reference**
TOGAF 9	At the core of TOGAF is the Architecture Development Method (ADM), which maps to the COBIT 5 practices of developing an architecture vision (ADM Phase A), defining reference architectures (ADM Phases B,C,D), selecting opportunities and solutions (ADM Phase E), and defining architecture implementation (ADM Phases F, G). A number of TOGAF components map to the COBIT 5 practice of providing enterprise architecture services. These include ADM Requirements Management, Architecture Principles, Stakeholder Management, Business Transformation Readiness Assessment, Risk Management, Capability-Based Planning, Architecture Compliance and Architecture Contracts.

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

APO04 Manage Innovation	Area: Management Domain: Align, Plan and Organise
Process Description Maintain an awareness of information technology and related service trends, identify innovation opportunities, and plan how to benefit from innovation in relation to business needs. Analyse what opportunities for business innovation or improvement can be created by emerging technologies, services or IT-enabled business innovation, as well as through existing established technologies and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions.	
Process Purpose Statement Achieve competitive advantage, business innovation, and improved operational effectiveness and efficiency by exploiting information technology developments.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
05 Realised benefits from IT-enabled investments and services portfolio	• Percent of IT-enabled investments where benefit realisation is monitored through the full economic life cycle • Percent of IT services where expected benefits are realised • Percent of IT-enabled investments where claimed benefits are met or exceeded
08 Adequate use of applications, information and technology solutions	• Percent of business process owners satisfied with supporting IT products and services • Level of business user understanding of how technology solutions support their processes • Satisfaction level of business users with training and user manuals • NPV showing business satisfaction level of the quality and usefulness of the technology solutions
09 IT agility	• Level of satisfaction of business executives with IT's responsiveness to new requirements • Number of critical business processes supported by up-to-date infrastructure and applications • Average time to turn strategic IT objectives into an agreed-on and approved initiative
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
17 Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of IT innovation possibilities • Level of stakeholder satisfaction with levels of IT innovation expertise and ideas • Number of approved initiatives resulting from innovative IT ideas
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Enterprise value is created through the qualification and staging of the most appropriate advances and innovations in technology, IT methods and solutions.	• Increase in market share or competitiveness due to innovations • Enterprise stakeholder perceptions and feedback on IT innovation
2. Enterprise objectives are met with improved quality benefits and/or reduced cost as a result of the identification and implementation of innovative solutions.	• Percent of implemented initiatives that realise the envisioned benefits • Percent of implemented initiatives with a clear linkage to an enterprise objective
3. Innovation is promoted and enabled and forms part of the enterprise culture.	• Inclusion of innovation or emerging technology-related objectives in performance goals for relevant staff • Stakeholder feedback and surveys

Personal Copy of: Dr. David Lanter

AP004 RACI Chart																										
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP004.01 Create an environment conducive to innovation.		A			R	R	R								R			R	R	R	R		R	R		
AP004.02 Maintain an understanding of the enterprise environment.				A	R	R	C											R	R	R	R					
AP004.03 Monitor and scan the technology environment.																		A	R	R	R		R	R		
AP004.04 Assess the potential of emerging technologies and innovation ideas.		I		I	C	C	C				C							A	R	R	R		R	R		
AP004.05 Recommend appropriate further initiatives.				I	R	R	A						C					R	R	R	R		R	R		
AP004.06 Monitor the implementation and use of innovation.					C	C	A						C					R	C	C	C		C	C		

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

AP004 Manage Innovation Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
AP004.01 Create an environment conducive to innovation. Create an environment that is conducive to innovation, considering issues such as culture, reward, collaboration, technology forums, and mechanisms to promote and capture employee ideas.	**From**	**Description**	**Description**	**To**
			Innovation plan	Internal
			Recognition and reward programme	AP007.04
Activities				
1. Create an innovation plan that includes risk appetite, the envisioned budget to spend on innovation initiatives, and innovation objectives.				
2. Provide infrastructure that can be an enabler for innovation, such as collaboration tools for enhancing work between geographic locations and divisions.				
3. Create an environment that is conducive to innovation by maintaining relevant HR initiatives, such as innovation recognition and reward programmes, appropriate job rotation, and discretionary time for experimentation.				
4. Maintain a programme enabling staff to submit innovation ideas and create an appropriate decision-making structure to assess and take these ideas forward.				
5. Encourage innovation ideas from customers, suppliers and business partners.				

Personal Copy of: Dr. David Lanter

APO04 Manage Innovation Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO04.02 Maintain an understanding of the enterprise environment. Work with relevant stakeholders to understand their challenges. Maintain an adequate understanding of enterprise strategy and the competitive environment or other constraints so that opportunities enabled by new technologies can be identified.	**From**	**Description**	**Description**	**To**
	Outside COBIT	Enterprise strategy and enterprise SWOT analysis	Innovation opportunities linked to business drivers	APO02.01
Activities				
1. Maintain an understanding of the business drivers, enterprise strategy, industry drivers, enterprise operations and other issues so that the potential value-add of technologies or IT innovation can be identified.				
2. Conduct regular meetings with business units, divisions and/or other stakeholder entities to understand current business problems, process bottlenecks, or other constraints where emerging technologies or IT innovation can create opportunities.				
3. Understand enterprise investment parameters for innovation and new technologies so appropriate strategies are developed.				
Management Practice	**Inputs**		**Outputs**	
APO04.03 Monitor and scan the technology environment. Perform systematic monitoring and scanning of the enterprise's external environment to identify emerging technologies that have the potential to create value (e.g., by realising the enterprise strategy, optimising costs, avoiding obsolescence, and better enabling enterprise and IT processes). Monitor the marketplace, competitive landscape, industry sectors, and legal and regulatory trends to be able to analyse emerging technologies or innovation ideas in the enterprise context.	**From**	**Description**	**Description**	**To**
	Outside COBIT	Emerging technologies	Research analyses of innovation possibilities	BAI03.01
Activities				
1. Understand the enterprise's interest and potential for adopting new technology innovations and focus awareness efforts on the most opportunistic technology innovations.				
2. Perform research and scanning of the external environment, including appropriate web sites, journals and conferences, to identify emerging technologies.				
3. Consult with third-party experts where needed to confirm research findings or as a source of information on emerging technologies.				
4. Capture staff members' IT innovation ideas and analyse them for potential implementation.				
Management Practice	**Inputs**		**Outputs**	
APO04.04 Assess the potential of emerging technologies and innovation ideas. Analyse identified emerging technologies and/or other IT innovation suggestions. Work with stakeholders to validate assumptions on the potential of new technologies and innovation.	**From**	**Description**	**Description**	**To**
			Evaluations of innovation ideas	BAI03.01
			Proof-of-concept scope and outline business case	APO05.03 APO06.02
			Test results from proof-of-concept initiatives	Internal
Activities				
1. Evaluate identified technologies, considering aspects such as time to reach maturity, inherent risk of new technologies (including potential legal implications), fit with the enterprise architecture, and potential to provide additional value.				
2. Identify any issues that may need to be resolved or proven through a proof-of-concept initiative.				
3. Scope the proof-of-concept initiative, including desired outcomes, required budget, time frames and responsibilities.				
4. Obtain approval for the proof-of-concept initiative.				
5. Conduct proof-of-concept initiatives to test emerging technologies or other innovation ideas, identify any issues, and determine whether further implementation or roll-out should be considered based on feasibility and potential ROI.				

Personal Copy of: Dr. David Lanter

AP004 Manage Innovation Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
AP004.05 Recommend appropriate further initiatives. Evaluate and monitor the results of proof-of-concept initiatives and, if favourable, generate recommendations for further initiatives and gain stakeholder support.	**From**	**Description**	**Description**	**To**
			Results and recommendations from proof-of-concept initiatives	APO02.03 BAI03.09
			Analysis of rejected initiatives	APO02.03 BAI03.08
Activities				
1. Document proof-of-concept results, including guidance and recommendations for trends and innovation programmes.				
2. Communicate viable innovation opportunities into the IT strategy and enterprise architecture processes.				
3. Follow up on proof-of-concept initiatives to measure the degree to which they have been leveraged in actual investment.				
4. Analyse and communicate reasons for rejected proof-of-concept initiatives.				
Management Practice	**Inputs**		**Outputs**	
AP004.06 Monitor the implementation and use of innovation. Monitor the implementation and use of emerging technologies and innovations during integration, adoption and for the full economic life cycle to ensure that the promised benefits are realised and to identify lessons learned.	**From**	**Description**	**Description**	**To**
			Assessments of using innovative approaches	APO02.04 BAI03.02
			Evaluation of innovation benefits	APO05.04
			Adjusted innovation plans	Internal
Activities				
1. Assess the implementation of the new technologies or IT innovations adopted as part of IT strategy and enterprise architecture developments and their realisation during programme management of initiatives.				
2. Capture lessons learned and opportunities for improvement.				
3. Adjust the innovation plan, if required.				
4. Identify and evaluate the potential value to be realised from the use of innovation.				

AP004 Related Guidance	
Related Standard	**Detailed Reference**
None	

Personal Copy of: Dr. David Lanter

APO05 Manage Portfolio	Area: Management Domain: Align, Plan and Organise
Process Description Execute the strategic direction set for investments in line with the enterprise architecture vision and the desired characteristics of the investment and related services portfolios, and consider the different categories of investments and the resources and funding constraints. Evaluate, prioritise and balance programmes and services, managing demand within resource and funding constraints, based on their alignment with strategic objectives, enterprise worth and risk. Move selected programmes into the active services portfolio for execution. Monitor the performance of the overall portfolio of services and programmes, proposing adjustments as necessary in response to programme and service performance or changing enterprise priorities.	
Process Purpose Statement Optimise the performance of the overall portfolio of programmes in response to programme and service performance and changing enterprise priorities and demands.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
05 Realised benefits from IT-enabled investments and services portfolio	• Percent of IT-enabled investments where benefit realisation is monitored through the full economic life cycle • Percent of IT services where expected benefits are realised • Percent of IT-enabled investments where claimed benefits are met or exceeded
13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	• Number of programmes/projects on time and within budget • Percent of stakeholders satisfied with programme/project quality • Number of programmes needing significant rework due to quality defects • Cost of application maintenance vs. overall IT cost
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. An appropriate investment mix is defined and aligned with enterprise strategy.	• Percent of IT investments that have traceability to the enterprise strategy • Degree to which enterprise management is satisfied with IT's contribution to the enterprise strategy
2. Sources of investment funding are identified and available.	• Ratio between funds allocated and funds used • Ratio between funds available and funds allocated
3. Programme business cases are evaluated and prioritised before funds are allocated.	• Percent of business units involved in the evaluation and prioritisation process
4. A comprehensive and accurate view of the investment portfolio performance exists.	• Level of satisfaction with the portfolio monitoring reports
5. Investment programme changes are reflected in the relevant IT service, asset and resource portfolios.	• Percent of changes from the investment programme reflected in the relevant IT portfolios
6. Benefits have been realised due to benefit monitoring.	• Percent of investments where realised benefits have been measured and compared to the business case

Personal Copy of: Dr. David Lanter

AP005 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP005.01 Establish the target investment mix.	A	R	R		C					I	C	C				C	C	C	C							
AP005.02 Determine the availability and sources of funds.	C		A		R					C								R								
AP005.03 Evaluate and select programmes to fund.	C	A	R		R		R			R								R	C							
AP005.04 Monitor, optimise and report on investment portfolio performance.	I	C	C	C	C	C	R			A						C	C	C	C				C			
AP005.05 Maintain portfolios.			I	I	R	C	A		R									R		C	C		C			
AP005.06 Manage benefits achievement.		C	C	C	A	R	I	R		I						C	C	R	C				C			

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

AP005 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
AP005.01 Establish the target investment mix. Review and ensure clarity of the enterprise and IT strategies and current services. Define an appropriate investment mix based on cost, alignment with strategy, and financial measures such as cost and expected ROI over the full economic life cycle, degree of risk, and type of benefit for the programmes in the portfolio. Adjust the enterprise and IT strategies where necessary.	**From**	**Description**	**Description**	**To**
	EDM02.02	Investment types and criteria	Defined investment mix	Internal
	AP002.05	• Strategic road map • Risk assessment initiatives • Definition of strategic initiatives	Identified resources and capabilities required to support strategy	Internal
	AP006.02	Prioritisation and ranking of IT initiatives	Feedback on strategy and goals	AP002.05
	AP009.01	Definitions of standard services		
	BAI03.11	Service definitions		
Activities				
1. Validate that IT-enabled investments and current IT services are aligned with enterprise vision, enterprise principles, strategic goals and objectives, enterprise architecture vision, and priorities.				
2. Obtain a common understanding between IT and the other business functions on the potential opportunities for IT to drive and support the enterprise strategy.				
3. Create an investment mix that achieves the right balance amongst a number of dimensions, including an appropriate balance of short- and long-term returns, financial and non-financial benefits, and high- and low-risk investments.				
4. Identify the broad categories of information systems, applications, data, IT services, infrastructure, IT assets, resources, skills, practices, controls and relationships needed to support the enterprise strategy.				
5. Agree on an IT strategy and goals, taking into account the inter-relationships between the enterprise strategy and the IT services, assets and other resources. Identify and leverage synergies that can be achieved.				

Personal Copy of: Dr. David Lanter

APO05 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO05.02 Determine the availability and sources of funds. Determine potential sources of funds, different funding options and the implications of the funding source on the investment return expectations.	**From**	**Description**	**Description**	**To**
			Funding options	APO02.05
			Investment return expectations	EDM02.01 APO02.04 APO06.02 BAI01.06
Activities				
1. Understand the current availability and commitment of funds, the current approved spending, and the actual amount spent to date.				
2. Identify options for obtaining additional funds for IT-enabled investments, internally and from external sources.				
3. Determine the implications of the funding source on the investment return expectations.				
Management Practice	**Inputs**		**Outputs**	
APO05.03 Evaluate and select programmes to fund. Based on the overall investment portfolio mix requirements, evaluate and prioritise programme business cases, and decide on investment proposals. Allocate funds and initiate programmes.	**From**	**Description**	**Description**	**To**
	EDM02.01	• Evaluation of investment and services portfolios • Evaluation of strategic alignment	Programme business case	APO06.02 BAI01.02
	EDM02.02	Investment types and criteria	Business case assessments	APO06.02 BAI01.06
	APO03.01	Architecture concept business case and value proposition	Selected programmes with return on investment (ROI) milestones	EDM02.01 BAI01.04
	APO04.04	Proof-of-concept scope and outline business case		
	APO06.02	Budget allocations		
	APO06.03	• Budget communications • IT budget and plan		
	APO09.01	Identified gaps in IT services to the business		
	APO09.03	SLAs		
	BAI01.02	• Programme benefit realisation plan • Programme mandate and brief • Programme concept business case		
Activities				
1. Recognise investment opportunities and classify them in line with the investment portfolio categories. Specify expected enterprise outcome(s), all initiatives required to achieve the expected outcomes, costs, dependencies and risk, and how all would be measured.				
2. Perform detailed assessments of all programme business cases, evaluating strategic alignment, enterprise benefits, risk and availability of resources.				
3. Assess the impact on the overall investment portfolio of adding candidate programmes, including any changes that might be required to other programmes.				
4. Decide which candidate programmes should be moved to the active investment portfolio. Decide whether rejected programmes should be held for future consideration or provided with some seed funding to determine whether the business case can be improved or discarded.				
5. Determine the required milestones for each selected programme's full economic life cycle. Allocate and reserve total programme funding per milestone. Move the programme into the active investment portfolio.				
6. Establish procedures to communicate the cost, benefit and risk-related aspects of these portfolios to the budget prioritisation, cost management and benefit management processes.				

Personal Copy of: Dr. David Lanter

APO05 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO05.04 Monitor, optimise and report on investment portfolio performance. On a regular basis, monitor and optimise the performance of the investment portfolio and individual programmes throughout the entire investment life cycle.	**From**	**Description**	**Description**	**To**
	EDM02.01	Evaluation of investment and services portfolios	Investment portfolio performance reports	EDM02.03 APO09.04 BAI01.06 MEA01.03
	EDM02.03	• Actions to improve value delivery • Feedback on portfolio and programme performance		
	APO04.06	Evaluation of innovation benefits		
	BAI01.06	Stage-gate review results		
Activities				
1. Review the portfolio on a regular basis to identify and exploit synergies, eliminate duplication between programmes, and identify and mitigate risk.				
2. When changes occur, re-evaluate and reprioritise the portfolio to ensure that the portfolio is aligned with the business strategy and the target mix of investments is maintained so the portfolio is optimising overall value. This may require programmes to be changed, deferred or retired, and new programmes to be initiated.				
3. Adjust the enterprise targets, forecasts, budgets and, if required, the degree of monitoring to reflect the expenditures to be incurred and enterprise benefits to be realised by programmes in the active investment portfolio. Incorporate programme expenditures into chargeback mechanisms.				
4. Provide an accurate view of the performance of the investment portfolio to all stakeholders.				
5. Provide management reports for senior management's review of the enterprise's progress towards identified goals, stating what still needs to be spent and accomplished over what time frames.				
6. Include in the regular performance monitoring information on the extent to which planned objectives have been achieved, risk mitigated, capabilities created, deliverables obtained and performance targets met.				
7. Identify deviations for: • Budget control between actual and budget • Benefit management of: – Actual vs. targets for investments for solutions, possibly expressed in terms of ROI, NPV or internal rate of return (IRR) – The actual trend of service portfolio cost for service delivery productivity improvements				
8. Develop metrics for measuring IT's contribution to the enterprise, and establish appropriate performance targets reflecting the required IT and enterprise capability targets. Use guidance from external experts and benchmark data to develop metrics.				
Management Practice	**Inputs**		**Outputs**	
APO05.05 Maintain portfolios. Maintain portfolios of investment programmes and projects, IT services and IT assets.	**From**	**Description**	**Description**	**To**
	BAI01.14	Communication of programme retirement and ongoing accountabilities	Updated portfolios of programmes, services and assets	APO09.02 BAI01.01
	BAI03.11	Updated service portfolio		
Activities				
1. Create and maintain portfolios of IT-enabled investment programmes, IT services and IT assets, which form the basis for the current IT budget and support the IT tactical and strategic plans.				
2. Work with service delivery managers to maintain the service portfolios and with operations managers and architects to maintain the asset portfolios. Prioritise portfolios to support investment decisions.				
3. Remove the programme from the active investment portfolio when the desired enterprise benefits have been achieved or when it is clear that benefits will not be achieved within the value criteria set for the programme.				

Personal Copy of: Dr. David Lanter

APO05 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO05.06 Manage benefits achievement. Monitor the benefits of providing and maintaining appropriate IT services and capabilities, based on the agreed-on and current business case.	**From**	**Description**	**Description**	**To**
	BAI01.04	Programme budget and benefits register	Benefit results and related communications	EDM02.01 APO09.04 BAI01.06
	BAI01.05	Results of benefit realisation monitoring	Corrective actions to improve benefit realisation	APO09.04 BAI01.06
Activities				
1. Use the agreed-on metrics and track how benefits are achieved, how they evolve throughout the life cycle of programmes and projects, how they are being delivered from IT services, and how they compare to internal and industry benchmarks. Communicate results to stakeholders.				
2. Implement corrective action when achieved benefits significantly deviate from expected benefits. Update the business case for new initiatives and implement business process and service improvements as required.				
3. Consider obtaining guidance from external experts, industry leaders and comparative benchmarking data to test and improve the metrics and targets.				

APO05 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	• 3.1 Management responsibility • 4.0 Planning and implementing service management • 5.0 Planning and implementing new or changed services
ITIL V3 2011	Service Strategy, 4.2 Service Portfolio Management
Skills Framework for the Information Age (SFIA)	

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

APO06 Manage Budget and Costs	Area: Management Domain: Align, Plan and Organise
Process Description Manage the IT-related financial activities in both the business and IT functions, covering budget, cost and benefit management, and prioritisation of spending through the use of formal budgeting practices and a fair and equitable system of allocating costs to the enterprise. Consult stakeholders to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed.	
Process Purpose Statement Foster partnership between IT and enterprise stakeholders to enable the effective and efficient use of IT-related resources and provide transparency and accountability of the cost and business value of solutions and services. Enable the enterprise to make informed decisions regarding the use of IT solutions and services.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
05 Realised benefits from IT-enabled investments and services portfolio	• Percent of IT-enabled investments where benefit realisation is monitored through the full economic life cycle • Percent of IT services where expected benefits are realised • Percent of IT-enabled investments where claimed benefits are met or exceeded
06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. A transparent and complete budget for IT accurately reflects planned expenditures.	• Number of budget changes due to omissions and errors • Numbers of deviations between expected and actual budget categories
2. The allocation of IT resources for IT initiatives is prioritised based on enterprise needs.	• Percent of alignment of IT resources with high-priority initiatives • Number of resource allocation issues escalated
3. Costs for services are allocated in an equitable way.	• Percent of overall IT costs that are allocated according to the agreed-on cost models
4. Budgets can be accurately compared to actual costs.	• Percent of variance amongst budgets, forecasts and actual costs

APO06 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO06.01 Manage finance and accounting.			A	C	C				C	R							C	C				R				
APO06.02 Prioritise resource allocation.		I	R		C	C	C	I	C	C		I						A	I	C	C	R	C	C		
APO06.03 Create and maintain budgets.		I	A		C	C	C	C	C	C								R	C	C	C	R	C	C	C	
APO06.04 Model and allocate costs.			C		C	C	C	C	C	C								A	C	C	C	R	C	C		
APO06.05 Manage costs.			R		C	C	C	C	C	C								A	C	C	C	R	C	C		

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

APO06 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
APO06.01 Manage finance and accounting. Establish and maintain a method to account for all IT-related costs, investments and depreciation as an integral part of the enterprise financial systems and chart of accounts to manage the investments and costs of IT. Capture and allocate actual costs, analyse variances between forecasts and actual costs, and report using the enterprise's financial measurement systems.	**From**	**Description**	**Description**	**To**
	BAI09.01	Asset register	Accounting processes	Internal
			IT costs classification scheme	Internal
			Financial planning practices	Internal
Activities				
1. Define processes, inputs and outputs, and responsibilities in alignment with the enterprise budgeting and cost accounting policies and approach to systematically drive IT budgeting and costing; enable fair, transparent, repeatable and comparable estimation of IT costs and benefits for input to the portfolio of IT-enabled business programmes; and ensure that budgets and costs are maintained in the IT asset and services portfolios.				
2. Define a classification scheme to identify all IT-related cost elements, how they are allocated across budgets and services, and how they are captured.				
3. Use financial and portfolio information to provide input to business cases for new investments in IT assets and services.				
4. Define how to analyse, report (to whom and how), and use the budget control and benefit management processes.				
5. Establish and maintain practices for financial planning, investment management and decision making, and the optimisation of recurring operational costs to deliver maximum value to the enterprise for the least expenditure.				
Management Practice	**Inputs**		**Outputs**	
APO06.02 Prioritise resource allocation. Implement a decision-making process to prioritise the allocation of resources and rules for discretionary investments by individual business units. Include the potential use of external service providers and consider the buy, develop and rent options.	**From**	**Description**	**Description**	**To**
	EDM02.01	Evaluation of investment and services portfolios	Prioritisation and ranking of IT initiatives	APO05.01
	EDM02.03	Actions to improve value delivery	Budget allocations	APO02.05 APO05.03 APO07.05 BAI03.11
	APO04.04	Proof-of-concept scope and outline business case		
	APO05.02	Investment return expectations		
	APO05.03	• Business case assessments • Programme business case		
Activities				
1. Establish a decision-making body for prioritising business and IT resources, including use of external service providers within the high-level budget allocations for IT-enabled programmes, IT services and IT assets as established by the strategic and tactical plans. Consider the options for buying or developing capitalised assets and services vs. externally utilised assets and services on a pay-for-use basis.				
2. Rank all IT initiatives based on business cases and strategic and tactical plans, and establish procedures to determine budget allocations and cut-off. Establish a procedure to communicate budget decisions and review them with the business unit budget holders.				
3. Identify, communicate and resolve significant impacts of budget decisions on business cases, portfolios and strategy plans (e.g., when budgets may require revision due to changing enterprise circumstances, when they are not sufficient to support strategic objectives or business case objectives).				
4. Obtain ratification from the executive committee for the overall IT budget changes that negatively impact the entity's strategic or tactical plans and offer suggested actions to resolve these impacts.				

Personal Copy of: Dr. David Lanter

APO06 Process Practices, Inputs/Outputs and Activities *(cont.)*

Management Practice	Inputs		Outputs	
APO06.03 Create and maintain budgets. Prepare a budget reflecting the investment priorities supporting strategic objectives based on the portfolio of IT-enabled programmes and IT services.	**From**	**Description**	**Description**	**To**
			IT budget and plan	APO02.05 APO05.03 APO07.01 BAI03.11
			Budget communications	APO02.05 APO05.03 APO07.01 BAI03.11

Activities

1. Implement a formal IT budget, including all expected IT costs of IT-enabled programmes, IT services and IT assets as directed by the strategy, programmes and portfolios.
2. When creating the budget, consider the following components:
   - Alignment with the business
   - Alignment with the sourcing strategy
   - Authorised sources of funding
   - Internal resource costs, including personnel, information assets and accommodations
   - Third-party costs, including outsourcing contracts, consultants and service providers
   - Capital and operational expenses
   - Cost elements that depend on the workload
3. Document the rationale to justify contingencies and review them regularly.
4. Instruct process, service and programme owners, as well as project and asset managers, to plan budgets.
5. Review the budget plans and make decisions about budget allocations. Compile and adjust the budget based on changing enterprise needs and financial considerations.
6. Record, maintain and communicate the current IT budget, including committed expenditures and current expenditures, considering IT projects recorded in the IT-enabled investment portfolios and operation and maintenance of asset and service portfolios.
7. Monitor the effectiveness of the different aspects of budgeting and use the results to implement improvements to ensure that future budgets are more accurate, reliable and cost-effective.

Management Practice	Inputs		Outputs	
APO06.04 Model and allocate costs. Establish and use an IT costing model based on the service definition, ensuring that allocation of costs for services is identifiable, measurable and predictable, to encourage the responsible use of resources including those provided by service providers. Regularly review and benchmark the appropriateness of the cost/chargeback model to maintain its relevance and appropriateness to the evolving business and IT activities.	**From**	**Description**	**Description**	**To**
			Categorised IT costs	Internal
			Cost allocation model	Internal
			Cost allocation communications	Internal
			Operational procedures	Internal

Activities

1. Categorise all IT costs appropriately, including those relating to service providers, according to the enterprise management accounting framework.
2. Inspect service definition catalogues to identify services subject to user chargeback and those that are shared services.
3. Define and agree on a model that:
   - Supports the calculation of chargeback rates per service
   - Defines how IT costs will be calculated/charged
   - Is differentiated, where and when appropriate
   - Is aligned with the IT budget
4. Design the cost model to be transparent enough to allow users to identify their actual usage and charges, and to better enable predictability of IT costs and efficient and effective utilisation of IT resources.
5. After review with user departments, obtain approval and communicate the IT costing model inputs and outputs to the management of user departments.
6. Communicate changes in the cost/chargeback model with enterprise process owners.

Personal Copy of: Dr. David Lanter

APO06 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO06.05 Manage costs. Implement a cost management process comparing actual costs to budgets. Costs should be monitored and reported and, in the case of deviations, identified in a timely manner and their impact on enterprise processes and services assessed.	**From**	**Description**	**Description**	**To**
	EDM02.03	Feedback on portfolio and programme performance	Cost data collection method	Internal
	BAI01.02	Programme benefit realisation plan	Cost consolidation method	Internal
	BAI01.04	Programme budget and benefits register	Cost optimisation opportunities	APO02.02
	BAI01.05	Results of benefit realisation monitoring		
Activities				
1. Ensure proper authority and independence between IT budget holders and the individuals who capture, analyse and report financial information.				
2. Establish time scales for the operation of the cost management process in line with budgeting and accounting requirements.				
3. Define a method for the collection of relevant data to identify deviations for: • Budget control between actual and budget • Benefit management of: – Actual vs. targets for investments for solutions; possibly expressed in terms of ROI, NPV or IRR – The actual trend of service cost for cost optimisation of services (e.g., defined as cost per user) – Actual vs. budget for responsiveness and predictability improvements of solutions delivery • Cost distribution between direct and indirect (absorbed and unabsorbed) costs				
4. Define how costs are consolidated for the appropriate levels in the enterprise and how they will be presented to the stakeholders. The reports provide information to enable the timely identification of required corrective actions.				
5. Instruct those responsible for cost management to capture, collect and consolidate the data, and present and report the data to the appropriate budget owners. Budget analysts and owners jointly analyse deviations and compare performance to internal and industry benchmarks. The result of the analysis provides an explanation of significant deviations and the suggested corrective actions.				
6. Ensure that the appropriate levels of management review the results of the analysis and approve suggested corrective actions.				
7. Align IT budgets and services to the IT infrastructure, enterprise processes and owners who use them.				
8. Ensure that changes in cost structures and enterprise needs are identified and budgets and forecasts are revised as required.				
9. At regular intervals, and especially when budgets are cut due to financial constraints, identify ways to optimise costs and introduce efficiencies without jeopardising services.				

APO06 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	6.4 Budgeting and accounting for IT services
ITIL V3 2011	Service Strategy, 4.3 Financial Management of IT Services

Personal Copy of: Dr. David Lanter

APO07 Manage Human Resources	Area: Management Domain: Align, Plan and Organise
Process Description Provide a structured approach to ensure optimal structuring, placement, decision rights and skills of human resources. This includes communicating the defined roles and responsibilities, learning and growth plans, and performance expectations, supported with competent and motivated people.	
Process Purpose Statement Optimise human resources capabilities to meet enterprise objectives.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	• Number of programmes/projects on time and within budget • Percent of stakeholders satisfied with programme/project quality • Number of programmes needing significant rework due to quality defects • Cost of application maintenance vs. overall IT cost
16 Competent and motivated business and IT personnel	• Percent of staff whose IT-related skills are sufficient for the competency required for their role • Percent of staff satisfied with their IT-related roles • Number of learning/training hours per staff member
17 Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of IT innovation possibilities • Level of stakeholder satisfaction with levels of IT innovation expertise and ideas • Number of approved initiatives resulting from innovative IT ideas
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. The IT organisational structure and relationships are flexible and responsive.	• Number of service definitions and service catalogues • Level of executive satisfaction with management decision making • Number of decisions that could not be resolved within management structures and were escalated to governance structures
2. Human resources are effectively and efficiently managed.	• Percent of staff turnover • Average duration of vacancies • Percent of IT posts vacant

Personal Copy of: Dr. David Lanter

APO07 RACI Chart																								
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO07.01 Maintain adequate and appropriate staffing.									R		I				R			A	R	R	R	R	R	R	R	
APO07.02 Identify key IT personnel.									R						R			A	R	R	R	R	R	R	R	
APO07.03 Maintain the skills and competencies of personnel.									R						R			A	R	R	R	R	R	R	R	
APO07.04 Evaluate employee job performance.									R						R			A	R	R	R	R	R	R	R	
APO07.05 Plan and track the usage of IT and business human resources.					R	C	A	R	R						I			R	R	R	R	R	R	R	R	
APO07.06 Manage contract staff.									R						R			A	R	R	R	R	R	R	R	

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

APO07 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
APO07.01 Maintain adequate and appropriate staffing. Evaluate staffing requirements on a regular basis or upon major changes to the enterprise or operational or IT environments to ensure that the enterprise has sufficient human resources to support enterprise goals and objectives. Staffing includes both internal and external resources.	EDM04.01	• Approved resources plan • Guiding principles for allocation of resources and capabilities	Staffing requirement evaluations	Internal
	EDM04.03	Remedial actions to address resource management deviations	Competency and career development plans	Internal
	APO01.02	Definition of supervisory practices	Personnel sourcing plans	Internal
	APO06.03	• Budget communications • IT budget and plan		
	Outside COBIT	• Enterprise goals and objectives • Enterprise HR policies and procedures		
Activities				
1. Evaluate staffing requirements on a regular basis or upon major changes to ensure that the: • IT function has sufficient resources to adequately and appropriately support enterprise goals and objectives • Enterprise has sufficient resources to adequately and appropriately support business processes and controls and IT-enabled initiatives				
2. Maintain business and IT personnel recruitment and retention processes in line with the overall enterprise's personnel policies and procedures.				
3. Include background checks in the IT recruitment process for employees, contractors and vendors. The extent and frequency of these checks should depend on the sensitivity and/or criticality of the function.				
4. Establish flexible resource arrangements to support changing business needs, such as the use of transfers, external contractors and third-party service arrangements.				
5. Ensure that cross-training takes place and there is backup to key staff to reduce single-person dependency.				

Personal Copy of: Dr. David Lanter

APO07 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO07.02 Identify key IT personnel. Identify key IT personnel while minimising reliance on a single individual performing a critical job function through knowledge capture (documentation), knowledge sharing, succession planning and staff backup.	**From**	**Description**	**Description**	**To**
			List of key personnel	Internal
Activities				
1. Minimise reliance on a single individual performing a critical job function through knowledge capture (documentation), knowledge sharing, succession planning, staff backup, cross-training and job rotation initiatives.				
2. As a security precaution, provide guidelines on a minimum time of annual vacation to be taken by key individuals.				
3. Take expedient actions regarding job changes, especially job terminations.				
4. Regularly test staff backup plans.				
Management Practice	**Inputs**		**Outputs**	
APO07.03 Maintain the skills and competencies of personnel. Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfil their roles on the basis of their education, training and/or experience, and verify that these competencies are being maintained, using qualification and certification programmes where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals.	**From**	**Description**	**Description**	**To**
	EDM01.02	Reward system approach	Skills and competencies matrix	APO01.02 BAI01.02 BAI01.04
	EDM04.03	Remedial actions to address resource management deviations	Skills development plans	EDM04.01 APO01.02
	BAI08.03	Published knowledge repositories	Review reports	Internal
	BAI08.04	Knowledge awareness and training schemes		
	DSS04.06	• Monitoring results of skills and competencies • Training requirements		
	Outside COBIT	Enterprise goals and objectives		
Activities				
1. Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.				
2. Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.				
3. Provide access to knowledge repositories to support the development of skills and competencies.				
4. Identify gaps between required and available skills and develop action plans to address them on an individual and collective basis, such as training (technical and behavioural skills), recruitment, redeployment and changed sourcing strategies.				
5. Develop and deliver training programmes based on organisational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct and security.				
6. Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.				
7. Review training materials and programmes on a regular basis to ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.				

Personal Copy of: Dr. David Lanter

AP007 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
AP007.04 Evaluate employee job performance. Perform timely performance evaluations on a regular basis against individual objectives derived from the enterprise's goals, established standards, specific job responsibilities, and the skills and competency framework. Employees should receive coaching on performance and conduct whenever appropriate.	**From**	**Description**	**Description**	**To**
	EDM01.02	Reward system approach	Personnel goals	Internal
	AP004.01	Recognition and reward programme	Performance evaluations	Internal
	BAI05.04	Aligned HR performance objectives	Improvement plans	Internal
	BAI05.06	HR performance review results		
	DSS06.03	Allocated access rights		
	Outside COBIT	Enterprise goals and objectives		
Activities				
1. Consider functional/enterprise goals as the context for setting individual goals.				
2. Set individual goals aligned with the relevant process goals so that there is a clear contribution to IT and enterprise goals. Base goals on SMART objectives (specific, measurable, achievable, relevant and time-bound) that reflect core competencies, enterprise values and skills required for the role(s).				
3. Compile 360-degree performance evaluation results.				
4. Implement and communicate a disciplinary process.				
5. Provide specific instructions for the use and storage of personal information in the evaluation process, in compliance with applicable personal data and employment legislation.				
6. Provide timely feedback regarding performance against the individual's goals.				
7. Implement a remuneration/recognition process that rewards appropriate commitment, competency development and successful attainment of performance goals. Ensure that the process is applied consistently and in line with organisational policies.				
8. Develop performance improvement plans based on the results of the evaluation process and identified training and skills development requirements.				
Management Practice	**Inputs**		**Outputs**	
AP007.05 Plan and track the usage of IT and business human resources. Understand and track the current and future demand for business and IT human resources with responsibilities for enterprise IT. Identify shortfalls and provide input into sourcing plans, enterprise and IT recruitment processes sourcing plans, and business and IT recruitment processes.	**From**	**Description**	**Description**	**To**
	EDM04.02	Communication of resourcing strategies	Inventory of business and IT human resources	BAI01.04
	EDM04.03	Feedback on allocation and effectiveness of resources and capabilities	Resourcing shortfall analyses	BAI01.06
	AP006.02	Budget allocations	Resource utilisation records	BAI01.06
	BAI01.04	Resource requirements and roles		
	BAI01.12	Project resource requirements		
	Outside COBIT	Enterprise organisation structure		
Activities				
1. Create and maintain an inventory of business and IT human resources.				
2. Understand the current and future demand for human resources to support the achievement of IT objectives and to deliver services and solutions based on the portfolio of current IT-related initiatives, the future investment portfolio and day-to-day operational needs.				
3. Identify shortfalls and provide input into sourcing plans as well as enterprise and IT recruitment processes. Create and review the staffing plan, keeping track of actual usage.				
4. Maintain adequate information on the time spent on different tasks, assignments, services or projects.				

Personal Copy of: Dr. David Lanter

APO07 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO07.06 Manage contract staff. Ensure that consultants and contract personnel who support the enterprise with IT skills know and comply with the organisation's policies and meet agreed-on contractual requirements.	**From**	**Description**	**Description**	**To**
	BAI01.04	Resource requirements and roles	Contract staff policies	Internal
	BAI01.12	Project resource requirements	Contract agreements	Internal
	BAI01.14	Communication of programme retirement and ongoing accountabilities	Contract agreement reviews	Internal
Activities				
1. Implement policies and procedures that describe when, how and what type of work can be performed or augmented by consultants and/or contractors, in accordance with the organisation's enterprisewide IT procurement policy and the IT control framework.				
2. Obtain formal agreement from contractors at the commencement of the contract that they are required to comply with the enterprise's IT control framework, such as policies for security clearance, physical and logical access control, use of facilities, information confidentiality requirements, and non-disclosure agreements.				
3. Advise contractors that management reserves the right to monitor and inspect all usage of IT resources, including email, voice communications, and all programs and data files.				
4. Provide contractors with a clear definition of their roles and responsibilities as part of their contracts, including explicit requirements to document their work to agreed-on standards and formats.				
5. Review contractors' work and base the approval of payments on the results.				
6. Define all work performed by external parties in formal and unambiguous contracts.				
7. Conduct periodic reviews to ensure that contract staff have signed and agreed on all necessary agreements.				
8. Conduct periodic reviews to ensure that contractors' roles and access rights are appropriate and in line with agreements.				

APO07 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 27002	8. Human Resources Security
SFIA	Skills reference

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

APO08 Manage Relationships	Area: Management Domain: Align, Plan and Organise
Process Description Manage the relationship between the business and IT in a formalised and transparent way that ensures a focus on achieving a common and shared goal of successful enterprise outcomes in support of strategic goals and within the constraint of budgets and risk tolerance. Base the relationship on mutual trust, using open and understandable terms and common language and a willingness to take ownership and accountability for key decisions.	
Process Purpose Statement Create improved outcomes, increased confidence, trust in IT and effective use of resources.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
12 Enablement and support of business processes by integrating applications and technology into business processes	• Number of business processing incidents caused by technology integration errors • Number of business process changes that need to be delayed or reworked because of technology integration issues • Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues • Number of applications or critical infrastructures operating in silos and not integrated
17 Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of IT innovation possibilities • Level of stakeholder satisfaction with levels of IT innovation expertise and ideas • Number of approved initiatives resulting from innovative IT ideas
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Business strategies, plans and requirements are well understood, documented and approved.	• Percent of alignment of IT services with enterprise business requirements
2. Good relationships exist between the enterprise and IT.	• Ratings of user and IT personnel satisfaction surveys
3. Business stakeholders are aware of technology-enabled opportunities.	• Survey of business stakeholder technology level of awareness • Inclusion rate of technology opportunities in investment proposals

Personal Copy of: Dr. David Lanter

AP008 RACI Chart																										
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP008.01 Understand business expectations.		C	C	C	C	R	C		C		C					C	C	A	C	R	R	C	R	R	R	
AP008.02 Identify opportunities, risk and constraints for IT to enhance the business.		I		I	I	R	R				C			I		C	C	A	R	R	R		R			
AP008.03 Manage the business relationship.		C	C	C	R	R	I											A		R	R		R			
AP008.04 Co-ordinate and communicate.		R	I	R	R	R	I											A		R	R		R			
AP008.05 Provide input to the continual improvement of services.		C		I	C	R	I		C							C	C	A	C	R	R		R	C	C	

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

AP008 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
AP008.01 Understand business expectations. Understand current business issues and objectives and business expectations for IT. Ensure that requirements are understood, managed and communicated, and their status agreed on and approved.	**From**	**Description**	**Description**	**To**
	AP002.05	Strategic road map	Clarified and agreed-on business expectations	Internal
Activities				
1. Identify business stakeholders, their interests and their areas of responsibilities.				
2. Review current enterprise direction, issues, strategic objectives, and alignment with enterprise architecture.				
3. Maintain an awareness of business processes and associated activities and understand demand patterns that relate to service volumes and use.				
4. Clarify business expectations for IT-enabled services and solutions and ensure that requirements are defined with associated business acceptance criteria and metrics.				
5. Confirm agreement of business expectations, acceptance criteria and metrics to relevant parts of IT by all stakeholders.				
6. Manage expectations by ensuring that business units understand priorities, dependencies, financial constraints and the need to schedule requests.				
7. Understand the current business environment, process constraints or issues, geographical expansion or contraction, and industry/regulatory drivers.				

Personal Copy of: Dr. David Lanter

APO08 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO08.02 Identify opportunities, risk and constraints for IT to enhance the business. Identify potential opportunities for IT to be an enabler of enhanced enterprise performance.	**From**	**Description**	**Description**	**To**
	APO09.01	Identified gaps in IT services to the business	Agreed-on next steps and action plans	Internal
	APO09.04	• Improvement action plans and remediations • Service level performance reports		
	APO11.05	Root causes of quality delivery failures		
Activities				
1. Understand technology trends and new technologies and how these can be applied innovatively to enhance business process performance.				
2. Play a proactive role in identifying and communicating with key stakeholders on opportunities, risk and constraints. This includes current and emerging technologies, services and business process models.				
3. Collaborate in agreeing on next steps for major new initiatives in co-operation with portfolio management, including business case development.				
4. Ensure that the business and IT understand and appreciate the strategic objectives and enterprise architecture vision.				
5. Co-ordinate when planning new IT initiatives to ensure integration and alignment with the enterprise architecture.				
Management Practice	**Inputs**		**Outputs**	
APO08.03 Manage the business relationship. Manage the relationship with customers (business representatives). Ensure that relationship roles and responsibilities are defined and assigned, and communication is facilitated.	**From**	**Description**	**Description**	**To**
	DSS02.02	Classified and prioritised incidents and service requests	Agreed-on key decisions	Internal
	DSS02.06	• User confirmation of satisfactory fulfilment or resolution • Closed service requests and incidents	Complaint and escalation status	Internal
	DSS02.07	• Request fulfilment status and trends report • Incident status and trends report		
Activities				
1. Assign a relationship manager as a single point of contact for each significant business unit. Ensure that a single counterpart is identified in the business organisation and the counterpart has business understanding, sufficient technology awareness and the appropriate level of authority.				
2. Manage the relationship in a formalised and transparent way that ensures a focus on achieving a common and shared goal of successful enterprise outcomes in support of strategic goals and within the constraint of budgets and risk tolerance.				
3. Define and communicate a complaints and escalation procedure to resolve any relationship issues.				
4. Plan specific interactions and schedules based on mutually agreed-on objectives and common language (service and performance review meetings, review of new strategies or plans, etc.).				
5. Ensure that key decisions are agreed on and approved by relevant accountable stakeholders.				

Personal Copy of: Dr. David Lanter

AP008 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
AP008.04 Co-ordinate and communicate. Work with stakeholders and co-ordinate the end-to-end delivery of IT services and solutions provided to the business.	**From**	**Description**	**Description**	**To**
	AP009.03	SLAs	Communication plan	Internal
	AP012.06	Risk impact communication	Communication packages	Internal
	BAI05.05	Operation and use plan	Customer responses	Internal
	BAI07.07	Supplemental support plan		
	BAI09.02	Communications of planned maintenance downtime		
	DSS03.04	Communication of knowledge learned		
Activities				
1. Co-ordinate and communicate changes and transition activities such as project or change plans, schedules, release policies, release known errors, and training awareness.				
2. Co-ordinate and communicate operational activities, roles and responsibilities, including the definition of request types, hierarchical escalation, major outages (planned and unplanned), and contents and frequency of service reports.				
3. Take ownership of the response to the business for major events that may influence the relationship with the business. Provide direct support if required.				
4. Maintain an end-to-end communication plan that defines the content, frequency and recipients of service delivery information, including status of value delivered and any risk identified.				
Management Practice	**Inputs**		**Outputs**	
AP008.05 Provide input to the continual improvement of services. Continually improve and evolve IT-enabled services and service delivery to the enterprise to align with changing enterprise and technology requirements.	**From**	**Description**	**Description**	**To**
	AP009.02	Service catalogues	Satisfaction analyses	AP009.04
	AP011.03	• Review results of quality of service, including customer feedback • Customer requirements for quality management	Definition of potential improvement projects	AP002.02 BAI03.11
	AP011.04	Results of quality reviews and audits		
	AP011.05	Results of solution and service delivery quality monitoring		
	BAI03.10	Maintenance plan		
	BAI05.05	Success measures and results		
	BAI07.07	Supplemental support plan		
Activities				
1. Perform customer and provider satisfaction analysis. Ensure that issues are actioned and report results and status.				
2. Work together to identify, communicate and implement improvement initiatives.				
3. Work with service management and process owners to ensure that IT-enabled services and service management processes are continually improved and the root causes of any issues are identified and resolved.				

AP008 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	7.2 Business relationship management
ITIL V3 2011	• Service Strategy, 4.4 Demand Management • Service Strategy, 4.5 Business Relationship Management

Personal Copy of: Dr. David Lanter

APO09 Manage Service Agreements	Area: Management Domain: Align, Plan and Organise
Process Description Align IT-enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators.	
Process Purpose Statement Ensure that IT services and service levels meet current and future enterprise needs.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
14 Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. The enterprise can effectively utilise IT services as defined in a catalogue.	• Number of business processes with undefined service agreements
2. Service agreements reflect enterprise needs and the capabilities of IT.	• Percent of live IT services covered by service agreements • Percent of customers satisfied that service delivery meets agreed-on levels
3. IT services perform as stipulated in service agreements.	• Number and severity of service breaches • Percent of services being monitored to service levels • Percent of service targets being met

APO09 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO09.01 Identify IT services.		C		R	R	R	C		I							I	I	R	I	C	C	C	A	I	I	
APO09.02 Catalogue IT-enabled services.					I	I			I							I	I	R	I	C	C	C	A	I	I	
APO09.03 Define and prepare service agreements.					R	C			C		C					C	C	R		C	R	R	A	C	C	
APO09.04 Monitor and report service levels.		I		I	I	R					C							I		I	I	I	A			
APO09.05 Review service agreements and contracts.					A	C			C		C					C	C	R		C	R	R	R	C	C	I

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

APO09 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
APO09.01 Identify IT services. Analyse business requirements and the way in which IT-enabled services and service levels support business processes. Discuss and agree on potential services and service levels with the business, and compare them with the current service portfolio to identify new or changed services or service level options.	**From**	**Description**	**Description**	**To**
			Identified gaps in IT services to the business	APO02.02 APO05.03 APO08.02
			Definitions of standard services	APO05.01
Activities				
1. Assess current IT services and service levels to identify gaps between existing services and the business activities they support. Identify areas for improvement of existing services and service level options.				
2. Analyse, study and estimate future demand and confirm capacity of existing IT-enabled services.				
3. Analyse business process activities to identify the need for new or redesigned IT services.				
4. Compare identified requirements to existing service components in the portfolio. If possible, package existing service components (IT services, service level options and service packages) into new service packages to meet identified business requirements.				
5. Where possible, match demands to service packages and create standardised services to obtain overall efficiencies.				
6. Regularly review the portfolio of IT services with portfolio management and business relationship management to identify obsolete services. Agree on retirement and propose change.				
Management Practice	**Inputs**		**Outputs**	
APO09.02 Catalogue IT-enabled services. Define and maintain one or more service catalogues for relevant target groups. Publish and maintain live IT-enabled services in the service catalogues.	**From**	**Description**	**Description**	**To**
	EDM04.01	Approved resources plan	Service catalogues	APO08.05
	EDM04.02	Communication of resourcing strategies		
	APO05.05	Updated portfolios of programmes, services and assets		
Activities				
1. Publish in catalogues relevant live IT-enabled services, service packages and service level options from the portfolio.				
2. Continually ensure that the service components in the portfolio and the related service catalogues are complete and up to date.				
3. Inform business relationship management of any updates to the service catalogues.				
Management Practice	**Inputs**		**Outputs**	
APO09.03 Define and prepare service agreements. Define and prepare service agreements based on the options in the service catalogues. Include internal operational agreements.	**From**	**Description**	**Description**	**To**
	APO11.03	Customer requirements for quality management	SLAs	APO05.03 APO08.04 DSS01.02 DSS02.01 DSS02.02 DSS04.01 DSS05.02 DSS05.03
	BAI03.02	SLA and OLA revisions		
			OLAs	DSS01.02 DSS02.07 DSS04.03 DSS05.03
Activities				
1. Analyse requirements for new or changed service agreements received from business relationship management to ensure that the requirements can be matched. Consider aspects such as service times, availability, performance, capacity, security, continuity, compliance and regulatory issues, usability, and demand constraints.				
2. Draft customer service agreements based on the services, service packages and service level options in the relevant service catalogues.				
3. Determine, agree on and document internal operational agreements to underpin the customer service agreements, if applicable.				
4. Liaise with supplier management to ensure that appropriate commercial contracts with external service providers underpin the customer service agreements, if applicable.				
5. Finalise customer service agreements with business relationship management.				

Personal Copy of: Dr. David Lanter

APO09 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO09.04 Monitor and report service levels. Monitor service levels, report on achievements and identify trends. Provide the appropriate management information to aid performance management.	**From**	**Description**	**Description**	**To**
	EDM04.03	Remedial actions to address resource management deviations	Service level performance reports	APO08.02 MEA01.03
	APO05.04	Investment portfolio performance reports	Improvement action plans and remediations	APO02.02 APO08.02
	APO05.06	• Corrective actions to improve benefit realisation • Benefit results and related communications		
	APO08.05	Satisfaction analyses		
	APO11.04	Results of quality reviews and audits		
	APO11.05	• Root causes of quality delivery failures • Results of solution and service delivery quality monitoring		
	DSS02.02	Classified and prioritised incidents and service requests		
	DSS02.06	Closed service requests and incidents		
	DSS02.07	• Request fulfilment status and trends report • Incident status and trends report		
Activities				
1. Establish and maintain measures to monitor and collect service level data.				
2. Evaluate performance and provide regular and formal reporting of service agreement performance, including deviations from the agreed-on values. Distribute this report to business relationship management.				
3. Perform regular reviews to forecast and identify trends in service level performance.				
4. Provide the appropriate management information to aid performance management.				
5. Agree on action plans and remediations for any performance issues or negative trends.				
Management Practice	**Inputs**		**Outputs**	
APO09.05 Review service agreements and contracts. Conduct periodic reviews of the service agreements and revise when needed.	**From**	**Description**	**Description**	**To**
	EDM04.03	Feedback on allocation and effectiveness of resources and capabilities	SLA revisions	Internal
	APO11.03	Results of quality of service, including customer feedback		
	APO11.04	Results of quality reviews and audits		
	BAI04.01	Evaluations against SLAs		
Activities				
1. Regularly review service agreements according to the agreed-on terms to ensure that they are effective and up to date and changes in requirements, IT-enabled services, service packages or service level options are taken into account, when appropriate.				

Personal Copy of: Dr. David Lanter

AP009 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	• 5.0 Planning and implementing new or changed services • 6.1 Service level management
ITIL V3 2011	• Service Strategy, 4.4 Demand Management • Service Strategy, 4.2 Service Portfolio Management • Service Design, 4.2 Service Catalogue Management • Service Design, 4.3 Service Level Management

Personal Copy of: Dr. David Lanter

APO10 Manage Suppliers	Area: Management Domain: Align, Plan and Organise
Process Description Manage IT-related services provided by all types of suppliers to meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance.	
Process Purpose Statement Minimise the risk associated with non-performing suppliers and ensure competitive pricing.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
09 IT agility	• Level of satisfaction of business executives with IT's responsiveness to new requirements • Number of critical business processes supported by up-to-date infrastructure and applications • Average time to turn strategic IT objectives into an agreed-on and approved initiative
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Suppliers perform as agreed.	• Percent of suppliers meeting agreed-on requirements • Number of service breaches to IT-related services caused by suppliers
2. Supplier risk is assessed and properly addressed.	• Number of risk-related events leading to service incidents • Frequency of risk management sessions with supplier • Percent of risk-related incidents resolved acceptably (time and cost)
3. Supplier relationships are working effectively.	• Number of supplier review meetings • Number of formal disputes with suppliers • Percent of disputes resolved amicably in a reasonable time frame

APO10 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO10.01 Identify and evaluate supplier relationships and contracts.			C			C									C	C	C	A	C	C	C	R	C	C	C	
APO10.02 Select suppliers.			C			C									C	C	C	A	C	C	C	R	C	C	C	
APO10.03 Manage supplier relationships and contracts.						I									C	C	C	A	C	R	R	R	C	C	C	
APO10.04 Manage supplier risk.						C					R				C	C	C	A	C	R	R		C	C	C	C
APO10.05 Monitor supplier performance and compliance.			I			C					C				C	C	C	A	C	R	R		C	C	C	C

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

APO10 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
APO10.01 Identify and evaluate supplier relationships and contracts. Identify suppliers and associated contracts and categorise them into type, significance and criticality. Establish supplier and contract evaluation criteria and evaluate the overall portfolio of existing and alternative suppliers and contracts.	**From**	**Description**	**Description**	**To**
	Outside COBIT	Supplier contracts	Supplier significance and evaluation criteria	Internal
			Supplier catalogue	BAI02.02
			Potential revisions to supplier contracts	Internal
Activities				
1. Establish and maintain criteria relating to type, significance and criticality of suppliers and supplier contracts, enabling a focus on preferred and important suppliers.				
2. Establish and maintain supplier and contract evaluation criteria to enable overall review and comparison of supplier performance in a consistent way.				
3. Identify, record and categorise existing suppliers and contracts according to defined criteria to maintain a detailed register of preferred suppliers that need to be managed carefully.				
4. Periodically evaluate and compare the performance of existing and alternative suppliers to identify opportunities or a compelling need to reconsider current supplier contracts.				
Management Practice	**Inputs**		**Outputs**	
APO10.02 Select suppliers. Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimised with input from potential suppliers.	**From**	**Description**	**Description**	**To**
	BAI02.02	High-level acquisition/ development plan	Supplier requests for information (RFIs) and requests for proposals (RFPs)	BAI02.01 BAI02.02
			RFI and RFP evaluations	BAI02.02
			Decision results of supplier evaluations	EDM04.01 BAI02.02
Activities				
1. Review all RFIs and RFPs to ensure that they: • Clearly define requirements • Include a procedure to clarify requirements • Allow vendors sufficient time to prepare their proposals • Clearly define award criteria and the decision process				
2. Evaluate RFIs and RFPs in accordance with the approved evaluation process/criteria, and maintain documentary evidence of the evaluations. Verify the references of candidate vendors.				
3. Select the supplier that best fits the RFP. Document and communicate the decision, and sign the contract.				
4. In the specific case of software acquisition, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include ownership and licencing of intellectual property, maintenance, warranties, arbitration procedures, upgrade terms, and fit for purpose, including security, escrow and access rights.				
5. In the specific case of acquisition of development resources, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include ownership and licencing of intellectual property; fit for purpose, including development methodologies; testing; quality management processes, including required performance criteria; performance reviews; basis for payment; warranties; arbitration procedures; human resource management; and compliance with the enterprise's policies.				
6. Obtain legal advice on resource development acquisition agreements regarding ownership and licencing of intellectual property.				
7. In the specific case of acquisition of infrastructure, facilities and related services, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include service levels, maintenance procedures, access controls, security, performance review, basis for payment and arbitration procedures.				

Personal Copy of: Dr. David Lanter

APO10 Process Practices, Inputs/Outputs and Activities *(cont.)*

Management Practice	Inputs		Outputs	
APO10.03 Manage supplier relationships and contracts. Formalise and manage the supplier relationship for each supplier. Manage, maintain and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal and regulatory requirements. Deal with contractual disputes.	**From**	**Description**	**Description**	**To**
	BAI03.04	Approved acquisition plans	Supplier roles and responsibilities	Internal
			Communication and review process	Internal
			Results and suggested improvements	Internal
Activities				
1. Assign relationship owners for all suppliers and make them accountable for the quality of service(s) provided.				
2. Specify a formal communication and review process, including supplier interactions and schedules.				
3. Agree on, manage, maintain and renew formal contracts with the supplier. Ensure that contracts conform to enterprise standards and legal and regulatory requirements.				
4. Within contracts with key service suppliers include provisions for the review of supplier site and internal practices and controls by management or independent third parties.				
5. Evaluate the effectiveness of the relationship and identify necessary improvements.				
6. Define, communicate and agree on ways to implement required improvements to the relationship.				
7. Use established procedures to deal with contract disputes, first using, wherever possible, effective relationships and communications to overcome service problems.				
8. Define and formalise roles and responsibilities for each service supplier. Where several suppliers combine to provide a service, consider allocating a lead contractor role to one of the suppliers to take responsibility for an overall contract.				
Management Practice	**Inputs**		**Outputs**	
APO10.04 Manage supplier risk. Identify and manage risk relating to suppliers' ability to continually provide secure, efficient and effective service delivery.	**From**	**Description**	**Description**	**To**
	APO12.04	• Results of third-party risk assessments • Risk analysis and risk profile reports for stakeholders	Identified supplier delivery risk	APO12.01 APO12.03 BAI01.01
			Identified contract requirements to minimise risk	Internal
Activities				
1. Identify, monitor and, where appropriate, manage risk relating to the supplier's ability to deliver service efficiently, effectively, securely, reliably and continually.				
2. When defining the contract, provide for potential service risk by clearly defining service requirements, including software escrow agreements, alternative suppliers or standby agreements to mitigate possible supplier failure; security and protection of intellectual property (IP); and any legal or regulatory requirements.				
Management Practice	**Inputs**		**Outputs**	
APO10.05 Monitor supplier performance and compliance. Periodically review the overall performance of suppliers, compliance to contract requirements, and value for money, and address identified issues.	**From**	**Description**	**Description**	**To**
			Supplier compliance monitoring criteria	Internal
			Supplier compliance monitoring review results	MEA01.03
Activities				
1. Define and document criteria to monitor supplier performance aligned with service level agreements and ensure that the supplier regularly and transparently reports on agreed-on criteria.				
2. Monitor and review service delivery to ensure that the supplier is providing an acceptable quality of service, meeting requirements and adhering to contract conditions.				
3. Review supplier performance and value for money to ensure that they are reliable and competitive, compared with alternative suppliers and market conditions.				
4. Request independent reviews of supplier internal practices and controls, if necessary.				
5. Record and assess review results periodically and discuss them with the supplier to identify needs and opportunities for improvement.				
6. Monitor and evaluate externally available information about the supplier.				

Personal Copy of: Dr. David Lanter

AP010 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	7.3 Supplier management
ITIL V3 2011	Service Design, 4.8 Supplier Management
Project Management Body of Knowledge (PMBOK)	PMBOK's procurement processes

Personal Copy of: Dr. David Lanter

APO11 Manage Quality	Area: Management Domain: Align, Plan and Organise
Process Description Define and communicate quality requirements in all processes, procedures and the related enterprise outcomes, including controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts.	
Process Purpose Statement Ensure consistent delivery of solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
05 Realised benefits from IT-enabled investments and services portfolio	• Percent of IT-enabled investments where benefit realisation is monitored through the full economic life cycle • Percent of IT services where expected benefits are realised • Percent of IT-enabled investments where claimed benefits are met or exceeded
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	• Number of programmes/projects on time and within budget • Percent of stakeholders satisfied with programme/project quality • Number of programmes needing significant rework due to quality defects • Cost of application maintenance vs. overall IT cost
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Stakeholders are satisfied with the quality of solutions and services.	• Average stakeholder satisfaction rating with solutions and services • Percent of stakeholders satisfied with IT quality • Number of services with a formal quality management plan
2. Project and service delivery results are predictable.	• Percent of projects reviewed that meet target quality goals and objectives • Percent of solutions and services delivered with formal certification • Number of defects uncovered prior to production
3. Quality requirements are implemented in all processes.	• Number of processes with a defined quality requirement • Number of processes with a formal quality assessment report • Number of SLAs that include quality acceptance criteria

Personal Copy of: Dr. David Lanter

APO11 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO11.01 Establish a quality management system (QMS).		C		A	C	I	C	I	I				C			C	C	R	C	C	I	R	R	I	I	I
APO11.02 Define and manage quality standards, practices and procedures.		C			C	R	C		R				C			C	C	A	R	R	R	R	R	R	R	R
APO11.03 Focus quality management on customers.					A	R	C		I							C	C	R	I	I	I	I	R	I	I	
APO11.04 Perform quality monitoring, control and reviews.			C		C	R	C	R	C		R					C	C	A	C	C	C	C	R	C	C	C
APO11.05 Integrate quality management into solutions for development and service delivery.					C	C					I							A	C	R	R		R			
APO11.06 Maintain continuous improvement.					C	R	C		R							C	C	A	R	R	R	R	R	R	R	

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

APO11 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
APO11.01 Establish a quality management system (QMS). Establish and maintain a QMS that provides a standard, formal and continuous approach to quality management for information, enabling technology and business processes that are aligned with business requirements and enterprise quality management.	**From**	**Description**	**Description**	**To**
	Outside COBIT	Enterprisewide quality system	QMS roles, responsibilities and decision rights	APO01.02 DSS06.03
			Quality management plans	BAI01.09
			Results of QMS effectiveness reviews	BAI03.06
Activities				
1. Ensure that the IT control framework and the business and IT processes include a standard, formal and continuous approach to quality management that is aligned with enterprise requirements. Within the IT control framework and the business and IT processes, identify quality requirements and criteria (e.g., based on legal requirements and requirements from customers).				
2. Define roles, tasks, decision rights and responsibilities for quality management in the organisational structure.				
3. Define quality management plans for important processes, projects or objectives in alignment with enterprise quality management criteria and policies. Record quality data.				
4. Monitor and measure the effectiveness and acceptance of quality management, and improve them when needed.				
5. Align IT quality management with an enterprisewide quality system to encourage a standardised and continuous approach to quality.				
6. Obtain input from management and external and internal stakeholders on the definition of quality requirements and quality management criteria.				
7. Effectively communicate the approach (e.g., through regular, formal quality training programmes).				
8. Regularly review the continued relevance, efficiency and effectiveness of specific quality management processes. Monitor the achievement of quality objectives.				

Personal Copy of: Dr. David Lanter

APO11 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO11.02 Define and manage quality standards, practices and procedures. Identify and maintain requirements, standards, procedures and practices for key processes to guide the enterprise in meeting the intent of the agreed-on QMS. This should be in line with the IT control framework requirements. Consider certification for key processes, organisational units, products or services.	**From**	**Description**	**Description**	**To**
	BAI02.04	Approved quality reviews	Quality management standards	All APO All BAI All DSS All MEA
	Outside COBIT	• Industry good practices • Available quality certifications		
Activities				
1. Define the quality management standards, practices and procedures in line with the IT control framework's requirements. Use industry good practices for reference when improving and tailoring the enterprise's quality practices.				
2. Consider the benefits and costs of quality certifications.				
Management Practice	**Inputs**		**Outputs**	
APO11.03 Focus quality management on customers. Focus quality management on customers by determining their requirements and ensuring alignment with the quality management practices.	**From**	**Description**	**Description**	**To**
	Outside COBIT	Business and customer quality requirements	Customer requirements for quality management	APO08.05 APO09.03 BAI01.09
			Acceptance criteria	BAI02.01 BAI02.02
			Review results of quality of service, including customer feedback	APO08.05 APO09.05 BAI05.01 BAI07.07
Activities				
1. Focus quality management on customers by determining internal and external customer requirements and ensuring alignment of the IT standards and practices. Define and communicate roles and responsibilities concerning conflict resolution between the user/customer and the IT organisation.				
2. Manage the business needs and expectations for each business process, IT operational service and new solutions, and maintain their quality acceptance criteria. Capture quality acceptance criteria for inclusion in SLAs.				
3. Communicate customer requirements and expectations throughout the business and IT organisation.				
4. Periodically obtain customer views on business process and service provisioning and IT solution delivery, to determine the impact on IT standards and practices and to ensure that customer expectations are met and are acted upon.				
5. Regularly monitor and review the QMS against agreed-on acceptance criteria. Include feedback from customers, users and management. Respond to discrepancies in review results to continuously improve the QMS.				
6. Capture quality acceptance criteria for inclusion in SLAs.				

Personal Copy of: Dr. David Lanter

APO11 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO11.04 Perform quality monitoring, control and reviews. Monitor the quality of processes and services on an ongoing basis as defined by the QMS. Define, plan and implement measurements to monitor customer satisfaction with quality as well as the value the QMS provides. The information gathered should be used by the process owner to improve quality.	**From**	**Description**	**Description**	**To**
	BAI03.06	• Quality review results, exceptions and corrections • Quality assurance plan	Results of quality reviews and audits	APO08.05 APO09.04 APO09.05 BAI07.08
	DSS02.07	• Request fulfilment status and trends report • Incident status and trends report	Process quality of service goals and metrics	All APO All BAI All DSS All MEA
Activities				
1. Monitor the quality of processes and services on an ongoing and systematic basis by describing, measuring, analysing, improving/engineering and controlling the processes.				
2. Prepare and conduct quality reviews.				
3. Report the review results and initiate improvements where appropriate.				
4. Monitor quality of processes, as well as the value quality provides. Ensure that measurement, monitoring and recording of information is used by the process owner to take appropriate corrective and preventive actions.				
5. Monitor goal-driven quality metrics aligned to overall quality objectives covering the quality of individual projects and services.				
6. Ensure that management and process owners regularly review quality management performance against defined quality metrics.				
7. Analyse overall quality management performance results.				
Management Practice	**Inputs**		**Outputs**	
APO11.05 Integrate quality management into solutions for development and service delivery. Incorporate relevant quality management practices into the definition, monitoring, reporting and ongoing management of solutions development and service offerings.	**From**	**Description**	**Description**	**To**
			Results of solution and service delivery quality monitoring	APO08.05 APO09.04 BAI07.08
			Root causes of quality delivery failures	APO08.02 APO09.04 BAI07.08 MEA02.04 MEA02.07 MEA02.08
Activities				
1. Integrate quality management practices in solutions development processes and practices.				
2. Continuously monitor service levels and incorporate quality management practices in the service delivery processes and practices.				
3. Identify and document root causes for non-conformance, and communicate findings to IT management and other stakeholders in a timely manner to enable remedial action to be taken. Where appropriate, perform follow-up reviews.				

Personal Copy of: Dr. David Lanter

APO11 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
APO11.06 Maintain continuous improvement. Maintain and regularly communicate an overall quality plan that promotes continuous improvement. This should include the need for, and benefits of, continuous improvement. Collect and analyse data about the QMS, and improve its effectiveness. Correct non-conformities to prevent recurrence. Promote a culture of quality and continual improvement.			Communications on continual improvement and good practices	All APO All BAI All DSS All MEA
			Examples of good practice to be shared	All APO All BAI All DSS All MEA
			Quality review benchmark results	All APO All BAI All DSS All MEA
Activities				
1. Maintain and regularly communicate the need for, and benefits of, continuous improvement.				
2. Establish a platform to share good practices and to capture information on defects and mistakes to enable learning from them.				
3. Identify recurring examples of quality defects, determine their root cause, evaluate their impact and result, and agree on improvement actions with the service and project delivery teams.				
4. Identify examples of excellent quality delivery processes that can benefit other services or projects, and share these with the service and project delivery teams to encourage improvement.				
5. Promote a culture of quality and continual improvement.				
6. Establish a feedback loop between quality management and problem management.				
7. Provide employees with training in the methods and tools of continual improvement.				
8. Benchmark the results of the quality reviews against internal historical data, industry guidelines, standards and data from similar types of enterprises.				

APO11 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 9001:2008	

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

APO12 Manage Risk	Area: Management Domain: Align, Plan and Organise
Process Description Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.	
Process Purpose Statement Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines
13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	• Number of programmes/projects on time and within budget • Percent of stakeholders satisfied with programme/project quality • Number of programmes needing significant rework due to quality defects • Cost of application maintenance vs. overall IT cost
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. IT-related risk is identified, analysed, managed and reported.	• Degree of visibility and recognition in the current environment • Number of loss events with key characteristics captured in repositories • Percent of audits, events and trends captured in repositories
2. A current and complete risk profile exists.	• Percent of key business processes included in the risk profile • Completeness of attributes and values in the risk profile
3. All significant risk management actions are managed and under control.	• Percent of risk management proposals rejected due to lack of consideration of other related risk • Number of significant incidents not identified and included in the risk management portfolio
4. Risk management actions are implemented effectively.	• Percent of IT risk action plans executed as designed • Number of measures not reducing residual risk

Personal Copy of: Dr. David Lanter

AP012 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP012.01 Collect data.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
AP012.02 Analyse risk.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
AP012.03 Maintain a risk profile.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
AP012.04 Articulate risk.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
AP012.05 Define a risk management action portfolio.		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
AP012.06 Respond to risk.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

AP012 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
	From	Description	Description	To
AP012.01 Collect data. Identify and collect relevant data to enable effective IT-related risk identification, analysis and reporting.	EDM03.01	Evaluation of risk management activities	Data on the operating environment relating to risk	Internal
	EDM03.02	• Approved process for measuring risk management • Key objectives to be monitored for risk management • Risk management policies	Data on risk events and contributing factors	Internal
	AP002.02	Gaps and risk related to current capabilities	Emerging risk issues and factors	EDM03.01 AP001.03 AP002.02
	AP002.05	Risk assessment initiatives		
	AP010.04	Identified supplier delivery risk		
	DSS02.07	Incident status and trends report		

Personal Copy of: Dr. David Lanter

AP012 Process Practices, Inputs/Outputs and Activities *(cont.)*

AP012.01 Activities

1. Establish and maintain a method for the collection, classification and analysis of IT risk-related data, accommodating multiple types of events, multiple categories of IT risk and multiple risk factors.
2. Record relevant data on the enterprise's internal and external operating environment that could play a significant role in the management of IT risk.
3. Survey and analyse the historical IT risk data and loss experience from externally available data and trends, industry peers through industry-based event logs, databases, and industry agreements for common event disclosure.
4. Record data on risk events that have caused or may cause impacts to IT benefit/value enablement, IT programme and project delivery, and/or IT operations and service delivery. Capture relevant data from related issues, incidents, problems and investigations.
5. For similar classes of events, organise the collected data and highlight contributing factors. Determine common contributing factors across multiple events.
6. Determine the specific conditions that existed or were absent when risk events occurred and the way the conditions affected event frequency and loss magnitude.
7. Perform periodic event and risk factor analysis to identify new or emerging risk issues and to gain an understanding of the associated internal and external risk factors.

Management Practice	Inputs		Outputs	
	From	Description	Description	To
AP012.02 Analyse risk. Develop useful information to support risk decisions that take into account the business relevance of risk factors.	DSS04.02	Business impact analyses	Scope of risk analysis efforts	Internal
	DSS05.01	Evaluations of potential threats	IT risk scenarios	Internal
	Outside COBIT	Threat advisories	Risk analysis results	EDM03.03 AP001.03 AP002.02 BAI01.10

Activities

1. Define the appropriate breadth and depth of risk analysis efforts, considering all risk factors and the business criticality of assets. Set the risk analysis scope after performing a cost-benefit analysis.
2. Build and regularly update IT risk scenarios, including compound scenarios of cascading and/or coincidental threat types, and develop expectations for specific control activities, capabilities to detect and other response measures.
3. Estimate the frequency and magnitude of loss or gain associated with IT risk scenarios. Take into account all applicable risk factors, evaluate known operational controls and estimate residual risk levels.
4 Compare residual risk to acceptable risk tolerance and identify exposures that may require a risk response.
5. Analyse cost-benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Propose the optimal risk response.
6. Specify high-level requirements for projects or programmes that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.
7. Validate the risk analysis results before using them in decision making, confirming that the analysis aligns with enterprise requirements and verifying that estimations were properly calibrated and scrutinised for bias.

Personal Copy of: Dr. David Lanter

AP012 Process Practices, Inputs/Outputs and Activities *(cont.)*

Management Practice	Inputs		Outputs	
AP012.03 Maintain a risk profile. Maintain an inventory of known risk and risk attributes (including expected frequency, potential impact and responses) and of related resources, capabilities and current control activities.	**From**	**Description**	**Description**	**To**
	EDM03.01	• Approved risk tolerance levels • Risk appetite guidance	Documented risk scenarios by line of business and function	Internal
	AP010.04	Identified supplier delivery risk	Aggregated risk profile, including status of risk management actions	EDM03.02 AP002.02
	DSS05.01	Evaluations of potential threats		

Activities

1. Inventory business processes, including supporting personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers and outsourcers, and document the dependency on IT service management processes and IT infrastructure resources.
2. Determine and agree on which IT services and IT infrastructure resources are essential to sustain the operation of business processes. Analyse dependencies and identify weak links.
3. Aggregate current risk scenarios by category, business line and functional area.
4. On a regular basis, capture all risk profile information and consolidate it into an aggregated risk profile.
5. Based on all risk profile data, define a set of risk indicators that allow the quick identification and monitoring of current risk and risk trends.
6. Capture information on IT risk events that have materialised, for inclusion in the IT risk profile of the enterprise.
7. Capture information on the status of the risk action plan, for inclusion in the IT risk profile of the enterprise.

Management Practice	Inputs		Outputs	
AP012.04 Articulate risk. Provide information on the current state of IT-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.	**From**	**Description**	**Description**	**To**
			Risk analysis and risk profile reports for stakeholders	EDM03.03 EDM05.02 AP010.04 MEA02.08
			Results of third-party risk assessments	EDM03.03 AP010.04 MEA02.01
			Opportunities for acceptance of greater risk	EDM03.03

Activities

1. Report the results of risk analysis to all affected stakeholders in terms and formats useful to support enterprise decisions. Wherever possible, include probabilities and ranges of loss or gain along with confidence levels that enable management to balance risk-return.
2. Provide decision makers with an understanding of worst-case and most-probable scenarios, due diligence exposures, and significant reputation, legal or regulatory considerations.
3. Report the current risk profile to all stakeholders, including effectiveness of the risk management process, control effectiveness, gaps, inconsistencies, redundancies, remediation status, and their impacts on the risk profile.
4. Review the results of objective third-party assessments, internal audit and quality assurance reviews, and map them to the risk profile. Review identified gaps and exposures to determine the need for additional risk analysis.
5. On a periodic basis, for areas with relative risk and risk capacity parity, identify IT-related opportunities that would allow the acceptance of greater risk and enhanced growth and return.

Management Practice	Inputs		Outputs	
AP012.05 Define a risk management action portfolio. Manage opportunities to reduce risk to an acceptable level as a portfolio.	**From**	**Description**	**Description**	**To**
			Project proposals for reducing risk	AP002.02 AP013.02

Activities

1. Maintain an inventory of control activities that are in place to manage risk and that enable risk to be taken in line with risk appetite and tolerance. Classify control activities and map them to specific IT risk statements and aggregations of IT risk.
2. Determine whether each organisational entity monitors risk and accepts accountability for operating within its individual and portfolio tolerance levels.
3. Define a balanced set of project proposals designed to reduce risk and/or projects that enable strategic enterprise opportunities, considering cost/benefits, effect on current risk profile and regulations.

Personal Copy of: Dr. David Lanter

APO12 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO12.06 Respond to risk. Respond in a timely manner with effective measures to limit the magnitude of loss from IT-related events.	**From**	**Description**	**Description**	**To**
	EDM03.03	Remedial actions to address risk management deviations	Risk-related incident response plans	DSS02.05
			Risk impact communications	APO01.04 APO08.04 DSS04.02
			Risk-related root causes	DSS02.03 DSS03.01 DSS03.02 DSS04.02 MEA02.04 MEA02.07 MEA02.08
Activities				
1. Prepare, maintain and test plans that document the specific steps to take when a risk event may cause a significant operational or development incident with serious business impact. Ensure that plans include pathways of escalation across the enterprise.				
2. Categorise incidents, and compare actual exposures against risk tolerance thresholds. Communicate business impacts to decision makers as part of reporting, and update the risk profile.				
3. Apply the appropriate response plan to minimise the impact when risk incidents occur.				
4. Examine past adverse events/losses and missed opportunities and determine root causes. Communicate root cause, additional risk response requirements and process improvements to appropriate decision makers and ensure that the cause, response requirements and process improvement are included in risk governance processes.				

APO12 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 27001:2005	Information security management systems—Requirements, Section 4
ISO/IEC 27002:2011	
ISO/IEC 31000	6. Processes for Managing Risk

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

APO13 Manage Security	Area: Management Domain: Align, Plan and Organise
Process Description Define, operate and monitor a system for information security management.	
Process Purpose Statement Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines
14 Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. A system is in place that considers and effectively addresses enterprise information security requirements.	• Number of key security roles clearly defined • Number of security related incidents
2. A security plan has been established, accepted and communicated throughout the enterprise.	• Level of stakeholder satisfaction with the security plan throughout the enterprise • Number of security solutions deviating from the plan • Number of security solutions deviating from the enterprise architecture
3. Information security solutions are implemented and operated consistently throughout the enterprise.	• Number of services with confirmed alignment to the security plan • Number of security incidents caused by non-adherence to the security plan • Number of solutions developed with confirmed alignment to the security plan

Personal Copy of: Dr. David Lanter

AP013 RACI Chart																										
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP013.01 Establish and maintain an ISMS.		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
AP013.02 Define and manage an information security risk treatment plan.		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
AP013.03 Monitor and review the ISMS.					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

AP013 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
AP013.01 Establish and maintain an information security management system (ISMS). Establish and maintain an ISMS that provides a standard, formal and continuous approach to security management for information, enabling secure technology and business processes that are aligned with business requirements and enterprise security management.	Outside COBIT	Enterprise security approach	ISMS policy	Internal
			ISMS scope statement	AP001.02 DSS06.03
Activities				
1. Define the scope and boundaries of the ISMS in terms of the characteristics of the enterprise, the organisation, its location, assets and technology. Include details of, and justification for, any exclusions from the scope.				
2. Define an ISMS in accordance with enterprise policy and aligned with the enterprise, the organisation, its location, assets and technology.				
3. Align the ISMS with the overall enterprise approach to the management of security.				
4. Obtain management authorisation to implement and operate or change the ISMS.				
5. Prepare and maintain a statement of applicability that describes the scope of the ISMS.				
6. Define and communicate Information security management roles and responsibilities.				
7. Communicate the ISMS approach.				

Personal Copy of: Dr. David Lanter

APO13 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO13.02 Define and manage an information security risk treatment plan. Maintain an information security plan that describes how information security risk is to be managed and aligned with the enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases and implemented as an integral part of services and solutions development, then operated as an integral part of business operation.	**From**	**Description**	**Description**	**To**
	APO02.04	Gaps and changes required to realise target capability	Information security risk treatment plan	All EDM All APO All BAI All DSS All MEA
	APO03.02	Baseline domain descriptions and architecture definition	Information security business cases	APO02.05
	APO12.05	Project proposals for reducing risk		
Activities				
1. Formulate and maintain an information security risk treatment plan aligned with strategic objectives and the enterprise architecture. Ensure that the plan identifies the appropriate and optimal management practices and security solutions, with associated resources, responsibilities and priorities for managing identified information security risk.				
2. Maintain as part of the enterprise architecture an inventory of solution components that are in place to manage security-related risk.				
3. Develop proposals to implement the information security risk treatment plan, supported by suitable business cases, which include consideration of funding and allocation of roles and responsibilities.				
4. Provide input to the design and development of management practices and solutions selected from the information security risk treatment plan.				
5. Define how to measure the effectiveness of the selected management practices and specify how these measurements are to be used to assess effectiveness to produce comparable and reproducible results.				
6. Recommend information security training and awareness programmes.				
7. Integrate the planning, design, implementation and monitoring of information security procedures and other controls capable of enabling prompt prevention, detection of security events and response to security incidents.				
Management Practice	**Inputs**		**Outputs**	
APO13.03 Monitor and review the ISMS. Maintain and regularly communicate the need for, and benefits of, continuous information security improvement. Collect and analyse data about the ISMS, and improve the effectiveness of the ISMS. Correct non-conformities to prevent recurrence. Promote a culture of security and continual improvement.	**From**	**Description**	**Description**	**To**
	DSS02.02	Classified and prioritised incidents and service requests	ISMS audit reports	MEA02.01
			Recommendations for improving the ISMS	Internal
Activities				
1. Undertake regular reviews of the effectiveness of the ISMS including meeting ISMS policy and objectives, and review of security practices. Take into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties.				
2. Conduct internal ISMS audits at planned intervals.				
3. Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified.				
4. Provide input to the maintenance of the security plans to take into account the findings of monitoring and reviewing activities.				
5. Record actions and events that could have an impact on the effectiveness or performance of the ISMS.				

APO13 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 27001:2005	Information security management systems—Requirements, Section 4
ISO/IEC 27002:2011	
National Institute of Standards and Technology (NIST) SP800-53 Rev 1	Recommended Security Controls for USA Federal Information Systems
ITIL V3 2011	Service Design, 4.7 Information Security Management

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

Build, Acquire and Implement (BAI)

01 Manage programmes and projects.

02 Manage requirements definition.

03 Manage solutions identification and build.

04 Manage availability and capacity.

05 Manage organisational change enablement.

06 Manage changes.

07 Manage change acceptance and transitioning.

08 Manage knowledge.

09 Manage assets.

10 Manage configuration.

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

BAI01 Manage Programmes and Projects	Area: Management Domain: Build, Acquire and Implement
Process Description Manage all programmes and projects from the investment portfolio in alignment with enterprise strategy and in a co-ordinated way. Initiate, plan, control, and execute programmes and projects, and close with a post-implementation review.	
Process Purpose Statement Realise business benefits and reduce the risk of unexpected delays, costs and value erosion by improving communications to and involvement of business and end users, ensuring the value and quality of project deliverables and maximising their contribution to the investment and services portfolio.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
05 Realised benefits from IT-enabled investments and services portfolio	• Percent of IT-enabled investments where benefit realisation is monitored through the full economic life cycle • Percent of IT services where expected benefits are realised • Percent of IT-enabled investments where claimed benefits are met or exceeded
13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	• Number of programmes/projects on time and within budget • Percent of stakeholders satisfied with programme/project quality • Number of programmes needing significant rework due to quality defects • Cost of application maintenance vs. overall IT cost
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Relevant stakeholders are engaged in the programmes and projects.	• Percent of stakeholders effectively engaged • Level of stakeholder satisfaction with involvement
2. The scope and outcomes of programmes and projects are viable and aligned with objectives.	• Percent of stakeholders approving enterprise need, scope, planned outcome and level of project risk • Percent of projects undertaken without approved business cases
3. Programme and project plans are likely to achieve the expected outcomes.	• Percent of activities aligned to scope and expected outcomes • Percent of active programmes undertaken without valid and updated programme value maps
4. The programme and project activities are executed according to the plans.	• Frequency of status reviews • Percent of deviations from plan addressed • Percent of stakeholder sign-offs for stage-gate reviews of active programmes
5. There are sufficient programme and project resources to perform activities according to the plans.	• Number of resource issues (e.g., skills, capacity)
6. The programme and project expected benefits are achieved and accepted.	• Percent of expected benefits achieved • Percent of outcomes with first-time acceptance • Level of stakeholder satisfaction expressed at project closure review

Personal Copy of: Dr. David Lanter

BAI01 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI01.01 Maintain a standard approach for programme and project management.	I	A	C	C	R		R		C		C					C	C	R								
BAI01.02 Initiate a programme.	I	R	C	C	A	R	R	R	R									C	C	C	C		C	C	C	C
BAI01.03 Manage stakeholder engagement.		A	C	R	R	R	C	R	I	I								R	C	C	C		C	C	C	C
BAI01.04 Develop and maintain the programme plan.			C	C	A	C		R	R	R	C					C	C	C	C	C	C		C	C	C	C
BAI01.05 Launch and execute the programme.			C	C	A	R		R	R	I	C					C	C	R	R	R	R		C	C	C	C
BAI01.06 Monitor, control and report on the programme outcomes.					A	C	I	R	R	R	C					C	R	R		C	C			C		
BAI01.07 Start up and initiate projects within a programme.					R	R	I	A	R									C	C	R	C		C	C	C	C
BAI01.08 Plan projects.						C	I	A	R									C	C	C	C	C	C	C	C	C
BAI01.09 Manage programme and project quality.					R	R	I	A	R		C					C	C	C	C	R	C		C	C	C	C
BAI01.10 Manage programme and project risk.					R	R	I	A	R		C					C	C	C	C	R	C		C	C	C	C
BAI01.11 Monitor and control projects.					I	R	I	A	R		C					C	R	C	C	R	C		C	C	C	C
BAI01.12 Manage project resources and work packages.						R	I	A	R		C					C	C	C	C	R	C		C	C	C	C
BAI01.13 Close a project or iteration.					C	C	I	A	R		C					C	C	C	C	C	C		C	C	C	C
BAI01.14 Close a programme.	I	C	C	C	A	R	I	R	R	R								R	C	C	C		C	C	C	C

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

BAI01 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
BAI01.01 Maintain a standard approach for programme and project management. Maintain a standard approach for programme and project management that enables governance and management review and decision making and delivery management activities focussed on achieving value and goals (requirements, risk, costs, schedule, quality) for the business in a consistent manner.	**From**	**Description**	**Description**	**To**
	EDM02.02	Requirements for stage-gate reviews	Updated programme and project management approaches	Internal
	EDM02.03	Actions to improve value delivery		
	AP003.04	• Architecture governance requirements • Implementation phase descriptions		
	AP005.05	Updated portfolios of programmes, services and assets		
	AP010.04	Identified supplier delivery risk		
Activities				
1. Maintain and enforce a standard approach to programme and project management aligned to the enterprise's specific environment and with good practice based on defined process and use of appropriate technology. Ensure that the approach covers the full life cycle and disciplines to be followed, including the management of scope, resources, risk, cost, quality, time, communication, stakeholder involvement, procurement, change control, integration and benefit realisation.				
2. Update the programme and project management approach based on lessons learned from its use.				
Management Practice	**Inputs**		**Outputs**	
BAI01.02 Initiate a programme. Initiate a programme to confirm the expected benefits and obtain authorisation to proceed. This includes agreeing on programme sponsorship, confirming the programme mandate through approval of the conceptual business case, appointing programme board or committee members, producing the programme brief, reviewing and updating the business case, developing a benefits realisation plan, and obtaining approval from sponsors to proceed.	**From**	**Description**	**Description**	**To**
	AP003.04	• Implementation phase descriptions • Resource requirements	Programme concept business case	AP005.03
	AP005.03	Programme business case	Programme mandate and brief	AP005.03
	AP007.03	Skills and competencies matrix	Programme benefit realisation plan	AP005.03 AP006.05
	BAI05.02	Common vision and goals		
Activities				
1. Agree on programme sponsorship and appoint a programme board/committee with members who have strategic interest in the programme, have responsibility for the investment decision making, will be significantly impacted by the programme and will be required to enable delivery of the change.				
2. Confirm the programme mandate with sponsors and stakeholders. Articulate the strategic objectives for the programme, potential strategies for delivery, improvement and benefits that are expected to result, and how the programme fits with other initiatives.				
3. Develop a detailed business case for a programme, if warranted. Involve all key stakeholders to develop and document a complete understanding of the expected enterprise outcomes, how they will be measured, the full scope of initiatives required, the risk involved and the impact on all aspects of the enterprise. Identify and assess alternative courses of action to achieve the desired enterprise outcomes.				
4. Develop a benefits realisation plan that will be managed throughout the programme to ensure that planned benefits always have owners and are achieved, sustained and optimised.				
5. Prepare and submit for in-principle approval the initial (conceptual) programme business case, providing essential decision-making information regarding purpose, contribution to business objectives, expected value created, time frames, etc.				
6. Appoint a dedicated manager for the programme, with the commensurate competencies and skills to manage the programme effectively and efficiently.				

Personal Copy of: Dr. David Lanter

BAI01 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI01.03 Manage stakeholder engagement. Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information that reaches all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	**From**	**Description**	**Description**	**To**
			Stakeholder engagement plan	Internal
			Results of stakeholder engagement effectiveness assessments	Internal
Activities				
1. Plan how stakeholders inside and outside the enterprise will be identified, analysed, engaged and managed through the life cycle of the projects.				
2. Identify, engage and manage stakeholders by establishing and maintaining appropriate levels of co-ordination, communication and liaison to ensure that they are involved in the programme/project.				
3. Measure the effectiveness of stakeholder engagement and take remedial actions as required.				
4. Analyse stakeholder interests and requirements.				
Management Practice	**Inputs**		**Outputs**	
BAI01.04 Develop and maintain the programme plan. Formulate a programme to lay the initial groundwork and to position it for successful execution by formalising the scope of the work to be accomplished and identifying the deliverables that will satisfy its goals and deliver value. Maintain and update the programme plan and business case throughout the full economic life cycle of the programme, ensuring alignment with strategic objectives and reflecting the current status and updated insights gained to date.	**From**	**Description**	**Description**	**To**
	APO05.03	Selected programmes with return on investment (ROI) milestones	Programme plan	Internal
	APO07.03	Skills and competencies matrix	Programme budget and benefits register	APO05.06 APO06.05
	APO07.05	Inventory of business and IT human resources	Resource requirements and roles	APO07.05 APO07.06
	BAI05.02	Implementation team and roles		
	BAI05.03	Vision communication plan		
	BAI05.04	Identified quick wins		
	BAI07.03	Approved acceptance test plan		
	BAI07.05	Approved acceptance and release for production		
Activities				
1. Define and document the programme plan covering all projects, including what is needed to bring about changes to the enterprise; its image, products and services; business processes; people skills and numbers; relationships with stakeholders, customers, suppliers and others; technology needs; and organisational restructuring required to achieve the programme's expected enterprise outcomes.				
2. Specify required resources and skills to execute the project, including project managers and project teams as well as business resources. Specify funding, cost, schedule and inter-dependencies of multiple projects. Specify the basis for acquiring and assigning competent staff members and/or contractors to the projects. Define the roles and responsibilities for all team members and other interested parties.				
3. Assign accountability clearly and unambiguously for each project, including achieving the benefits, controlling the costs, managing the risk and co-ordinating the project activities.				
4. Ensure that there is effective communication of programme plans and progress reports amongst all projects and with the overall programme. Ensure that any changes made to individual plans are reflected in the other enterprise programme plans.				
5. Maintain the programme plan to ensure that it is up to date and reflects alignment with current strategic objectives, actual progress and material changes to outcomes, benefits, costs and risk. Have the business drive the objectives and prioritise the work throughout to ensure that the programme as designed will meet enterprise requirements. Review progress of individual projects and adjust the projects as necessary to meet scheduled milestones releases.				
6. Update and maintain throughout the programme's economic life the business case and a benefits register to identify and define key benefits arising from undertaking the programme.				
7. Prepare a programme budget that reflects the full economic life cycle costs and the associated financial and non-financial benefits.				

Personal Copy of: Dr. David Lanter

BAI01 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI01.05 Launch and execute the programme. Launch and execute the programme to acquire and direct the resources needed to accomplish the goals and benefits of the programme as defined in the programme plan. In accordance with stage-gate or release review criteria, prepare for stage-gate, iteration or release reviews to report on the progress of the programme and to be able to make the case for funding up to the following stage-gate or release review.	**From**	**Description**	**Description**	**To**
	BAI05.03	Vision communications	Results of benefit realisation monitoring	APO05.06 APO06.05
			Results of programme goal achievement monitoring	APO02.04
			Programme audit plans	MEA02.06
Activities				
1. Plan, resource and commission the necessary projects required to achieve the programme results, based on funding review and approvals at each stage-gate review.				
2. Establish agreed-on stages of the development process (development checkpoints). At the end of each stage, facilitate formal discussions of approved criteria with the stakeholders. After successful completion of functionality, performance and quality reviews, and before finalising stage activities, obtain formal approval and sign-off from all stakeholders and the sponsor/business process owner.				
3. Undertake a benefits realisation process throughout the programme to ensure that planned benefits always have owners and are likely to be achieved, sustained and optimised. Monitor benefits delivery and report against performance targets at the stage-gate or iteration and release reviews. Perform root cause analysis for deviations from the plan and identify and address any necessary remedial actions.				
4. Manage each programme or project to ensure that decision making and delivery activities are focussed on value by achieving benefits for the business and goals in a consistent manner, addressing risk and achieving stakeholder requirements.				
5. Set up programme/project management office(s) and plan audits, quality reviews, phase/stage-gate reviews and reviews of realised benefits.				
Management Practice	**Inputs**		**Outputs**	
BAI01.06 Monitor, control and report on the programme outcomes. Monitor and control programme (solution delivery) and enterprise (value/outcome) performance against plan throughout the full economic life cycle of the investment. Report this performance to the programme steering committee and the sponsors.	**From**	**Description**	**Description**	**To**
	EDM02.03	Feedback on portfolio and programme performance	Results of programme performance reviews	MEA01.03
	APO05.02	Investment return expectations	Stage-gate review results	EDM02.01 APO02.04 APO05.04
	APO05.03	Business case assessments		
	APO05.04	Investment portfolio performance reports		
	APO05.06	• Corrective actions to improve benefit realisation • Benefit results and related communications		
	APO07.05	• Resource utilisation records • Resourcing shortfall analyses		
	BAI05.04	Communication of benefits		
	BAI06.03	Change request status reports		
	BAI07.05	Evaluation of acceptance results		

Personal Copy of: Dr. David Lanter

BAI01 Process Practices, Inputs/Outputs and Activities *(cont.)*

BAI01.06 Activities

1. Monitor and control the performance of the overall programme and the projects within the programme, including contributions of the business and IT to the projects, and report in a timely, complete and accurate fashion. Reporting may include schedule, funding, functionality, user satisfaction, internal controls and acceptance of accountabilities.
2. Monitor and control performance against enterprise and IT strategies and goals, and report to management on enterprise changes implemented, benefits realised against the benefits realisation plan, and the adequacy of the benefits realisation process.
3. Monitor and control IT services, assets and resources created or changed as a result of the programme. Note implementation and in-service dates. Report to management on performance levels, sustained service delivery and contribution to value.
4. Manage programme performance against key criteria (e.g., scope, schedule, quality, benefits realisation, costs, risk, velocity), identify deviations from the plan and take timely remedial action when required.
5. Monitor individual project performance related to delivery of the expected capabilities, schedule, benefits realisation, costs, risk or other metrics to identify potential impacts on programme performance. Take timely remedial action when required.
6. Update operational IT portfolios reflecting changes that result from the programme in the relevant IT service, asset or resource portfolios.
7. In accordance with stage-gate, release or iteration review criteria, undertake reviews to report on the progress of the programme so that management can make go/no-go or adjustment decisions and approve further funding up to the following stage-gate, release or iteration.

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI01.07 Start up and initiate projects within a programme. Define and document the nature and scope of the project to confirm and develop amongst stakeholders a common understanding of project scope and how it relates to other projects within the overall IT-enabled investment programme. The definition should be formally approved by the programme and project sponsors.			Project scope statements	Internal
			Project definitions	Internal

Activities

1. To create a common understanding of project scope amongst stakeholders, provide to the stakeholders a clear written statement defining the nature, scope and benefit of every project.
2. Ensure that each project has one or more sponsors with sufficient authority to manage execution of the project within the overall programme.
3. Ensure that key stakeholders and sponsors within the enterprise and IT agree on and accept the requirements for the project, including definition of project success (acceptance) criteria and key performance indicators (KPIs).
4. Ensure that the project definition describes the requirements for a project communication plan that identifies internal and external project communications.
5. With the approval of stakeholders, maintain the project definition throughout the project, reflecting changing requirements.
6. To track the execution of a project, put in place mechanisms such as regular reporting and stage-gate, release or phase reviews in a timely manner with appropriate approval.

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI01.08 Plan projects. Establish and maintain a formal, approved integrated project plan (covering business and IT resources) to guide project execution and control throughout the life of the project. The scope of projects should be clearly defined and tied to building or enhancing business capability.	BAI07.03	Approved acceptance test plan	Project plans	Internal
			Project baseline	Internal
			Project reports and communications	Internal

Activities

1. Develop a project plan that provides information to enable management to control project progress progressively. The plan should include details of project deliverables and acceptance criteria, required internal and external resources and responsibilities, clear work breakdown structures and work packages, estimates of resources required, milestones/release plan/phases, key dependencies, and identification of a critical path.
2. Maintain the project plan and any dependent plans (e.g., risk plan, quality plan, benefits realisation plan) to ensure that they are up to date and reflect actual progress and approved material changes.
3. Ensure that there is effective communication of project plans and progress reports amongst all projects and with the overall programme. Ensure that any changes made to individual plans are reflected in the other plans.
4. Determine the activities, interdependencies and required collaboration and communication among multiple projects within a programme.
5. Ensure that each milestone is accompanied by a significant deliverable requiring review and sign-off.
6. Establish a project baseline (e.g., cost, schedule, scope, quality) that is appropriately reviewed, approved and incorporated into the integrated project plan.

Personal Copy of: Dr. David Lanter

BAI01 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI01.09 Manage programme and project quality. Prepare and execute a quality management plan, processes and practices, aligned with the QMS that describes the programme and project quality approach and how it will be implemented. The plan should be formally reviewed and agreed on by all parties concerned and then incorporated into the integrated programme and project plans.	**From**	**Description**	**Description**	**To**
	AP011.01	Quality management plans	Quality management plan	BAI02.04 BAI03.06 BAI07.01
	AP011.03	Customer requirements for quality management	Requirements for independent verification of deliverables	BAI07.03
Activities				
1. Identify assurance tasks and practices required to support the accreditation of new or modified systems during programme and project planning, and include them in the integrated plans. Ensure that the tasks provide assurance that internal controls and security solutions meet the defined requirements.				
2. To provide quality assurance for the project deliverables, identify ownership and responsibilities, quality review processes, success criteria and performance metrics.				
3. Define any requirements for independent validation and verification of the quality of deliverables in the plan.				
4. Perform quality assurance and control activities in accordance with the quality management plan and QMS.				
Management Practice	**Inputs**		**Outputs**	
BAI01.10 Manage programme and project risk. Eliminate or minimise specific risk associated with programmes and projects through a systematic process of planning, identifying, analysing, responding to, and monitoring and controlling the areas or events that have the potential to cause unwanted change. Risk faced by programme and project management should be established and centrally recorded.	**From**	**Description**	**Description**	**To**
	AP012.02	Risk analysis results	Project risk management plan	Internal
	BAI02.03	• Risk mitigation actions • Requirements risk register	Project risk assessment results	Internal
	Outside COBIT	ERM framework	Project risk register	Internal
Activities				
1. Establish a formal project risk management approach aligned with the ERM framework. Ensure that the approach includes identifying, analysing, responding to, mitigating, monitoring and controlling risk.				
2. Assign to appropriately skilled personnel the responsibility for executing the enterprise's project risk management process within a project and ensuring that this is incorporated into the solution development practices. Consider allocating this role to an independent team, especially if an objective viewpoint is required or a project is considered critical.				
3. Perform the project risk assessment of identifying and quantifying risk continuously throughout the project. Manage and communicate risk appropriately within the project governance structure.				
4. Reassess project risk periodically, including at initiation of each major project phase and as part of major change request assessments.				
5. Identify owners for actions to avoid, accept or mitigate risk.				
6. Maintain and review a project risk register of all potential project risk, and a risk mitigation log of all project issues and their resolution. Analyse the log periodically for trends and recurring problems to ensure that root causes are corrected.				

Personal Copy of: Dr. David Lanter

BAI01 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI01.11 Monitor and control projects. Measure project performance against key project performance criteria such as schedule, quality, cost and risk. Identify any deviations from the expected. Assess the impact of deviations on the project and overall programme, and report results to key stakeholders.	**From**	**Description**	**Description**	**To**
			Project performance criteria	Internal
			Project progress reports	Internal
			Agreed-on changes to project	Internal
Activities				
1. Establish and use a set of project criteria including, but not limited to, scope, schedule, quality, cost and level of risk.				
2. Measure project performance against key project performance criteria. Analyse deviations from established key project performance criteria for cause, and assess positive and negative effects on the programme and its component projects.				
3. Report to identified key stakeholders project progress within the programme, deviations from established key project performance criteria, and potential positive and negative effects on the programme and its component projects.				
4. Monitor changes to the programme and review existing key project performance criteria to determine whether they still represent valid measures of progress.				
5. Document and submit any necessary changes to the programme's key stakeholders for their approval before adoption. Communicate revised criteria to project managers for use in future performance reports.				
6. Recommend and monitor remedial action, when required, in line with the programme and project governance framework.				
7. Gain approval and sign-off on the deliverables produced in each iteration, release or project phase from designated managers and users in the affected business and IT functions.				
8. Base the approval process on clearly defined acceptance criteria agreed on by key stakeholders prior to work commencing on the project phase or iteration deliverable.				
9. Assess the project at agreed-on major stage-gates, releases or iterations and make formal go/no-go decisions based on predetermined critical success criteria.				
10. Establish and operate a change control system for the project so that all changes to the project baseline (e.g., cost, schedule, scope, quality) are appropriately reviewed, approved and incorporated into the integrated project plan in line with the programme and project governance framework.				
Management Practice	**Inputs**		**Outputs**	
BAI01.12 Manage project resources and work packages. Manage project work packages by placing formal requirements on authorising and accepting work packages, and assigning and co-ordinating appropriate business and IT resources.	**From**	**Description**	**Description**	**To**
			Project resource requirements	APO07.05 APO07.06
			Project roles and responsibilities	Internal
			Gaps in project planning	Internal
Activities				
1. Identify business and IT resource needs for the project and clearly map appropriate roles and responsibilities, with escalation and decision-making authorities agreed on and understood.				
2. Identify required skills and time requirements for all individuals involved in the project phases in relation to defined roles. Staff the roles based on available skills information (e.g., IT skills matrix).				
3. Utilise experienced project management and team leader resources with skills appropriate to the size, complexity and risk of the project.				
4. Consider and clearly define the roles and responsibilities of other involved parties, including finance, legal, procurement, HR, internal audit and compliance.				
5. Clearly define and agree on the responsibility for procurement and management of third-party products and services, and manage the relationships.				
6. Identify and authorise the execution of the work according to the project plan.				
7. Identify project plan gaps and provide feedback to the project manager to remediate.				

Personal Copy of: Dr. David Lanter

BAI01 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI01.13 Close a project or iteration. At the end of each project, release or iteration, require the project stakeholders to ascertain whether the project, release or iteration delivered the planned results and value. Identify and communicate any outstanding activities required to achieve the planned results of the project and the benefits of the programme, and identify and document lessons learned for use on future projects, releases, iterations and programmes.	**From**	**Description**	**Description**	**To**
	BAI07.08	• Remedial action plan • Post-implementation review report	Post-implementation review results	APO02.04
			Project lessons learned	Internal
			Stakeholder project acceptance confirmations	Internal
Activities				
1. Define and apply key steps for project closure, including post-implementation reviews that assess whether a project attained desired results and benefits.				
2. Plan and execute post-implementation reviews to determine whether projects delivered expected benefits and to improve the project management and system development process methodology.				
3. Identify, assign, communicate and track any uncompleted activities required to achieve planned programme project results and benefits.				
4. Regularly, and upon completion of the project, collect from the project participants the lessons learned. Review them and key activities that led to delivered benefits and value. Analyse the data and make recommendations for improving the current project as well as project management method for future projects.				
5. Obtain stakeholder acceptance of project deliverables and transfer ownership.				
Management Practice	**Inputs**		**Outputs**	
BAI01.14 Close a programme. Remove the programme from the active investment portfolio when there is agreement that the desired value has been achieved or when it is clear it will not be achieved within the value criteria set for the programme.	**From**	**Description**	**Description**	**To**
	BAI07.08	• Remedial action plan • Post-implementation review report	Communication of programme retirement and ongoing accountabilities	APO05.05 APO07.06
Activities				
1. Bring the programme to an orderly closure, including formal approval, disbanding of the programme organisation and supporting function, validation of deliverables, and communication of retirement.				
2. Review and document lessons learned. Once the programme is retired, remove it from the active investment portfolio.				
3. Put accountability and processes in place to ensure that the enterprise continues to optimise value from the service, asset or resources. Additional investments may be required at some future time to ensure that this occurs.				

BAI01 Related Guidance	
Related Standard	**Detailed Reference**
PMBOK	
PRINCE2	

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

BAI02 Manage Requirements Definition	Area: Management Domain: Build, Acquire and Implement
Process Description Identify solutions and analyse requirements before acquisition or creation to ensure that they are in line with enterprise strategic requirements covering business processes, applications, information/data, infrastructure and services. Co-ordinate with affected stakeholders the review of feasible options including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.	
Process Purpose Statement Create feasible optimal solutions that meet enterprise needs while minimising risk.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
12 Enablement and support of business processes by integrating applications and technology into business processes	• Number of business processing incidents caused by technology integration errors • Number of business process changes that need to be delayed or reworked because of technology integration issues • Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues • Number of applications or critical infrastructures operating in silos and not integrated
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Business functional and technical requirements reflect enterprise needs and expectations.	• Percent of requirements reworked due to misalignment with enterprise needs and expectations • Level of stakeholder satisfaction with requirements
2. The proposed solution satisfies business functional, technical and compliance requirements.	• Percent of requirements satisfied by proposed solution
3. Risk associated with the requirements has been addressed in the proposed solution.	• Number of incidents not identified as risk • Percent of risk unsuccessfully mitigated
4. Requirements and proposed solutions meet business case objectives (value expected and likely costs).	• Percent of business case objectives met by proposed solution • Percent of stakeholders not approving solution in relation to business case

Personal Copy of: Dr. David Lanter

BAI02 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI02.01 Define and maintain business functional and technical requirements.					I	R		A	R		C					C	C	C	R	R	C		C	C	C	C
BAI02.02 Perform a feasibility study and formulate alternative solutions.					R	R		A	R							C	C	C	C	R	C		C	C	C	C
BAI02.03 Manage requirements risk.					R	R		A	R		R					C	C	R	C	R	R		C	C	C	C
BAI02.04 Obtain approval of requirements and solutions.					R	R		A	R							C	C	C	C	C	C		C	C	C	C

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

BAI02 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI02.01 Define and maintain business functional and technical requirements. Based on the business case, identify, prioritise, specify and agree on business information, functional, technical and control requirements covering the scope/understanding of all initiatives required to achieve the expected outcomes of the proposed IT-enabled business solution.	AP001.06	• Data integrity procedures • Data security and control guidelines • Data classification guidelines	Requirements definition repository	BAI03.01 BAI03.02 BAI04.01 BAI05.01
	AP003.01	Architecture principles	Confirmed acceptance criteria from stakeholders	BAI03.01 BAI03.02 BAI04.03 BAI05.01 BAI05.02
	AP003.02	• Information architecture model • Baseline domain descriptions and architecture definition	Record of requirement change requests	BAI03.09
	AP003.05	Solution development guidance		
	AP010.02	Supplier RFIs and RFPs		
	AP011.03	Acceptance criteria		

Personal Copy of: Dr. David Lanter

BAI02 Process Practices, Inputs/Outputs and Activities *(cont.)*

BAI02.01 Activities

1. Define and implement a requirements definition and maintenance procedure and a requirements repository that are appropriate for the size, complexity, objectives and risk of the initiative that the enterprise is considering undertaking.
2. Express business requirements in terms of how the gap between current and desired business capabilities needs to be addressed and how a role will interact with and use the solution.
3. Throughout the project, elicit, analyse and confirm that all stakeholder requirements, including relevant acceptance criteria, are considered, captured, prioritised and recorded in a way that is understandable to the stakeholders, business sponsors and technical implementation personnel, recognising that the requirements may change and will become more detailed as they are implemented.
4. Specify and prioritise the information, functional and technical requirements based on the confirmed stakeholder requirements. Include information control requirements in the business processes, automated processes and IT environments to address information risk and to comply with laws, regulations and commercial contracts.
5. Validate all requirements through approaches such as peer review, model validation or operational prototyping.
6. Confirm acceptance of key aspects of the requirements, including enterprise rules, information controls, business continuity, legal and regulatory compliance, auditability, ergonomics, operability and usability, safety, and supporting documentation.
7. Track and control scope, requirements and changes through the life cycle of the solution throughout the project as understanding of the solution evolves.
8. Consider requirements relating to enterprise policies and standards, enterprise architecture, strategic and tactical IT plans, in-house and outsourced business and IT processes, security requirements, regulatory requirements, people competencies, organisational structure, business case, and enabling technology.

Management Practice	Inputs		Outputs	
BAI02.02 Perform a feasibility study and formulate alternative solutions. Perform a feasibility study of potential alternative solutions, assess their viability and select the preferred option. If appropriate, implement the selected option as a pilot to determine possible improvements.	**From**	**Description**	**Description**	**To**
	AP003.05	Solution development guidance	Feasibility study report	BAI03.02 BAI03.03
	AP010.01	Supplier catalogue	High-level acquisition/ development plan	AP010.02 BAI03.01
	AP010.02	• Decision results of supplier evaluations • RFI and RFP evaluations • Supplier RFIs and RFPs		
	AP011.03	Acceptance criteria		

Activities

1. Define and execute a feasibility study, pilot or basic working solution that clearly and concisely describes the alternative solutions that will satisfy the business and functional requirements. Include an evaluation of their technological and economic feasibility.
2. Identify required actions for solution acquisition or development based on the enterprise architecture, and take into account scope and/or time and/or budget limitations.
3. Review the alternative solutions with all stakeholders and select the most appropriate one based on feasibility criteria, including risk and cost.
4. Translate the preferred course of action into a high-level acquisition/development plan identifying resources to be used and stages requiring a go/no-go decision.

Personal Copy of: Dr. David Lanter

BAI02 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI02.03 Manage requirements risk. Identify, document, prioritise and mitigate functional, technical and information processing-related risk associated with the enterprise requirements and proposed solution.	**From**	**Description**	**Description**	**To**
			Requirements risk register	BAI01.10 BAI03.02 BAI04.01 BAI05.01
			Risk mitigation actions	BAI01.10 BAI03.02 BAI05.01
Activities				
1. Involve the stakeholders to create a list of potential quality, functional, and technical requirements and risk related to information processing (due to, e.g., lack of user involvement, unrealistic expectations, developers adding unnecessary functionality).				
2. Analyse and prioritise the requirements risk according to probability and impact. If applicable, determine budget and schedule impacts.				
3. Identify ways to control, avoid or mitigate the requirements risk in order of priority.				
Management Practice	**Inputs**		**Outputs**	
BAI02.04 Obtain approval of requirements and solutions. Co-ordinate feedback from affected stakeholders and, at predetermined key stages, obtain business sponsor or product owner approval and sign-off on functional and technical requirements, feasibility studies, risk analyses and recommended solutions.	**From**	**Description**	**Description**	**To**
	BAI01.09	Quality management plan	Sponsor approvals of requirements and proposed solutions	BAI03.02 BAI03.03 BAI03.04
			Approved quality reviews	APO11.02
Activities				
1. Ensure that the business sponsor or product owner makes the final decision with respect to the choice of solution, acquisition approach and high-level design, according to the business case. Co-ordinate feedback from affected stakeholders and obtain sign-off from appropriate business and technical authorities (e.g., business process owner, enterprise architect, operations manager, security) for the proposed approach.				
2. Obtain quality reviews throughout, and at the end of, each key project stage, iteration or release to assess the results against the original acceptance criteria. Have business sponsors and other stakeholders sign off on each successful quality review.				

BAI02 Related Guidance	
Related Standard	**Detailed Reference**
ITIL V3 2011	Service Design, 4.1 Design Coordination

Personal Copy of: Dr. David Lanter

BAI03 Manage Solutions Identification and Build	Area: Management Domain: Build, Acquire and Implement
Process Description Establish and maintain identified solutions in line with enterprise requirements covering design, development, procurement/sourcing and partnering with suppliers/vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.	
Process Purpose Statement Establish timely and cost-effective solutions capable of supporting enterprise strategic and operational objectives.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. The solution design, including relevant components, meets enterprise needs, aligns with standards and addresses all identified risk.	• Number of reworked solution designs due to misalignment with requirements • Time taken to approve that design deliverable has met requirements
2. The solution conforms to the design, is in accordance with organisational standards, and has appropriate control, security and auditability.	• Number of solution exceptions to design noted during stage reviews
3. The solution is of acceptable quality and has been successfully tested.	• Number of errors found during testing • Time and effort to complete tests
4. Approved changes to requirements are correctly incorporated into the solution.	• Number of tracked approved changes that generate new errors
5. Maintenance activities successfully address business and technological needs.	• Number of demands for maintenance that go unsatisfied

Personal Copy of: Dr. David Lanter

BAI03 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI03.01 Design high-level solutions.						R		I	R							C	C	I	C	A	C		C	C	C	C
BAI03.02 Design detailed solution components.						R		I	R							C	C	I	C	A	C		C	C	C	C
BAI03.03 Develop solution components.						R		I	R							C	C	I	C	A	C		C	C	C	C
BAI03.04 Procure solution components.					I	R		I	I							C	C	A	I	R	R	R	C	C	C	C
BAI03.05 Build solutions.						R		I	R							C	C	I	C	A	C		C	C	C	C
BAI03.06 Perform quality assurance.					I	R		A	R							C	C	I	C	R	C		C	C	C	C
BAI03.07 Prepare for solution testing.						R		A	I							C	C	I		R	R		R	R	R	R
BAI03.08 Execute solution testing.						R		A	I							I	I	I		R	R		I	I	I	I
BAI03.09 Manage changes to requirements.					I	R		A	R							I	I	C	R	R	C		C	C	C	C
BAI03.10 Maintain solutions.						R			R							C	C	I	C	A	C		C	C	C	C
BAI03.11 Define IT services and maintain the service portfolio.					I	I			I							I	I	R	I	C	C	C	A	I	I	

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

BAI03 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
BAI03.01 Design high-level solutions. Develop and document high-level designs using agreed-on and appropriate phased or rapid agile development techniques. Ensure alignment with the IT strategy and enterprise architecture. Reassess and update the designs when significant issues occur during detailed design or building phases or as the solution evolves. Ensure that stakeholders actively participate in the design and approve each version.	APO03.01	Architecture principles	Approved high-level design specification	BAI04.03 BAI05.01
	APO03.02	Baseline domain descriptions and architecture definition		
	APO04.03	Research analyses of innovation possibilities		
	APO04.04	Evaluations of innovation ideas		
	BAI02.01	• Confirmed acceptance criteria from stakeholders • Requirements definition repository		
	BAI02.02	High-level acquisition/ development plan		
Activities				
1. Establish a high-level design specification that translates the proposed solution into business processes, supporting services, applications, infrastructure, and information repositories capable of meeting business and enterprise architecture requirements.				
2. Involve appropriately qualified and experienced users and IT specialists in the design process to make sure that the design provides a solution that optimally uses the proposed IT capabilities to enhance the business process.				
3. Create a design that is compliant with the organisation's design standards, at a level of detail that is appropriate for the solution and development method and consistent with business, enterprise and IT strategies, the enterprise architecture, security plan, and applicable laws, regulations and contracts.				
4. After quality assurance approval, submit the final high-level design to the project stakeholders and the sponsor/business process owner, for approval based on agreed-on criteria. This design will evolve throughout the project as understanding grows.				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
BAI03.02 Design detailed solution components. Develop, document and elaborate detailed designs progressively using agreed-on and appropriate phased or rapid agile development techniques, addressing all components (business processes and related automated and manual controls, supporting IT applications, infrastructure services and technology products, and partners/suppliers). Ensure that the detailed design includes internal and external SLAs and OLAs.	APO03.01	Architecture principles	Approved detailed design specification	BAI04.03 BAI05.01
	APO03.02	• Information architecture model • Baseline domain descriptions and architecture definition	SLA and OLA revisions	APO09.03 BAI04.02
	APO03.05	Solution development guidance		
	APO04.06	Assessments of using innovative approaches		
	BAI02.01	• Confirmed acceptance criteria from stakeholders • Requirements definition repository		
	BAI02.02	Feasibility study report		
	BAI02.03	• Risk mitigation actions • Requirements risk register		
	BAI02.04	Sponsor approvals of requirements and proposed solutions		

Personal Copy of: Dr. David Lanter

BAI03 Process Practices, Inputs/Outputs and Activities *(cont.)*

BAI03.02 Activities

1. Design progressively the business process activities and work flows that need to be performed in conjunction with the new application system to meet the enterprise objectives, including the design of the manual control activities.
2. Design the application processing steps, including specification of transaction types and business processing rules, automated controls, data definitions/business objects, use cases, external interfaces, design constraints, and other requirements (e.g., licencing, legal, standards and internationalisation/localisation).
3. Classify data inputs and outputs according to enterprise architecture standards. Specify the source data collection design, documenting the data inputs (regardless of source) and validation for processing transactions as well as the methods for validation. Design the identified outputs, including data sources.
4. Design system/solution interface, including any automated data exchange.
5. Design data storage, location, retrieval and recoverability.
6. Design appropriate redundancy, recovery and backup.
7. Design the interface between the user and the system application so that it is easy to use and self-documenting.
8. Consider the impact of the solution's need for infrastructure performance, being sensitive to the number of computing assets, bandwidth intensity and time sensitivity of the information.
9. Proactively evaluate for design weaknesses (e.g., inconsistencies, lack of clarity, potential flaws) throughout the life cycle, identifying improvements when required.
10. Provide an ability to audit transactions and identify root causes of processing errors.

Management Practice	Inputs		Outputs	
BAI03.03 Develop solution components. Develop solution components progressively in accordance with detailed designs following development methods and documentation standards, quality assurance (QA) requirements, and approval standards. Ensure that all control requirements in the business processes, supporting IT applications and infrastructure services, services and technology products, and partners/suppliers are addressed.	**From**	**Description**	**Description**	**To**
	BAI02.02	Feasibility study report	Documented solution components	BAI04.03 BAI05.05 BAI08.03 BAI08.04
	BAI02.04	Sponsor approvals of requirements and proposed solutions		

Activities

1. Develop business processes, supporting services, applications and infrastructure, and information repositories based on agreed-on specifications and business, functional and technical requirements.
2. When third-party providers are involved with the solution development, ensure that maintenance, support, development standards and licencing are addressed and adhered to in contractual obligations.
3. Track change requests and design, performance and quality reviews, ensuring active participation of all impacted stakeholders.
4. Document all solution components according to defined standards and maintain version control over all developed components and associated documentation.
5. Assess the impact of solution customisation and configuration on the performance and efficiency of acquired solutions and on inter-operability with existing applications, operating systems and other infrastructure. Adapt business processes as required to leverage the application capability.
6. Ensure that responsibilities for using high security or restricted access infrastructure components are clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.

Management Practice	Inputs		Outputs	
BAI03.04 Procure solution components. Procure solution components based on the acquisition plan in accordance with requirements and detailed designs, architecture principles and standards, and the enterprise's overall procurement and contract procedures, QA requirements, and approval standards. Ensure that all legal and contractual requirements are identified and addressed by the supplier.	**From**	**Description**	**Description**	**To**
	BAI02.04	Sponsor approvals of requirements and proposed solutions	Approved acquisition plan	APO10.03
			Updates to asset inventory	BAI09.01

Activities

1. Create and maintain a plan for the acquisition of solution components, considering future flexibility for capacity additions, transition costs, risk and upgrades over the lifetime of the project.
2. Review and approve all acquisition plans, considering risk, costs, benefits and technical conformance with enterprise architecture standards.
3. Assess and document the degree to which acquired solutions require adaptation of business process to leverage the benefits of the acquired solution.
4. Follow required approvals at key decision points during the procurement processes.
5. Record receipt of all infrastructure and software acquisitions in an asset inventory.

Personal Copy of: Dr. David Lanter

BAI03 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI03.05 Build solutions. Install and configure solutions and integrate with business process activities. Implement control, security and auditability measures during configuration, and during integration of hardware and infrastructural software, to protect resources and ensure availability and data integrity. Update the services catalogue to reflect the new solutions.	**From**	**Description**	**Description**	**To**
			Integrated and configured solution components	BAI06.01
Activities				
1. Integrate and configure business and IT solution components and information repositories in line with detailed specifications and quality requirements. Consider the role of users, business stakeholders and the process owner in the configuration of business processes.				
2. Complete and update business process and operational manuals, where necessary, to account for any customisation or special conditions unique to the implementation.				
3. Consider all relevant information control requirements in solution component integration and configuration, including implementation of business controls, where appropriate, into automated application controls such that processing is accurate, complete, timely, authorised and auditable.				
4. Implement audit trails during configuration and integration of hardware and infrastructural software to protect resources and ensure availability and integrity.				
5. Consider when the effect of cumulative customisations and configurations (including minor changes that were not subjected to formal design specifications) require a high-level reassessment of the solution and associated functionality.				
6. Ensure the interoperability of solution components with supporting tests, preferably automated.				
7. Configure acquired application software to meet business processing requirements.				
8. Define service catalogues for relevant internal and external target groups based on business requirements.				
Management Practice	**Inputs**		**Outputs**	
BAI03.06 Perform quality assurance (QA). Develop, resource and execute a QA plan aligned with the QMS to obtain the quality specified in the requirements definition and the enterprise's quality policies and procedures.	**From**	**Description**	**Description**	**To**
	APO11.01	Results of QMS effectiveness reviews	Quality assurance plan	APO11.04
	BAI01.09	Quality management plan	Quality review results, exceptions and corrections	APO11.04
Activities				
1. Define a QA plan and practices including, e.g., specification of quality criteria, validation and verification processes, definition of how quality will be reviewed, necessary qualifications of quality reviewers, and roles and responsibilities for the achievement of quality.				
2. Frequently monitor the solution quality based on project requirements, enterprise policies, adherence to development methodologies, quality management procedures and acceptance criteria.				
3. Employ code inspection, test-driven development practices, automated testing, continuous integration, walk-throughs and testing of applications as appropriate. Report on outcomes of the monitoring process and testing to the application software development team and IT management.				
4. Monitor all quality exceptions and address all corrective actions. Maintain a record of all reviews, results, exceptions and corrections. Repeat quality reviews, where appropriate, based on the amount of rework and corrective action.				
Management Practice	**Inputs**		**Outputs**	
BAI03.07 Prepare for solution testing. Establish a test plan and required environments to test the individual and integrated solution components, including the business processes and supporting services, applications and infrastructure.	**From**	**Description**	**Description**	**To**
			Test plan	BAI07.03
			Test procedures	BAI07.03
Activities				
1. Create an integrated test plan and practices commensurate with the enterprise environment and strategic technology plans that will enable the creation of suitable testing and simulation environments to help verify that the solution will operate successfully in the live environment and deliver the intended results and that controls are adequate.				
2. Create a test environment that supports the full scope of the solution and reflects, as closely as possible, real-world conditions, including the business processes and procedures, range of users, transaction types, and deployment conditions.				
3. Create test procedures that align with the plan and practices and allow evaluation of the operation of the solution in real-world conditions. Ensure that the test procedures evaluate the adequacy of the controls, based on enterprisewide standards that define roles, responsibilities and testing criteria, and are approved by project stakeholders and the sponsor/business process owner.				

Personal Copy of: Dr. David Lanter

BAI03 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI03.08 Execute solution testing. Execute testing continually during development, including control testing, in accordance with the defined test plan and development practices in the appropriate environment. Engage business process owners and end users in the test team. Identify, log and prioritise errors and issues identified during testing.	**From**	**Description**	**Description**	**To**
	APO04.05	Analysis of rejected initiatives	Test result logs and audit trails	BAI07.03
			Test result communications	BAI07.03
Activities				
1. Undertake testing of solutions and their components in accordance with the testing plan. Include testers independent from the solution team, with representative business process owners and end users. Ensure that testing is conducted only within the development and test environments.				
2. Use clearly defined test instructions, as defined in the test plan, and consider the appropriate balance between automated scripted tests and interactive user testing.				
3. Undertake all tests in accordance with the test plan and practices including the integration of business processes and IT solution components and of non-functional requirements (e.g., security, interoperability, usability).				
4. Identify, log and classify (e.g., minor, significant and mission-critical) errors during testing. Repeat tests until all significant errors have been resolved. Ensure that an audit trail of test results is maintained.				
5. Record testing outcomes and communicate results of testing to stakeholders in accordance with the test plan.				
Management Practice	**Inputs**		**Outputs**	
BAI03.09 Manage changes to requirements. Track the status of individual requirements (including all rejected requirements) throughout the project life cycle and manage the approval of changes to requirements.	**From**	**Description**	**Description**	**To**
	APO04.05	Results and recommendations from proof-of-concept initiatives	Record of all approved and applied change requests	BAI06.03
	BAI02.01	Record of requirement change requests		
Activities				
1. Assess the impact of all solution change requests on the solution development, the original business case and the budget, and categorise and prioritise them accordingly.				
2. Track changes to requirements, enabling all stakeholders to monitor, review and approve the changes. Ensure that the outcomes of the change process are fully understood and agreed on by all the stakeholders and the sponsor/business process owner.				
3. Apply change requests, maintaining the integrity of integration and configuration of solution components. Assess the impact of any major solution upgrade and classify it according to agreed-on objective criteria (such as enterprise requirements), based on the outcome of analysis of the risk involved (such as impact on existing systems and processes or security), cost-benefit justification and other requirements.				
Management Practice	**Inputs**		**Outputs**	
BAI03.10 Maintain solutions. Develop and execute a plan for the maintenance of solution and infrastructure components. Include periodic reviews against business needs and operational requirements.	**From**	**Description**	**Description**	**To**
			Maintenance plan	APO08.05
			Updated solution components and related documentation	BAI05.05
Activities				
1. Develop and execute a plan for the maintenance of solution components that includes periodic reviews against business needs and operational requirements such as patch management, upgrade strategies, risk, vulnerabilities assessment and security requirements.				
2. Assess the significance of a proposed maintenance activity on current solution design, functionality and/or business processes. Consider risk, user impact and resource availability. Ensure that the business process owners understand the effect of designating changes as maintenance.				
3. In the event of major changes to existing solutions that result in significant change in current designs and/or functionality and/or business processes, follow the development process used for new systems. For maintenance updates, use the change management process.				
4. Ensure that the pattern and volume of maintenance activities are analysed periodically for abnormal trends indicating underlying quality or performance problems, cost/benefit of major upgrade, or replacement in lieu of maintenance.				
5. For maintenance updates, use the change management process to control all maintenance requests.				

Personal Copy of: Dr. David Lanter

BAI03 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
BAI03.11 Define IT services and maintain the service portfolio. Define and agree on new or changed IT services and service level options. Document new or changed service definitions and service level options to be updated in the services portfolio.	EDM04.01	Guiding principles for allocation of resources and capabilities	Service definitions	APO05.01 DSS01.03
	APO02.04	• Value benefit statement for target environment • Gaps and changes required to realise target capability	Updated service portfolio	APO05.05
	APO06.02	Budget allocations		
	APO06.03	• Budget communications • IT budget and plan		
	APO08.05	Definition of potential improvement projects		
	BAI10.02	Configuration baseline		
	BAI10.03	Approved changes to baseline		
	BAI10.04	Configuration status reports		
Activities				
1. Propose definitions of the new or changed IT services to ensure that the services are fit for purpose. Document the proposed service definitions in the portfolio list of services to be developed.				
2. Propose new or changed service level options (service times, user satisfaction, availability, performance, capacity, security, continuity, compliance and usability) to ensure that the IT services are fit for use. Document the proposed service options in the portfolio.				
3. Interface with business relationship management and portfolio management to agree on the proposed service definitions and service level options.				
4. If service change falls within agreed-on approval authority, build the new or changed IT services or service level options. Otherwise, pass the service change to portfolio management for investment review.				

BAI03 Related Guidance	
Related Standard	**Detailed Reference**
None	

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

BAI04 Manage Availability and Capacity	Area: Management Domain: Build, Acquire and Implement
Process Description Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.	
Process Purpose Statement Maintain service availability, efficient management of resources, and optimisation of system performance through prediction of future performance and capacity requirements.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
14 Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. The availability plan anticipates the business expectation of critical capacity requirements.	• Number of unplanned capacity, performance or availability upgrades
2. Capacity, performance and availability meet requirements.	• Number of transaction peaks where target performance is exceeded • Number of availability incidents • Number of events where capacity has exceeded planned limits
3. Availability, performance and capacity issues are identified and routinely resolved.	• Number and percentage of unresolved availability, performance and capacity issues

Personal Copy of: Dr. David Lanter

BAI04 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI04.01 Assess current availability, performance and capacity and create a baseline.						I												C		C	A		R	C	C	
BAI04.02 Assess business impact.						A												C		C	R		R	C	C	
BAI04.03 Plan for new or changed service requirements.						R												C		C	A		R	C	C	
BAI04.04 Monitor and review availability and capacity.						R												C		C	A		R	C	C	
BAI04.05 Investigate and address availability, performance and capacity issues.					I	R												I	R	C	A		R	I	I	

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

BAI04 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
BAI04.01 Assess current availability, performance and capacity and create a baseline. Assess availability, performance and capacity of services and resources to ensure that cost-justifiable capacity and performance are available to support business needs and deliver against SLAs. Create availability, performance and capacity baselines for future comparison.	**From**	**Description**	**Description**	**To**
	BAI02.01	Requirements definition repository	Availability, performance and capacity baselines	Internal
	BAI02.03	Requirements risk register	Evaluations against SLAs	AP009.05
Activities				
1. Consider the following (current and forecasted) in the assessment of availability, performance and capacity of services and resources: customer requirements, business priorities, business objectives, budget impact, resource utilisation, IT capabilities and industry trends.				
2. Monitor actual performance and capacity usage against defined thresholds, supported where necessary with automated software.				
3. Identify and follow up on all incidents caused by inadequate performance or capacity.				
4. Regularly evaluate the current levels of performance for all processing levels (business demand, service capacity and resource capacity) by comparing them against trends and SLAs, taking into account changes in the environment.				

Personal Copy of: Dr. David Lanter

BAI04 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI04.02 Assess business impact. Identify important services to the enterprise, map services and resources to business processes, and identify business dependencies. Ensure that the impact of unavailable resources is fully agreed on and accepted by the customer. Ensure that, for vital business functions, the SLA availability requirements can be satisfied.	**From**	**Description**	**Description**	**To**
	APO09.03	SLAs and OLAs	Availability, performance and capacity scenarios	Internal
	BAI03.02	SLA and OLA revisions	Availability, performance and capacity business impact assessments	Internal
Activities				
1. Identify only those solutions or services that are critical in the availability and capacity management process.				
2. Map the selected solutions or services to application(s) and infrastructure (IT and facility) on which they depend to enable a focus on critical resources for availability planning.				
3. Collect data on availability patterns from logs of past failures and performance monitoring. Use modelling tools that help predict failures based on past usage trends and management expectations of new environment or user conditions.				
4. Create scenarios based on the collected data, describing future availability situations to illustrate a variety of potential capacity levels needed to achieve the availability performance objective.				
5. Determine the likelihood that the availability performance objective will not be achieved based on the scenarios.				
6. Determine the impact of the scenarios on the business performance measures (e.g., revenue, profit, customer services). Engage the business line, functional (especially finance) and regional leaders to understand their evaluation of impact.				
7. Ensure that business process owners fully understand and agree to the results of this analysis. From the business owners, obtain a list of unacceptable risk scenarios that require a response to reduce risk to acceptable levels.				
Management Practice	**Inputs**		**Outputs**	
BAI04.03 Plan for new or changed service requirements. Plan and prioritise availability, performance and capacity implications of changing business needs and service requirements.	**From**	**Description**	**Description**	**To**
	BAI02.01	Confirmed acceptance criteria from stakeholders	Prioritised improvements	APO02.02
	BAI03.01	Approved high-level design specification	Performance and capacity plans	APO02.02
	BAI03.02	Approved detailed design specification		
	BAI03.03	Documented solution components		
Activities				
1. Review availability and capacity implications of service trend analysis.				
2. Identify availability and capacity implications of changing business needs and improvement opportunities. Use modelling techniques to validate availability, performance and capacity plans.				
3. Prioritise needed improvements and create cost-justifiable availability and capacity plans.				
4. Adjust the performance and capacity plans and SLAs based on realistic, new, proposed and/or projected business processes and supporting services, applications and infrastructure changes as well as reviews of actual performance and capacity usage, including workload levels.				
5. Ensure that management performs comparisons of actual demand on resources with forecasted supply and demand to evaluate current forecasting techniques and make improvements where possible.				

Personal Copy of: Dr. David Lanter

BAI04 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI04.04 Monitor and review availability and capacity. Monitor, measure, analyse, report and review availability, performance and capacity. Identify deviations from established baselines. Review trend analysis reports identifying any significant issues and variances, initiating actions where necessary, and ensuring that all outstanding issues are followed up.	**From**	**Description**	**Description**	**To**
			Availability, performance and capacity reports	MEA01.03
Activities				
1. Establish a process for gathering data to provide management with monitoring and reporting information for availability, performance and capacity workload of all information-related resources.				
2. Provide regular reporting of the results in an appropriate form for review by IT and business management and communication to enterprise management.				
3. Integrate monitoring and reporting activities in the iterative capacity management activities (monitoring, analysis, tuning and implementations).				
4. Provide capacity reports to the budgeting processes.				
Management Practice	**Inputs**		**Outputs**	
BAI04.05 Investigate and address availability, performance and capacity issues. Address deviations by investigating and resolving identified availability, performance and capacity issues.	**From**	**Description**	**Description**	**To**
			Performance and capacity gaps	Internal
			Corrective actions	APO02.02
			Emergency escalation procedure	DSS02.02
Activities				
1. Obtain guidance from vendor product manuals to ensure an appropriate level of performance availability for peak processing and workloads.				
2. Identify performance and capacity gaps based on monitoring current and forecasted performance. Use the known availability, continuity and recovery specifications to classify resources and allow prioritisation.				
3. Define corrective actions (e.g., shifting workload, prioritising tasks or adding resources, when performance and capacity issues are identified).				
4. Integrate required corrective actions into the appropriate planning and change management processes.				
5. Define an escalation procedure for swift resolution in case of emergency capacity and performance problems.				

BAI04 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	6.3 Service continuity and availability management
ITIL V3 2011	• Service Design, 4.4 Availability Management • Service Design, 4.5 Capacity Management

Personal Copy of: Dr. David Lanter

BAI05 Manage Organisational Change Enablement	Area: Management Domain: Build, Acquire and Implement
Process Description Maximise the likelihood of successfully implementing sustainable enterprisewide organisational change quickly and with reduced risk, covering the complete life cycle of the change and all affected stakeholders in the business and IT.	
Process Purpose Statement Prepare and commit stakeholders for business change and reduce the risk of failure.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
08 Adequate use of applications, information and technology solutions	• Percent of business process owners satisfied with supporting IT products and services • Level of business user understanding of how technology solutions support their processes • Satisfaction level of business users with training and user manuals • NPV showing business satisfaction level of the quality and usefulness of the technology solutions
13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	• Number of programmes/projects on time and within budget • Percent of stakeholders satisfied with programme/project quality • Number of programmes needing significant rework due to quality defects • Cost of application maintenance vs. overall IT cost
17 Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of IT innovation possibilities • Level of stakeholder satisfaction with levels of IT innovation expertise and ideas • Number of approved initiatives resulting from innovative IT ideas
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Stakeholder desire for the change has been understood.	• Level of stakeholder desire for the change • Level of senior management involvement
2. Implementation team is competent and able to drive the change.	• Satisfaction ratings of implementation team by affected stakeholders • Number of identified skills or capacity issues
3. Desired change is understood and accepted by stakeholders.	• Stakeholder feedback on level of understanding • Number of queries received
4. Role players are empowered to deliver the change.	• Percent of role players with appropriately assigned authority • Role player feedback on level of empowerment
5. Role players are enabled to operate, use and maintain the change.	• Percent of role players trained • Role player self-assessment of relevant capabilities • Level of satisfaction of role players operating, using and maintaining the change
6. The change is embedded and sustained.	• Percent of users appropriately trained for the change • Level of satisfaction of users with adoption of the change

Personal Copy of: Dr. David Lanter

BAI05 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI05.01 Establish the desire to change.	R	A	C	C	R	C	R	R			C				R	C	C	R	C	C	C	C	C	C		
BAI05.02 Form an effective implementation team.		I	I	C	A	C	C	R	R						C	C	C	R		R	C	C	C	C	C	C
BAI05.03 Communicate desired vision.		A	C	C	R	I	R	I	I				I		I	I	I	R	I	I	I	I	I	I	I	I
BAI05.04 Empower role players and identify short-term wins.				R	A	C	C	R	C						R	C	C	R	C	C	C		C	C	C	C
BAI05.05 Enable operation and use.				C	A	R			R									R	C	R	R		R	R	R	R
BAI05.06 Embed new approaches.		R	R	R	A	R			R									R	C	R	R		R	R	R	R
BAI05.07 Sustain changes.	R	R	R	R	A	R			R									R	C	R	R		R	R	R	R

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

BAI05 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI05.01 Establish the desire to change. Understand the scope and impact of the envisioned change and stakeholder readiness/willingness to change. Identify actions to motivate stakeholders to accept and want to make the change work successfully.	APO11.03	Results of quality of service, including customer feedback	Communications of drivers for change	Internal
	BAI02.01	• Confirmed acceptance criteria from stakeholders • Requirements definition repository	Communications from executive management committing to change	Internal
	BAI02.03	• Risk mitigation actions • Requirements risk register		
	BAI03.01	Approved high-level design specification		
	BAI03.02	Approved detailed design specification		

Activities

1. Assess the scope and impact of the envisioned change, the various stakeholders who are affected, the nature of the impact on and involvement required from each stakeholder group, and the current readiness and ability to adopt the change.
2. Identify, leverage and communicate current pain points, negative events, risk, customer dissatisfaction and business problems, as well as initial benefits, future opportunities and rewards, and competitor advantages, as a foundation for establishing the desire to change.
3. Issue key communications from the executive committee or CEO to demonstrate the commitment to the change.
4. Provide visible leadership from senior management to establish direction and to align, motivate and inspire stakeholders to desire the change.

Personal Copy of: Dr. David Lanter

BAI05 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI05.02 Form an effective implementation team. Establish an effective implementation team by assembling appropriate members, creating trust, and establishing common goals and effectiveness measures.	**From**	**Description**	**Description**	**To**
	BAI02.01	Confirmed acceptance criteria from stakeholders	Implementation team and roles	BAI01.04
			Common vision and goals	BAI01.02
Activities				
1. Identify and assemble an effective core implementation team that includes appropriate members from business and IT with the capacity to spend the required amount of time and contribute knowledge and expertise, experience, credibility and authority. Consider including external parties such as consultants to provide an independent view or to address skill gaps. Identify potential change agents within different parts of the enterprise with whom the core team can work to support the vision and cascade changes down.				
2. Create trust within the core implementation team through carefully planned events with effective communication and joint activities.				
3. Develop a common vision and goals that support the enterprise objectives.				
Management Practice	**Inputs**		**Outputs**	
BAI05.03 Communicate desired vision. Communicate the desired vision for the change in the language of those affected by it. The communication should be made by senior management and include the rationale for, and benefits of, the change, the impacts of not making the change; and the vision, the road map and the involvement required of the various stakeholders.	**From**	**Description**	**Description**	**To**
			Vision communication plan	BAI01.04
			Vision communications	BAI01.05
Activities				
1. Develop a vision communication plan to address the core audience groups, their behavioural profiles and information requirements, communication channels, and principles.				
2. Deliver the communication at appropriate levels of the enterprise in accordance with the plan.				
3. Reinforce the communication through multiple forums and repetition.				
4. Check understanding of the desired vision and respond to any issues highlighted by staff.				
5. Make all levels of leadership accountable for demonstrating the vision.				
Management Practice	**Inputs**		**Outputs**	
BAI05.04 Empower role players and identify short-term wins. Empower those with implementation roles by ensuring that accountabilities are assigned, providing training, and aligning organisational structures and HR processes. Identify and communicate short-term wins that can be realised and are important from a change enablement perspective.	**From**	**Description**	**Description**	**To**
	Outside COBIT	Enterprise organisational structure	Aligned HR performance objectives	APO07.04
			Identified quick wins	BAI01.04
			Communications of benefits	BAI01.06
Activities				
1. Identify organisational structures compatible with the vision; if required, make changes to ensure alignment.				
2. Plan the training staff needs to develop the appropriate skills and attitudes to feel empowered.				
3. Align HR processes and measurement systems (e.g., performance evaluation, compensation decisions, promoting decisions, recruiting and hiring) to support the vision.				
4. Identify and manage leaders who continue to resist needed change.				
5. Identify, prioritise and deliver opportunities for quick wins. These could be related to current known areas of difficulty or external factors that need to be addressed urgently.				
6. Leverage delivered quick wins by communicating the benefits to those impacted to show the vision is on track. Fine-tune the vision, keep leaders on board and build momentum.				

Personal Copy of: Dr. David Lanter

BAI05 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI05.05 Enable operation and use. Plan and implement all technical, operational and usage aspects such that all those who are involved in the future state environment can exercise their responsibility.	**From**	**Description**	**Description**	**To**
	BAI03.03	Documented solution components	Operation and use plan	APO08.04 BAI08.04 DSS01.01 DSS01.02 DSS06.02
	BAI03.10	Updated solution components and related documentation	Success measures and results	APO08.05 BAI07.07 BAI07.08 MEA01.03
Activities				
1. Develop a plan for operation and use of the change that communicates and builds on realised quick wins, addresses behavioural and cultural aspects of the broader transition, and increases buy-in and engagement. Ensure that the plan covers a holistic view of the change and provides documentation (e.g., procedures), mentoring, training, coaching, knowledge transfer, enhanced immediate post-go-live support and ongoing support.				
2. Implement the operation and use plan. Define and track success measures, including hard business measures and perception measures that indicate how people feel about a change, taking remedial action as necessary.				
Management Practice	**Inputs**		**Outputs**	
BAI05.06 Embed new approaches. Embed the new approaches by tracking implemented changes, assessing the effectiveness of the operation and use plan, and sustaining ongoing awareness through regular communication. Take corrective measures as appropriate, which may include enforcing compliance.	**From**	**Description**	**Description**	**To**
			Compliance audit results	MEA02.02 MEA03.03
			Awareness communications	Internal
			HR performance review results	APO07.04
Activities				
1. Celebrate successes and implement reward and recognition programmes to reinforce the change.				
2. Use performance measurement systems to identify root causes for low adoption and take corrective action.				
3. Make process owners accountable for normal day-to-day operations.				
4. Conduct compliance audits to identify root causes for low adoption and recommend corrective action.				
5. Provide ongoing awareness through regular communication of the change and its adoption.				
Management Practice	**Inputs**		**Outputs**	
BAI05.07 Sustain changes. Sustain changes through effective training of new staff, ongoing communication campaigns, continued top management commitment, adoption monitoring and sharing of lessons learned across the enterprise.	**From**	**Description**	**Description**	**To**
			Knowledge transfer plans	BAI08.03 BAI08.04
			Communications of management's commitment	Internal
			Reviews of operational use	MEA02.02
Activities				
1. Provide mentoring, training, coaching and knowledge transfer to new staff to sustain the change.				
2. Sustain and reinforce the change through regular communication demonstrating top management commitment.				
3. Perform periodic reviews of the operation and use of the change and identify improvements.				
4. Capture lessons learned relating to implementation of the change and share knowledge across the enterprise.				

BAI05 Related Guidance	
Related Standard	**Detailed Reference**
	Kotter, John; *Leading Change*, Harvard Business School Press, USA, 1996

Personal Copy of: Dr. David Lanter

BAI06 Manage Changes	Area: Management Domain: Build, Acquire and Implement
Process Description Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation.	
Process Purpose Statement Enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Authorised changes are made in a timely manner and with minimal errors.	• Amount of rework caused by failed changes • Reduced time and effort required to make changes • Number and age of backlogged change requests
2. Impact assessments reveal the effect of the change on all affected components.	• Percent of unsuccessful changes due to inadequate impact assessments
3. All emergency changes are reviewed and authorised after the change.	• Percent of total changes that are emergency fixes • Number of emergency changes not authorised after the change
4. Key stakeholders are kept informed of all aspects of the change.	• Stakeholder feedback ratings on satisfaction with communications

BAI06 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C		C					C	C	R	C	R	R	C	R	C		
BAI06.02 Manage emergency changes.					A	I					C					C	C	R	I	R	R		I	C		
BAI06.03 Track and report change status.					C	R			C									A		R	R		R			
BAI06.04 Close and document the changes.					A	R			R		C					C	C	R	C	R	R	I	I			

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

BAI06 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
BAI06.01 Evaluate, prioritise and authorise change requests. Evaluate all requests for change to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritised, categorised, assessed, authorised, planned and scheduled.	**From**	**Description**	**Description**	**To**
	BAI03.05	Integrated and configured solution components	Impact assessments	Internal
	DSS02.03	Approved service requests	Approved requests for change	BAI07.01
	DSS03.03	Proposed solutions to known errors		
	DSS03.05	Identified sustainable solutions	Change plan and schedule	BAI07.01
	DSS04.08	Approved changes to the plans		
	DSS06.01	Root cause analyses and recommendations		
Activities				
1. Use formal change requests to enable business process owners and IT to request changes to business process, infrastructure, systems or applications. Make sure that all such changes arise only through the change request management process.				
2. Categorise all requested changes (e.g., business process, infrastructure, operating systems, networks, application systems, purchased/packaged application software) and relate affected configuration items.				
3. Prioritise all requested changes based on the business and technical requirements, resources required, and the legal, regulatory and contractual reasons for the requested change.				
4. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies amongst changes. Involve business process owners in the assessment process, as appropriate.				
5. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes.				
6. Plan and schedule all approved changes.				
7. Consider the impact of contracted services providers (e.g., of outsourced business processing, infrastructure, application development and shared services) on the change management process, including integration of organisational change management processes with change management processes of service providers and the impact on contractual terms and SLAs.				
Management Practice	**Inputs**		**Outputs**	
BAI06.02 Manage emergency changes. Carefully manage emergency changes to minimise further incidents and make sure the change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorised after the change.	**From**	**Description**	**Description**	**To**
			Post-implementation review of emergency changes	Internal
Activities				
1. Ensure that a documented procedure exists to declare, assess, give preliminary approval, authorise after the change and record an emergency change.				
2. Verify that all emergency access arrangements for changes are appropriately authorised, documented and revoked after the change has been applied.				
3. Monitor all emergency changes, and conduct post-implementation reviews involving all concerned parties. The review should consider and initiate corrective actions based on root causes such as problems with business process, application system development and maintenance, development and test environments, documentation and manuals, and data integrity.				
4. Define what constitutes an emergency change.				

Personal Copy of: Dr. David Lanter

BAI06 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI06.03 Track and report change status. Maintain a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned.	**From**	**Description**	**Description**	**To**
	BAI03.09	Record of all approved and applied change requests	Change request status reports	BAI01.06 BAI10.03
Activities				
1. Categorise change requests in the tracking process (e.g., rejected, approved but not yet initiated, approved and in process, and closed).				
2. Implement change status reports with performance metrics to enable management review and monitoring of both the detailed status of changes and the overall state (e.g., aged analysis of change requests). Ensure that status reports form an audit trail so changes can subsequently be tracked from inception to eventual disposition.				
3. Monitor open changes to ensure that all approved changes are closed in a timely fashion, depending on priority.				
4. Maintain a tracking and reporting system for all change requests.				
Management Practice	**Inputs**		**Outputs**	
BAI06.04 Close and document the changes. Whenever changes are implemented, update accordingly the solution and user documentation and the procedures affected by the change.	**From**	**Description**	**Description**	**To**
			Change documentation	Internal
Activities				
1. Include changes to documentation (e.g., business and IT operational procedures, business continuity and disaster recovery documentation, configuration information, application documentation, help screens, and training materials) within the change management procedure as an integral part of the change.				
2. Define an appropriate retention period for change documentation and pre- and post-change system and user documentation.				
3. Subject documentation to the same level of review as the actual change.				

BAI06 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	9.2 Change management
ITIL V3 2011	Service Transition, 4.2 Change Management

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

BAI07 Manage Change Acceptance and Transitioning	Area: Management Domain: Build, Acquire and Implement
Process Description Formally accept and make operational new solutions, including implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and IT services, early production support, and a post-implementation review.	
Process Purpose Statement Implement solutions safely and in line with the agreed-on expectations and outcomes.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
08 Adequate use of applications, information and technology solutions	• Percent of business process owners satisfied with supporting IT products and services • Level of business user understanding of how technology solutions support their processes • Satisfaction level of business users with training and user manuals • NPV showing business satisfaction level of the quality and usefulness of the technology solutions
12 Enablement and support of business processes by integrating applications and technology into business processes	• Number of business processing incidents caused by technology integration errors • Number of business process changes that need to be delayed or reworked because of technology integration issues • Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues • Number of applications or critical infrastructures operating in silos and not integrated
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Acceptance testing meets stakeholder approval and takes into account all aspects of the implementation and conversion plans.	• Percent of stakeholders satisfied with the completeness of testing process
2. Releases are ready for promotion into production with stakeholder readiness and support.	• Number and percent of releases not ready for release on schedule
3. Releases are promoted successfully, are stable and meet expectations.	• Number or percent of releases that fail to stabilise within an acceptable period • Percent of releases causing downtime
4. Lessons learned contribute to future releases.	• Number and percent of root cause analyses completed

Personal Copy of: Dr. David Lanter

BAI07 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI07.01 Establish an implementation plan.					C	R		A	C		R					C	C	R	C	R	C		R	R	R	C
BAI07.02 Plan business process, system and data conversion.					C	R		A	C		R					C	C	R	C	R	C		R	R	R	C
BAI07.03 Plan acceptance tests.					A	R		R	I								C	I		R	R		I	R	R	C
BAI07.04 Establish a test environment.					A	R		R	I									I		R	R		I	R	R	C
BAI07.05 Perform acceptance tests.					A	R		R	I									I		R	R		I	R	R	C
BAI07.06 Promote to production and manage releases.						R		A	I									I		R	R		R	I	I	I
BAI07.07 Provide early production support.						R		A	I									I		R	R		R	I	I	I
BAI07.08 Perform a post-implementation review.						R		A	I							C	C	I		R	R		R	C	I	I

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

BAI07 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
BAI07.01 Establish an implementation plan. Establish an implementation plan that covers system and data conversion, acceptance testing criteria, communication, training, release preparation, promotion to production, early production support, a fallback/backout plan, and a post-implementation review. Obtain approval from relevant parties.	**From**	**Description**	**Description**	**To**
	BAI01.09	Quality management plan	Approved implementation plan	Internal
	BAI06.01	• Change plan and schedule • Approved requests for change	Implementation fallback and recovery process	Internal
Activities				
1. Create an implementation plan that reflects the broad implementation strategy, the sequence of implementation steps, resource requirements, inter-dependencies, criteria for management acceptance of the production implementation, installation verification requirements, transition strategy for production support, and update of BCPs.				
2. Confirm that all implementation plans are approved by technical and business stakeholders and reviewed by internal audit, as appropriate.				
3. Obtain commitment from external solution providers to their involvement in each step of the implementation.				
4. Identify and document the fallback and recovery process.				
5. Formally review the technical and business risk associated with implementation and ensure that the key risk is considered and addressed in the planning process.				

Personal Copy of: Dr. David Lanter

BAI07 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI07.02 Plan business process, system and data conversion. Prepare for business process, IT service data and infrastructure migration as part of the enterprise's development methods, including audit trails and a recovery plan should the migration fail.	**From**	**Description**	**Description**	**To**
			Migration plan	DSS06.02
Activities				
1. Define a business process, IT: service data and infrastructure migration plan. Consider, for example, hardware, networks, operating systems, software, transaction data, master files, backups and archives, interfaces with other systems (both internal and external), possible compliance requirements, business procedures, and system documentation, in the development of the plan.				
2. Consider all necessary adjustments to procedures, including revised roles and responsibilities and control procedures, in the business process conversion plan.				
3. Incorporate in the data conversion plan methods for collecting, converting and verifying data to be converted, and identifying and resolving any errors found during conversion. Include comparing the original and converted data for completeness and integrity.				
4. Confirm that the data conversion plan does not require changes in data values unless absolutely necessary for business reasons. Document changes made to data values, and secure approval from the business process data owner.				
5. Rehearse and test the conversion before attempting a live conversion.				
6. Consider the risk of conversion problems, business continuity planning, and fallback procedures in the business process, data and infrastructure migration plan where there are risk management, business needs or regulatory/compliance requirements.				
7. Co-ordinate and verify the timing and completeness of the conversion cutover so there is a smooth, continuous transition with no loss of transaction data. Where necessary, in the absence of any other alternative, freeze live operations.				
8. Plan to back up all systems and data taken at the point prior to conversion. Maintain audit trails to enable the conversion to be retraced and ensure that there is a recovery plan covering rollback of migration and fallback to previous processing should the migration fail.				
9. Plan retention of backup and archived data to conform to business needs and regulatory or compliance requirements.				
Management Practice	**Inputs**		**Outputs**	
BAI07.03 Plan acceptance tests. Establish a test plan based on enterprisewide standards that define roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.	**From**	**Description**	**Description**	**To**
	BAI01.09	Requirements for independent verification of deliverables	Approved acceptance test plan	BAI01.04 BAI01.08
	BAI03.07	• Test procedures • Test plan		
	BAI03.08	• Test result communications • Test result logs and audit trails		
Activities				
1. Develop and document the test plan, which aligns to the programme and project quality plan and relevant organisational standards. Communicate and consult with appropriate business process owners and IT stakeholders.				
2. Ensure that the test plan reflects an assessment of risk from the project and that all functional and technical requirements are tested. Based on assessment of the risk of system failure and faults on implementation, the plan should include requirements for performance, stress, usability, pilot and security testing.				
3. Ensure that the test plan addresses the potential need for internal or external accreditation of outcomes of the test process (e.g., financial regulatory requirements).				
4. Ensure that the test plan identifies necessary resources to execute testing and evaluate the results. Examples of resources include construction of test environments and use of staff time for the test group, including potential temporary replacement of test staff in the production or development environments. Ensure that stakeholders are consulted on the resource implications of the test plan.				
5. Ensure that the test plan identifies testing phases appropriate to the operational requirements and environment. Examples of such testing phases include unit test, system test, integration test, user acceptance test, performance test, stress test, data conversion test, security test, operational readiness test, and backup and recovery tests.				
6. Confirm that the test plan considers test preparation (including site preparation), training requirements, installation or an update of a defined test environment, planning/performing/documenting/retaining test cases, error and problem handling, correction and escalation, and formal approval.				
7. Ensure that the test plan establishes clear criteria for measuring the success of undertaking each testing phase. Consult the business process owners and IT stakeholders in defining the success criteria. Determine that the plan establishes remediation procedures when the success criteria are not met (e.g., in a case of significant failures in a testing phase, the plan provides guidance on whether to proceed to the next phase, stop testing or postpone implementation).				
8. Confirm that all test plans are approved by stakeholders, including business process owners and IT, as appropriate. Examples of such stakeholders are application development managers, project managers and business process end users.				

Personal Copy of: Dr. David Lanter

BAI07 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI07.04 Establish a test environment. Define and establish a secure test environment representative of the planned business process and IT operations environment, performance and capacity, security, internal controls, operational practices, data quality and privacy requirements, and workloads.	**From**	**Description**	**Description**	**To**
			Test data	Internal
Activities				
1. Create a database of test data that are representative of the production environment. Sanitise data used in the test environment from the production environment according to business needs and organisational standards (e.g., consider whether compliance or regulatory requirements oblige the use of sanitised data).				
2. Protect sensitive test data and results against disclosure, including access, retention, storage and destruction. Consider the effect of interaction of organisational systems with those of third parties.				
3. Put in place a process to enable proper retention or disposal of test results, media and other associated documentation to enable adequate review and subsequent analysis as required by the test plan. Consider the effect of regulatory or compliance requirements.				
4. Ensure that the test environment is representative of the future business and operational landscape, including business process procedures and roles, likely workload stress, operating systems, necessary application software, database management systems, and network and computing infrastructure found in the production environment.				
5. Ensure that the test environment is secure and incapable of interacting with production systems.				
Management Practice	**Inputs**		**Outputs**	
BAI07.05 Perform acceptance tests. Test changes independently in accordance with the defined test plan prior to migration to the live operational environment.	**From**	**Description**	**Description**	**To**
			Test results log	Internal
			Evaluation of acceptance results	BAI01.06
			Approved acceptance and release for production	BAI01.04
Activities				
1. Review the categorised log of errors found in the testing process by the development team, verifying that all errors have been remediated or formally accepted.				
2. Evaluate the final acceptance against the success criteria and interpret the final acceptance testing results. Present them in a form that is understandable to business process owners and IT so an informed review and evaluation can take place.				
3. Approve the acceptance with formal sign-off by the business process owners, third parties (as appropriate) and IT stakeholders prior to promotion to production.				
4. Ensure that testing of changes is undertaken in accordance with the testing plan. Ensure that the testing is designed and conducted by a test group independent from the development team. Consider the extent to which business process owners and end users are involved in the test group. Ensure that testing is conducted only within the test environment.				
5. Ensure that the tests and anticipated outcomes are in accordance with the defined success criteria set out in the testing plan.				
6. Consider using clearly defined test instructions (scripts) to implement the tests. Ensure that the independent test group assesses and approves each test script to confirm that it adequately addresses test success criteria set out in the test plan. Consider using scripts to verify the extent to which the system meets security requirements.				
7. Consider the appropriate balance between automated scripted tests and interactive user testing.				
8. Undertake tests of security in accordance with the test plan. Measure the extent of security weaknesses or loopholes. Consider the effect of security incidents since construction of the test plan. Consider the effect on access and boundary controls.				
9. Undertake tests of system and application performance in accordance with the test plan. Consider a range of performance metrics (e.g., end-user response times and database management system update performance).				
10. When undertaking testing, ensure that the fallback and rollback elements of the test plan have been addressed.				
11. Identify, log and classify (e.g., minor, significant, mission-critical) errors during testing. Ensure that an audit trail of test results is available. Communicate results of testing to stakeholders in accordance with the test plan to facilitate bug fixing and further quality enhancement.				

Personal Copy of: Dr. David Lanter

BAI07 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI07.06 Promote to production and manage releases. Promote the accepted solution to the business and operations. Where appropriate, run the solution as a pilot implementation or in parallel with the old solution for a defined period and compare behaviour and results. If significant problems occur, revert back to the original environment based on the fallback/backout plan. Manage releases of solution components.	**From**	**Description**	**Description**	**To**
			Release plan	BAI10.01
			Release log	Internal
Activities				
1. Prepare for transfer of business procedures and supporting services, applications and infrastructure from testing to the production environment in accordance with organisational change management standards.				
2. Determine the extent of pilot implementation or parallel processing of the old and new systems in line with the implementation plan.				
3. Promptly update relevant business process and system documentation, configuration information and contingency plan documents, as appropriate.				
4. Ensure that all media libraries are updated promptly with the version of the solution component being transferred from testing to the production environment. Archive the existing version and its supporting documentation. Ensure that promotion to production of systems, application software and infrastructure is under configuration control.				
5. Where distribution of solution components is conducted electronically, control automated distribution to ensure that users are notified and distribution occurs only to authorised and correctly identified destinations. Include in the release process backout procedures to enable the distribution of changes to be reviewed in the event of a malfunction or error.				
6. Where distribution takes physical form, keep a formal log of what items have been distributed, to whom, where they have been implemented, and when each has been updated.				
Management Practice	**Inputs**		**Outputs**	
BAI07.07 Provide early production support. Provide early support to the users and IT operations for an agreed-on period of time to deal with issues and help stabilise the new solution.	**From**	**Description**	**Description**	**To**
	APO11.03	Review results of quality of service, including customer feedback	Supplemental support plan	APO08.04 APO08.05 DSS02.04
	BAI05.05	Success measures and results		
Activities				
1. Provide additional resources, as required, to end users and support personnel until the release has stabilised.				
2. Provide additional IT systems resources, as required, until the release is in a stable operational environment.				

Personal Copy of: Dr. David Lanter

BAI07 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI07.08 Perform a post-implementation review. Conduct a post-implementation review to confirm outcome and results, identify lessons learned, and develop an action plan. Evaluate and check the actual performance and outcomes of the new or changed service against the predicted performance and outcomes (i.e., the service expected by the user or customer).	**From**	**Description**	**Description**	**To**
	APO11.04	Results of quality reviews and audits	Post-implementation review report	BAI01.13 BAI01.14
	APO11.05	• Root causes of quality delivery failures • Results of solution and service delivery quality monitoring	Remedial action plan	BAI01.13 BAI01.14
	BAI05.05	Success measures and results		
Activities				
1. Establish procedures to ensure that post-implementation reviews identify, assess and report on the extent to which: • Enterprise requirements have been met. • Expected benefits have been realised. • The system is considered usable. • Internal and external stakeholder expectations are met. • Unexpected impacts on the enterprise have occurred. • Key risk is mitigated. • The change management, installation and accreditation processes were performed effectively and efficiently.				
2. Consult business process owners and IT technical management in the choice of metrics for measurement of success and achievement of requirements and benefits.				
3. Conduct the post-implementation review in accordance with the organisational change management process. Engage business process owners and third parties, as appropriate.				
4. Consider requirements for post-implementation review arising from outside business and IT (e.g., internal audit, ERM, compliance).				
5. Agree on and implement an action plan to address issues identified in the post-implementation review. Engage business process owners and IT technical management in the development of the action plan.				

BAI07 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	0.1 Release management process
ITIL V3 2011	• Service Transition, 4.1 Transition Planning and Support • Service Transition, 4.4 Release and Deployment Management • Service Transition, 4.5 Service Validation and Testing • Service Transition, 4.6 Change Evaluation
PMBOK	PMBOK quality assurance and acceptance of all products
PRINCE2	PRINCE2 product-based planning

Personal Copy of: Dr. David Lanter

BAI08 Manage Knowledge	Area: Management Domain: Build, Acquire and Implement
Process Description Maintain the availability of relevant, current, validated and reliable knowledge to support all process activities and to facilitate decision making. Plan for the identification, gathering, organising, maintaining, use and retirement of knowledge.	
Process Purpose Statement Provide the knowledge required to support all staff in their work activities and for informed decision making and enhanced productivity.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
09 IT agility	• Level of satisfaction of business executives with IT's responsiveness to new requirements • Number of critical business processes supported by up-to-date infrastructure and applications • Average time to turn strategic IT objectives into an agreed-on and approved initiative
17 Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of IT innovation possibilities • Level of stakeholder satisfaction with levels of IT innovation expertise and ideas • Number of approved initiatives resulting from innovative IT ideas
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Sources of information are identified and classified.	• Percent of information categories covered • Volume of information classified • Percent of categorised information validated
2. Knowledge is used and shared.	• Percent of available knowledge actually used • Number of users trained in using and sharing knowledge
3. Knowledge sharing is embedded in the culture of the enterprise.	• Level of satisfaction of users • Percent of knowledge repository used
4. Knowledge is updated and improved to support requirements.	• Frequency of update

BAI08 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI08.01 Nurture and facilitate a knowledge-sharing culture.					A	R										R	R	R	R	R	R	R	R	R	R	R
BAI08.02 Identify and classify sources of information.					A	R									C	C	C	R		R	R		R			
BAI08.03 Organise and contextualise information into knowledge.						C									C	I	I	A		R	R	R				
BAI08.04 Use and share knowledge.						A										R	R	R	C	C	C	R	C	C	C	C
BAI08.05 Evaluate and retire information.						A										C	C	R	R	R	R	R	R	R	R	R

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

BAI08 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
BAI08.01 Nurture and facilitate a knowledge-sharing culture. Devise and implement a scheme to nurture and facilitate a knowledge-sharing culture.	**From**	**Description**	**Description**	**To**
			Communications on value of knowledge	APO01.04
Activities				
1. Proactively communicate the value of knowledge to encourage knowledge creation, use, re-use and sharing.				
2. Encourage the sharing and transfer of knowledge by identifying and leveraging motivational factors.				
3. Create an environment, tools and artefacts that support the sharing and transfer of knowledge.				
4. Embed knowledge management practices into other IT processes.				
5. Set management expectations and demonstrate appropriate attitude regarding the usefulness of knowledge and the need to share enterprise knowledge.				
Management Practice	**Inputs**		**Outputs**	
BAI08.02 Identify and classify sources of information. Identify, validate and classify diverse sources of internal and external information required to enable effective use and operation of business processes and IT services.	**From**	**Description**	**Description**	**To**
	Outside COBIT	Knowledge requirements and sources	Classification of information sources	Internal
Activities				
1. Identify potential knowledge users, including owners of information who may need to contribute and approve knowledge. Obtain knowledge requirements and sources of information from identified users.				
2. Consider content types (procedures, processes, structures, concepts, policies, rules, facts, classifications), artefacts (documents, records, video, voice), and structured and unstructured information (experts, social media, email, voice mail, RSS feeds).				
3. Classify sources of information based on a content classification scheme (e.g., information architecture model). Map sources of information to the classification scheme.				
4. Collect, collate and validate information sources based on information validation criteria (e.g., understandability, relevance, importance, integrity, accuracy, consistency, confidentiality, currency and reliability).				
Management Practice	**Inputs**		**Outputs**	
BAI08.03 Organise and contextualise information into knowledge. Organise information based on classification criteria. Identify and create meaningful relationships between information elements and enable use of information. Identify owners and define and implement levels of access to knowledge resources.	**From**	**Description**	**Description**	**To**
	BAI03.03	Documented solution components	Published knowledge repositories	APO07.03
	BAI05.07	Knowledge transfer plans		
Activities				
1. Identify shared attributes and match sources of information, creating relationships between information sets (information tagging).				
2. Create views to related data sets, considering stakeholder and organisational requirements.				
3. Devise and implement a scheme to manage unstructured knowledge not available through formal sources (e.g., expert knowledge).				
4. Publish and make knowledge accessible to relevant stakeholders based on roles and access mechanisms.				
Management Practice	**Inputs**		**Outputs**	
BAI08.04 Use and share knowledge. Propagate available knowledge resources to relevant stakeholders and communicate how these resources can be used to address different needs (e.g., problem solving, learning, strategic planning and decision making).	**From**	**Description**	**Description**	**To**
	BAI03.03	Documented solution components	Knowledge user database	Internal
	BAI05.05	Operation and use plan	Knowledge awareness and training schemes	APO07.03
	BAI05.07	Knowledge transfer plans		
Activities				
1. Identify potential knowledge users by knowledge classification.				
2. Transfer knowledge to knowledge users based on a needs gap analysis and effective learning techniques and access tools.				
3. Educate and train users on available knowledge, access to knowledge and use of knowledge access tools.				

Personal Copy of: Dr. David Lanter

BAI08 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
BAI08.05 Evaluate and retire information. Measure the use and evaluate the currency and relevance of information. Retire obsolete information.			Knowledge use evaluation results	Internal
			Rules for knowledge retirement	Internal
Activities				
1. Measure the use and evaluate the usefulness, relevance and value of knowledge elements. Identify related information that is no longer relevant to the enterprise's knowledge requirements.				
2. Define the rules for knowledge retirement and retire knowledge accordingly.				

BAI08 Related Guidance	
Related Standard	**Detailed Reference**
ITIL V3 2011	Service Transition, 4.7 Knowledge Management

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

BAI09 Manage Assets	Area: Management Domain: Build, Acquire and Implement
Process Description Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available. Manage software licences to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with licence agreements.	
Process Purpose Statement Account for all IT assets and optimise the value provided by these assets.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Licences are compliant and aligned with business need.	• Percent of used licences against paid-for licences
2. Assets are maintained at optimal levels.	• Number of assets not utilised • Benchmark costs • Number of obsolete assets

BAI09 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI09.01 Identify and record current assets.			C			C												I	C	C	A	R	C			
BAI09.02 Manage critical assets.			C		I	C										C	C		R	R	A	R	C	C	C	
BAI09.03 Manage the asset life cycle.						C													C	C	A	R	R			
BAI09.04 Optimise asset costs.			R		I	C												A	R	R	R	R	R			
BAI09.05 Manage licences.					I	C										C	R	A		R	R	R	C			

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

BAI09 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
BAI09.01 Identify and record current assets. Maintain an up-to-date and accurate record of all IT assets required to deliver services and ensure alignment with configuration management and financial management.	**From**	**Description**	**Description**	**To**
	BAI03.04	Updates to asset inventory	Asset register	APO06.01 BAI10.03
	BAI10.02	Configuration repository	Results of physical inventory checks	BAI10.03 BAI10.04 DSS05.03
			Results of fit-for-purpose reviews	APO02.02
Activities				
1. Identify all owned assets in an asset register that records current status. Maintain alignment with the change management and configuration management processes, the configuration management system, and the financial accounting records.				
2. Identify legal, regulatory or contractual requirements that need to be addressed when managing the asset.				
3. Verify the existence of all owned assets by performing regular physical and logical inventory checks and reconciliation including the use of software discovery tools.				
4. Verify that the assets are fit for purpose (i.e., in a useful condition).				
5. Determine on a regular basis whether each asset continues to provide value and, if so, estimate the expected useful life for delivering value.				
6. Ensure accounting for all assets.				
Management Practice	**Inputs**		**Outputs**	
BAI09.02 Manage critical assets. Identify assets that are critical in providing service capability and take steps to maximise their reliability and availability to support business needs.	**From**	**Description**	**Description**	**To**
			Communication of planned maintenance downtime	APO08.04
			Maintenance agreements	Internal
Activities				
1. Identify assets that are critical in providing service capability by referencing requirements in service definitions, SLAs and the configuration management system.				
2. Monitor performance of critical assets by examining incident trends and, where necessary, take action to repair or replace.				
3. On a regular basis, consider the risk of failure or need for replacement of each critical asset.				
4. Maintain the resilience of critical assets by applying regular preventive maintenance, monitoring performance, and, if required, providing alternative and/or additional assets to minimise the likelihood of failure.				
5. Establish a preventive maintenance plan for all hardware, considering cost-benefit analysis, vendor recommendations, risk of outage, qualified personnel and other relevant factors.				
6. Establish maintenance agreements involving third-party access to organisational IT facilities for on-site and off-site activities (e.g., outsourcing). Establish formal service contracts containing or referring to all necessary security conditions, including access authorisation procedures, to ensure compliance with the organisational security policies and standards.				
7. Communicate to affected customers and users the expected impact (e.g., performance restrictions) of maintenance activities.				
8. Ensure that remote access services and user profiles (or other means used for maintenance or diagnosis) are active only when required.				
9. Incorporate planned downtime in an overall production schedule, and schedule the maintenance activities to minimise the adverse impact on business processes.				

Personal Copy of: Dr. David Lanter

BAI09 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI09.03 Manage the asset life cycle. Manage assets from procurement to disposal to ensure that assets are utilised as effectively and efficiently as possible and are accounted for and physically protected.	**From**	**Description**	**Description**	**To**
			Approved asset procurement requests	Internal
			Asset register revisions	BAI10.03
			Authorised asset retirements	BAI10.03
Activities				
1. Procure all assets based on approved requests and in accordance with the enterprise procurement policies and practices.				
2. Source, receive, verify, test and record all assets in a controlled manner, including physical labelling, as required.				
3. Approve payments and complete the process with suppliers according to agreed-on contract conditions.				
4. Deploy assets following the standard implementation life cycle, including change management and acceptance testing.				
5. Allocate assets to users, with acceptance of responsibilities and sign-off, as appropriate.				
6. Reallocate assets whenever possible when they are no longer required due to a change of user role, redundancy within a service, or retirement of a service.				
7. Dispose of assets when they serve no useful purpose due to retirement of all related services, obsolete technology or lack of users.				
8. Dispose of assets securely, considering, e.g., the permanent deletion of any recorded data on media devices and potential damage to the environment.				
9. Plan, authorise and implement retirement-related activities, retaining appropriate records to meet ongoing business and regulatory needs.				
Management Practice	**Inputs**		**Outputs**	
BAI09.04 Optimise asset costs. Regularly review the overall asset base to identify ways to optimise costs and maintain alignment with business needs.	**From**	**Description**	**Description**	**To**
			Results of cost optimisation reviews	APO02.02
			Opportunities to reduce asset costs or increase value	APO02.02
Activities				
1. On a regular basis, review the overall asset base, considering whether it is aligned with business requirements.				
2. Assess maintenance costs, consider reasonableness, and identify lower-cost options, including, where necessary, replacement with new alternatives.				
3. Review warranties and consider value for money and replacement strategies to determine lowest-cost options.				
4. Review the overall base to identify opportunities for standardisation, single sourcing, and other strategies that may lower procurement, support and maintenance costs.				
5. Use capacity and utilisation statistics to identify underutilised or redundant assets that could be considered for disposal or replacement to lower costs.				
6. Review the overall state to identify opportunities to leverage emerging technologies or alternative sourcing strategies to reduce costs or increase value for money.				

Personal Copy of: Dr. David Lanter

BAI09 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI09.05 Manage licences. Manage software licences so that the optimal number of licences is maintained to support business requirements and the number of licences owned is sufficient to cover the installed software in use.	**From**	**Description**	**Description**	**To**
			Register of software licences	BAI10.02
			Results of installed licence audits	MEA03.03
			Action plan to adjust licence numbers and allocations	APO02.05
Activities				
1. Maintain a register of all purchased software licences and associated licence agreements.				
2. On a regular basis, conduct an audit to identify all instances of installed licenced software.				
3. Compare the number of installed software instances with the number of licences owned.				
4. When instances are lower than the number owned, decide whether there is a need to retain or terminate licences, considering the potential to save on unnecessary maintenance, training and other costs.				
5. When instances are higher than the number owned, consider first the opportunity to uninstall instances that are no longer required or justified, and then, if necessary, purchase additional licences to comply with the licence agreement.				
6. On a regular basis, consider whether better value can be obtained by upgrading products and associated licences.				

BAI09 Related Guidance	
Related Standard	**Detailed Reference**
ITIL V3 2011	Service Transition, 4.3 Service Asset and Configuration Management

Personal Copy of: Dr. David Lanter

BAI10 Manage Configuration	Area: Management Domain: Build, Acquire and Implement
Process Description Define and maintain descriptions and relationships between key resources and capabilities required to deliver IT-enabled services, including collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository.	
Process Purpose Statement Provide sufficient information about service assets to enable the service to be effectively managed, assess the impact of changes and deal with service incidents.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
14 Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Configuration repository is accurate, complete and up to date.	• Number of deviations between the configuration repository and live configuration • Number of discrepancies relating to incomplete or missing configuration information

BAI10 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI10.01 Establish and maintain a configuration model.						C											C	C	C	I	A	R	R			
BAI10.02 Establish and maintain a configuration repository and baseline.																			C	R	A	R	R			
BAI10.03 Maintain and control configuration items.																		A	C	R	R	R	C			
BAI10.04 Produce status and configuration reports.						I											I	I	C	C	A	R	I			
BAI10.05 Verify and review integrity of the configuration repository.						I											R		R	R	A		R			

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

BAI10 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
BAI10.01 Establish and maintain a configuration model. Establish and maintain a logical model of the services, assets and infrastructure and how to record configuration items (CIs) and the relationships amongst them. Include the CIs considered necessary to manage services effectively and to provide a single reliable description of the assets in a service.	**From**	**Description**	**Description**	**To**
	BAI07.06	Release plan	Scope of configuration management model	Internal
			Logical configuration model	Internal
Activities				
1. Define and agree on the scope and level of detail for configuration management (i.e., which services, assets and infrastructure configurable items to include).				
2. Establish and maintain a logical model for configuration management, including information on configuration item types, configuration item attributes, relationship types, relationship attributes and status codes.				
Management Practice	**Inputs**		**Outputs**	
BAI10.02 Establish and maintain a configuration repository and baseline. Establish and maintain a configuration management repository and create controlled configuration baselines.	**From**	**Description**	**Description**	**To**
	BAI09.05	Register of software licences	Configuration repository	BAI09.01 DSS02.01
			Configuration baseline	BAI03.11
Activities				
1. Identify and classify configuration items and populate the repository.				
2. Create, review and formally agree on configuration baselines of a service, application or infrastructure.				
Management Practice	**Inputs**		**Outputs**	
BAI10.03 Maintain and control configuration items. Maintain an up-to-date repository of configuration items by populating with changes.	**From**	**Description**	**Description**	**To**
	BAI06.03	Change request status reports	Updated repository with configuration items	DSS02.01
	BAI09.01	• Results of physical inventory checks • Asset register	Approved changes to baseline	BAI03.11
	BAI09.03	• Authorised asset retirements • Asset register revisions		
Activities				
1. Regularly identify all changes to configuration items.				
2. Review proposed changes to configuration items against the baseline to ensure completeness and accuracy.				
3. Update configuration details for approved changes to configuration items.				
4. Create, review and formally agree on changes to configuration baselines whenever needed.				
Management Practice	**Inputs**		**Outputs**	
BAI10.04 Produce status and configuration reports. Define and produce configuration reports on status changes of configuration items.	**From**	**Description**	**Description**	**To**
	BAI09.01	Results of physical inventory checks	Configuration status reports	BAI03.11 DSS02.01
Activities				
1. Identify status changes of configuration items and report against the baseline.				
2. Match all configuration changes with approved requests for change to identify any unauthorised changes. Report unauthorised changes to change management.				
3. Identify reporting requirements from all stakeholders, including content, frequency and media. Produce reports according to the identified requirements.				

Personal Copy of: Dr. David Lanter

BAI10 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
BAI10.05 Verify and review integrity of the configuration repository. Periodically review the configuration repository and verify completeness and correctness against the desired target.			Results of physical verification of configuration items	Internal
			Licence deviations	MEA03.03
			Results of repository completeness reviews	Internal
Activities				
1. Periodically verify live configuration items against the configuration repository by comparing physical and logical configurations and using appropriate discovery tools, as required.				
2. Report and review all deviations for approved corrections or action to remove any unauthorised assets.				
3. Periodically verify that all physical configuration items, as defined in the repository, physically exist. Report any deviations to management.				
4. Set and periodically review the target for completeness of the configuration repository based on business need.				
5. Periodically compare the degree of completeness and accuracy against targets and take remedial action, as necessary, to improve the quality of the repository data.				

BAI10 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	9.1 Configuration management
ITIL V3 2011	Service Transition, 4.3 Service Asset and Configuration Management

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

Deliver, Service and Support (DSS)

01 Manage operations.

02 Manage service requests and incidents.

03 Manage problems.

04 Manage continuity.

05 Manage security services.

06 Manage business process controls.

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

DSS01 Manage Operations	Area: Management Domain: Deliver, Service and Support
Process Description Co-ordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services, including the execution of pre-defined standard operating procedures and the required monitoring activities.	
Process Purpose Statement Deliver IT operational service outcomes as planned.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Operational activities are performed as required and scheduled.	• Number of non-standard operational procedures executed • Number of incidents caused by operational problems
2. Operations are monitored, measured, reported and remediated.	• Ratio of events compared to the number of incidents • Percent of critical operational event types covered by automatic detection systems

DSS01 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS01.01 Perform operational procedures.																					A		C	C	C	
DSS01.02 Manage outsourced IT services.											I							A			R					
DSS01.03 Monitor IT infrastructure.				I		C					I						C	I		C	A		C	C		
DSS01.04 Manage the environment.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS01.05 Manage facilities.						I					C	A				C	C	C	I	C	R		I	R	I	

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

DSS01 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
DSS01.01 Perform operational procedures. Maintain and perform operational procedures and operational tasks reliably and consistently.	**From**	**Description**	**Description**	**To**
	BAI05.05	Operation and use plan	Operational schedule	Internal
			Backup log	Internal
Activities				
1. Develop and maintain operational procedures and related activities to support all delivered services.				
2. Maintain a schedule of operational activities, perform the activities, and manage the performance and throughput of the scheduled activities.				
3. Verify that all data expected for processing are received and processed completely, accurately and in a timely manner. Deliver output in accordance with enterprise requirements. Support restart and reprocessing needs. Ensure that users are receiving the right outputs in a secure and timely manner.				
4. Ensure that applicable security standards are met for the receipt, processing, storage and output of data in a way that meets enterprise objectives, the enterprise's security policy and regulatory requirements.				
5. Schedule, take and log backups in accordance with established policies and procedures.				
Management Practice	**Inputs**		**Outputs**	
DSS01.02 Manage outsourced IT services. Manage the operation of outsourced IT services to maintain the protection of enterprise information and reliability of service delivery.	**From**	**Description**	**Description**	**To**
	AP009.03	• OLAs • SLAs	Independent assurance plans	MEA02.06
	BAI05.05	Operation and use plan		
Activities				
1. Ensure that the enterprise's requirements for security of information processes are adhered to in accordance with contracts and SLAs with third parties hosting or providing services.				
2. Ensure that the enterprise's operational business and IT processing requirements and priorities for service delivery are adhered to in accordance with contracts and SLAs with third parties hosting or providing services.				
3. Integrate critical internal IT management processes with those of outsourced service providers, covering, e.g., performance and capacity planning, change management, configuration management, service request and incident management, problem management, security management, business continuity, and the monitoring of process performance and reporting.				
4. Plan for independent audit and assurance of the operational environments of outsourced providers to confirm that agreed-on requirements are being adequately addressed.				
Management Practice	**Inputs**		**Outputs**	
DSS01.03 Monitor IT infrastructure. Monitor the IT infrastructure and related events. Store sufficient chronological information in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.	**From**	**Description**	**Description**	**To**
	BAI03.11	Service definitions	Asset monitoring rules and event conditions	DSS02.01 DSS02.02
			Event logs	Internal
			Incident tickets	DSS02.02
Activities				
1. Log events, identifying the level of information to be recorded based on a consideration of risk and performance.				
2. Identify and maintain a list of infrastructure assets that need to be monitored based on service criticality and the relationship between configuration items and services that depend on them.				
3. Define and implement rules that identify and record threshold breaches and event conditions. Find a balance between generating spurious minor events and significant events so event logs are not overloaded with unnecessary information.				
4. Produce event logs and retain them for an appropriate period to assist in future investigations.				
5. Establish procedures for monitoring event logs and conduct regular reviews.				
6. Ensure that incident tickets are created in a timely manner when monitoring identifies deviations from defined thresholds.				

Personal Copy of: Dr. David Lanter

DSS01 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS01.04 Manage the environment. Maintain measures for protection against environmental factors. Install specialised equipment and devices to monitor and control the environment.	**From**	**Description**	**Description**	**To**
			Environmental policies	APO01.08
			Insurance policy reports	MEA03.03
Activities				
1. Identify natural and man-made disasters that might occur in the area within which the IT facilities are located. Assess the potential effect on the IT facilities.				
2. Identify how IT equipment, including mobile and off-site equipment, is protected against environmental threats. Ensure that the policy limits or excludes eating, drinking and smoking in sensitive areas, and prohibits storage of stationery and other supplies posing a fire hazard within computer rooms.				
3. Situate and construct IT facilities to minimise and mitigate susceptibility to environmental threats.				
4. Regularly monitor and maintain devices that proactively detect environmental threats (e.g., fire, water, smoke, humidity).				
5. Respond to environmental alarms and other notifications. Document and test procedures, which should include prioritisation of alarms and contact with local emergency response authorities, and train personnel in these procedures.				
6. Compare measures and contingency plans against insurance policy requirements and report results. Address points of non-compliance in a timely manner.				
7. Ensure that IT sites are built and designed to minimise the impact of environmental risk (e.g., theft, air, fire, smoke, water, vibration, terror, vandalism, chemicals, explosives). Consider specific security zones and/or fireproof cells (e.g., locating production and development environments/servers away from each other).				
8. Keep the IT sites and server rooms clean and in a safe condition at all times (i.e., no mess, no paper or cardboard boxes, no filled dustbins, no flammable chemicals or materials).				
Management Practice	**Inputs**		**Outputs**	
DSS01.05 Manage facilities. Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.	**From**	**Description**	**Description**	**To**
			Facilities assessment reports	MEA01.03
			Health and safety awareness	Internal
Activities				
1. Examine the IT facilities' requirement for protection against power fluctuations and outages, in conjunction with other business continuity planning requirements. Procure suitable uninterruptible supply equipment (e.g., batteries, generators) to support business continuity planning.				
2. Regularly test the uninterruptible power supply's mechanisms, and ensure that power can be switched to the supply without any significant effect on business operations.				
3. Ensure that the facilities housing the IT systems have more than one source for dependent utilities (e.g., power, telecommunications, water, gas). Separate the physical entrance of each utility.				
4. Confirm that cabling external to the IT site is located underground or has suitable alternative protection. Determine that cabling within the IT site is contained within secured conduits, and wiring cabinets have access restricted to authorised personnel. Properly protect cabling against damage caused by fire, smoke, water, interception and interference.				
5. Ensure that cabling and physical patching (data and phone) are structured and organised. Cabling and conduit structures should be documented (e.g., blueprint building plan and wiring diagrams).				
6. Analyse the facilities housing's high-availability systems for redundancy and fail-over cabling requirements (external and internal).				
7. Ensure that IT sites and facilities are in ongoing compliance with relevant health and safety laws, regulations, guidelines, and vendor specifications.				
8. Educate personnel on a regular basis on health and safety laws, regulations, and relevant guidelines. Educate personnel on fire and rescue drills to ensure knowledge and actions taken in case of fire or similar incidents.				
9. Record, monitor, manage and resolve facilities incidents in line with the IT incident management process. Make available reports on facilities incidents where disclosure is required in terms of laws and regulations.				
10. Ensure that IT sites and equipment are maintained according to the supplier's recommended service intervals and specifications. The maintenance must be carried out only by authorised personnel.				
11. Analyse physical alterations to IT sites or premises to reassess the environmental risk (e.g., fire or water damage). Report results of this analysis to business continuity and facilities management.				

DSS01 Related Guidance	
Related Standard	**Detailed Reference**
ITIL V3 2011	Service Operation, 4.1 Event Management

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

DSS02 Manage Service Requests and Incidents	Area: Management Domain: Deliver, Service and Support
Process Description Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.	
Process Purpose Statement Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. IT-related services are available for use.	• Number and percent of incidents causing disruption to business-critical processes • Mean time between incidents according to IT-enabled service
2. Incidents are resolved according to agreed-on service levels.	• Percent of incidents resolved within an agreed-on/acceptable period of time
3. Service requests are dealt with according to agreed-on service levels and to the satisfaction of users.	• Level of user satisfaction with service request fulfilment • Mean elapsed time for handling each type of service request

Personal Copy of: Dr. David Lanter

DSS02 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS02.01 Define incident and service request classification schemes.						C					I	I						A	C	R	R		R	C	C	C
DSS02.02 Record, classify and prioritise requests and incidents.						I					I	I									A		R			I
DSS02.03 Verify, approve and fulfil service requests.						R												I		R	R		A			
DSS02.04 Investigate, diagnose and allocate incidents.						R					I	I				I	I	I		C	R		A	C		
DSS02.05 Resolve and recover from incidents.						I					I	I				C	C	I		R	R		A	R		C
DSS02.06 Close service requests and incidents.						I					I	I				I	I	I		I	A		I	R		I
DSS02.07 Track status and produce reports.						I					I	I				I	I	I		I	A		R	I		

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

DSS02 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
DSS02.01 Define incident and service request classification schemes. Define incident and service request classification schemes and models.	AP009.03	SLAs	Incident and service request classification schemes and models	Internal
	BAI10.02	Configuration repository	Rules for incident escalation	Internal
	BAI10.03	Updated repository with configuration items	Criteria for problem registration	DSS03.01
	BAI10.04	Configuration status reports		
	DSS01.03	Asset monitoring rules and event conditions		
	DSS03.01	Problem classification scheme		
	DSS04.03	Incident response actions and communications		
Activities				
1. Define incident and service request classification and prioritisation schemes and criteria for problem registration, to ensure consistent approaches for handling, informing users about and conducting trend analysis.				
2. Define incident models for known errors to enable efficient and effective resolution.				
3. Define service request models according to service request type to enable self-help and efficient service for standard requests.				
4. Define incident escalation rules and procedures, especially for major incidents and security incidents.				
5. Define incident and request knowledge sources and their use.				

Personal Copy of: Dr. David Lanter

DSS02 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS02.02 Record, classify and prioritise requests and incidents. Identify, record and classify service requests and incidents, and assign a priority according to business criticality and service agreements.	**From**	**Description**	**Description**	**To**
	AP009.03	SLAs	Incident and service request log	Internal
	BAI04.05	Emergency escalation procedure	Classified and prioritised incidents and service requests	AP008.03 AP009.04 AP013.03
	DSS01.03	• Incident tickets • Asset monitoring rules and event conditions		
	DSS05.07	Security incident tickets		
Activities				
1. Log all service requests and incidents, recording all relevant information so that they can be handled effectively and a full historical record can be maintained.				
2. To enable trend analysis, classify service requests and incidents by identifying type and category.				
3. Prioritise service requests and incidents based on SLA service definition of business impact and urgency.				
Management Practice	**Inputs**		**Outputs**	
DSS02.03 Verify, approve and fulfil service requests. Select the appropriate request procedures and verify that the service requests fulfil defined request criteria. Obtain approval, if required, and fulfil the requests.	**From**	**Description**	**Description**	**To**
	AP012.06	Risk-related root causes	Approved service requests	BAI06.01
			Fulfilled service requests	Internal
Activities				
1. Verify entitlement for service requests using, where possible, a predefined process flow and standard changes.				
2. Obtain financial and functional approval or sign-off, if required, or predefined approvals for agreed-on standard changes.				
3. Fulfil the requests by performing the selected request procedure, using, where possible, self-help automated menus and predefined request models for frequently requested items.				
Management Practice	**Inputs**		**Outputs**	
DSS02.04 Investigate, diagnose and allocate incidents. Identify and record incident symptoms, determine possible causes, and allocate for resolution.	**From**	**Description**	**Description**	**To**
	BAI07.07	Supplemental support plan	Incident symptoms	Internal
			Problem log	DSS03.01
Activities				
1. Identify and describe relevant symptoms to establish the most probable causes, of the incidents. Reference available knowledge resources (including known errors and problems) to identify possible incident resolutions (temporary workarounds and/or permanent solutions).				
2. If a related problem or known error does not already exist and if the incident satisfies agreed-on criteria for problem registration, log a new problem.				
3. Assign incidents to specialist functions if deeper expertise is needed, and engage the appropriate level of management, where and if needed.				
Management Practice	**Inputs**		**Outputs**	
DSS02.05 Resolve and recover from incidents. Document, apply and test the identified solutions or workarounds and perform recovery actions to restore the IT-related service.	**From**	**Description**	**Description**	**To**
	AP012.06	Risk-related incident response plans	Incident resolutions	DSS03.04
	DSS03.03	Known-error records		
	DSS03.04	Communication of knowledge learned		
Activities				
1. Select and apply the most appropriate incident resolutions (temporary workaround and/or permanent solution).				
2. Record whether workarounds were used for incident resolution.				
3. Perform recovery actions, if required.				
4. Document incident resolution and assess if the resolution can be used as a future knowledge source.				

Personal Copy of: Dr. David Lanter

DSS02 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS02.06 Close service requests and incidents. Verify satisfactory incident resolution and/or request fulfilment, and close.	**From**	**Description**	**Description**	**To**
	DSS03.04	Closed problem records	Closed service requests and incidents	APO08.03 APO09.04 DSS03.04
			User confirmation of satisfactory fulfilment or resolution	APO08.03
Activities				
1. Verify with the affected users (if agreed on) that the service request has been satisfactory fulfilled or the incident has been satisfactory resolved.				
2. Close service requests and incidents.				
Management Practice	**Inputs**		**Outputs**	
DSS02.07 Track status and produce reports. Regularly track, analyse and report incident and request fulfilment trends to provide information for continual improvement.	**From**	**Description**	**Description**	**To**
	APO09.03	OLAs	Incident status and trends report	APO08.03 APO09.04 APO11.04 APO12.01 MEA01.03
	DSS03.01	Problem status reports		
	DSS03.02	Problem resolution reports		
	DSS03.05	Problem resolution monitoring reports	Request fulfilment status and trends report	APO08.03 APO09.04 APO11.04 MEA01.03
Activities				
1. Monitor and track incident escalations and resolutions and request handling procedures to progress towards resolution or completion.				
2. Identify information stakeholders and their needs for data or reports. Identify reporting frequency and medium.				
3. Analyse incidents and service requests by category and type to establish trends and identify patterns of recurring issues, SLA breaches or inefficiencies. Use the information as input to continual improvement planning.				
4. Produce and distribute timely reports or provide controlled access to online data.				

DSS02 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	• 6.1 Service level management • 8.2 Incident management
ISO 27002	13. Information Security Incident Management
ITIL V3 2011	• Service Operation, 4.2 Incident Management • Service Operation, 4.3 Request Fulfilment

Personal Copy of: Dr. David Lanter

DSS03 Manage Problems	Area: Management Domain: Deliver, Service and Support
Process Description Identify and classify problems and their root causes and provide timely resolution to prevent recurring incidents. Provide recommendations for improvements.	
Process Purpose Statement Increase availability, improve service levels, reduce costs, and improve customer convenience and satisfaction by reducing the number of operational problems.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
14 Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. IT-related problems are resolved so that they do not reoccur.	• Decrease in number of recurring incidents caused by unresolved problems • Percent of major incidents for which problems were logged • Percent of workarounds defined for open problems • Percent of problems logged as part of the proactive problem management activity • Number of problems for which a satisfactory resolution that addressed root causes were found

Personal Copy of: Dr. David Lanter

DSS03 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS03.01 Identify and classify problems.					I	C					I	I				I	I	R	C	R	R		A	C		
DSS03.02 Investigate and diagnose problems.											I	I							C	C	A		R	R		
DSS03.03 Raise known errors.																					A		R	R		
DSS03.04 Resolve and close problems.					I	C					I	I				C	C	I	C	C	R		A			
DSS03.05 Perform proactive problem management.						C													C	C	R		A			

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

DSS03 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
DSS03.01 Identify and classify problems. Define and implement criteria and procedures to report problems identified, including problem classification, categorisation and prioritisation.	**From**	**Description**	**Description**	**To**
	APO12.06	Risk-related root causes	Problem classification scheme	DSS02.01
	DSS02.01	Criteria for problem registration	Problem status reports	DSS02.07
	DSS02.04	Problem log	Problem register	Internal
Activities				
1. Identify problems through the correlation of incident reports, error logs and other problem identification resources. Determine priority levels and categorisation to address problems in a timely manner based on business risk and service definition.				
2. Handle all problems formally with access to all relevant data, including information from the change management system and IT configuration/asset and incident details.				
3. Define appropriate support groups to assist with problem identification, root cause analysis and solution determination to support problem management. Determine support groups based on pre-defined categories, such as hardware, network, software, applications and support software.				
4. Define priority levels through consultation with the business to ensure that problem identification and root cause analysis are handled in a timely manner according to the agreed-on SLAs. Base priority levels on business impact and urgency.				
5. Report the status of identified problems to the service desk so customers and IT management can be kept informed.				
6. Maintain a single problem management catalogue to register and report problems identified and to establish audit trails of the problem management processes, including the status of each problem (i.e., open, reopen, in progress or closed).				
Management Practice	**Inputs**		**Outputs**	
DSS03.02 Investigate and diagnose problems. Investigate and diagnose problems using relevant subject management experts to assess and analyse root causes.	**From**	**Description**	**Description**	**To**
	APO12.06	Risk-related root causes	Root causes of problems	Internal
			Problem resolution reports	DSS02.07
Activities				
1. Identify problems that may be known errors by comparing incident data with the database of known and suspected errors (e.g., those communicated by external vendors) and classify problems as a known error.				
2. Associate the affected configuration items to the established/known error.				
3. Produce reports to communicate the progress in resolving problems and to monitor the continuing impact of problems not solved. Monitor the status of the problem-handling process throughout its life cycle, including input from change and configuration management.				

Personal Copy of: Dr. David Lanter

DSS03 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS03.03 Raise known errors. As soon as the root causes of problems are identified, create known-error records and an appropriate workaround, and identify potential solutions.	**From**	**Description**	**Description**	**To**
			Known-error records	DSS02.05
			Proposed solutions to known errors	BAI06.01
Activities				
1. As soon as the root causes of problems are identified, create known-error records and develop a suitable workaround.				
2. Identify, evaluate, prioritise and process (via change management) solutions to known errors based on a cost-benefit business case and business impact and urgency.				
Management Practice	**Inputs**		**Outputs**	
DSS03.04 Resolve and close problems. Identify and initiate sustainable solutions addressing the root cause, raising change requests via the established change management process if required to resolve errors. Ensure that the personnel affected are aware of the actions taken and the plans developed to prevent future incidents from occurring.	**From**	**Description**	**Description**	**To**
	DSS02.05	Incident resolutions	Closed problem records	DSS02.06
	DSS02.06	Closed service requests and incidents	Communication of knowledge learned	APO08.04 DSS02.05
Activities				
1. Close problem records either after confirmation of successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.				
2. Inform the service desk of the schedule of problem closure, e.g., the schedule for fixing the known errors, the possible workaround or the fact that the problem will remain until the change is implemented, and the consequences of the approach taken. Keep affected users and customers informed as appropriate.				
3. Throughout the resolution process, obtain regular reports from change management on progress in resolving problems and errors.				
4. Monitor the continuing impact of problems and known errors on services.				
5. Review and confirm the success of resolutions of major problems.				
6. Make sure the knowledge learned from the review is incorporated into a service review meeting with the business customer.				
Management Practice	**Inputs**		**Outputs**	
DSS03.05 Perform proactive problem management. Collect and analyse operational data (especially incident and change records) to identify emerging trends that may indicate problems. Log problem records to enable assessment.	**From**	**Description**	**Description**	**To**
			Problem resolution monitoring reports	DSS02.07
			Identified sustainable solutions	BAI06.01
Activities				
1. Capture problem information related to IT changes and incidents and communicate it to key stakeholders. This communication could take the form of reports to and periodic meetings amongst incident, problem, change and configuration management process owners to consider recent problems and potential corrective actions.				
2. Ensure that process owners and managers from incident, problem, change and configuration management meet regularly to discuss known problems and future planned changes.				
3. To enable the enterprise to monitor the total costs of problems, capture change efforts resulting from problem management process activities (e.g., fixes to problems and known errors) and report on them.				
4. Produce reports to monitor the problem resolution against the business requirements and SLAs. Ensure the proper escalation of problems, e.g., escalation to a higher management level according to agreed-on criteria, contacting external vendors, or referring to the change advisory board to increase the priority of an urgent request for change (RFC) to implement a temporary workaround.				
5. To optimise the use of resources and reduce workarounds, track problem trends.				
6. Identify and initiate sustainable solutions (permanent fix) addressing the root cause, and raise change requests via the established change management processes.				

DSS03 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	8.3 Problem management
ITIL V3 2011	Service Operation, 4.4 Problem Management

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

DSS04 Manage Continuity	Area: Management Domain: Deliver, Service and Support
Process Description Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise.	
Process Purpose Statement Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
14 Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Business-critical information is available to the business in line with minimum required service levels.	• Percent of IT services meeting uptime requirements • Percent of successful and timely restoration from backup or alternate media copies • Percent of backup media transferred and stored securely
2. Sufficient resilience is in place for critical services.	• Number of critical business systems not covered by the plan
3. Service continuity tests have verified the effectiveness of the plan.	• Number of exercises and tests that have achieved recovery objectives • Frequency of tests
4. An up-to-date continuity plan reflects current business requirements.	• Percent of agreed-on improvements to the plan that have been reflected in the plan • Percent of issues identified that have been subsequently addressed in the plan
5. Internal and external parties have been trained in the continuity plan.	• Percent of internal and external stakeholders that have received training • Percent of issues identified that have been subsequently addressed in the training materials

Personal Copy of: Dr. David Lanter

DSS04 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS04.01 Define the business continuity policy, objectives and scope.				A	C	R					C					C	C	R			R	C	R		R	
DSS04.02 Maintain a continuity strategy.				A	C	R					I					C	C	R	R	C	R				R	
DSS04.03 Develop and implement a business continuity response.					I	R									I	C	C	R	C	C	R				A	
DSS04.04 Exercise, test and review the BCP.					I	R									I		R	R		C	R				A	
DSS04.05 Review, maintain and improve the continuity plan.				A	I	R					I							R		C	R				R	
DSS04.06 Conduct continuity plan training.					I	R												R		R	R	R			A	
DSS04.07 Manage backup arrangements.																				C	A				R	
DSS04.08 Conduct post-resumption review.					C	R					I							R	C	C	R	R			A	

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

DSS04 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
DSS04.01 Define the business continuity policy, objectives and scope. Define business continuity policy and scope aligned with enterprise and stakeholder objectives.	**From**	**Description**	**Description**	**To**
	APO09.03	SLAs	Policy and objectives for business continuity	APO01.04
			Disruptive incident scenarios	Internal
			Assessments of current continuity capabilities and gaps	Internal
Activities				
1. Identify internal and outsourced business processes and service activities that are critical to the enterprise operations or necessary to meet legal and/or contractual obligations.				
2. Identify key stakeholders and roles and responsibilities for defining and agreeing on continuity policy and scope.				
3. Define and document the agreed-on minimum policy objectives and scope for business continuity and embed the need for continuity planning in the enterprise culture.				
4. Identify essential supporting business processes and related IT services.				

Personal Copy of: Dr. David Lanter

DSS04 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS04.02 Maintain a continuity strategy. Evaluate business continuity management options and choose a cost-effective and viable continuity strategy that will ensure enterprise recovery and continuity in the face of a disaster or other major incident or disruption.	**From**	**Description**	**Description**	**To**
	APO12.06	• Risk-related root causes • Risk impact communications	Business impact analyses	APO12.02
			Continuity requirements	Internal
			Approved strategic options	APO02.05
Activities				
1. Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.				
2. Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption would have on them.				
3. Establish the minimum time required to recover a business process and supporting IT based on an acceptable length of business interruption and maximum tolerable outage.				
4. Assess the likelihood of threats that could cause loss of business continuity and identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.				
5. Analyse continuity requirements to identify the possible strategic business and technical options.				
6. Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.				
7. Identify resource requirements and costs for each strategic technical option and make strategic recommendations.				
8. Obtain executive business approval for selected strategic options.				
Management Practice	**Inputs**		**Outputs**	
DSS04.03 Develop and implement a business continuity response. Develop a business continuity plan (BCP) based on the strategy that documents the procedures and information in readiness for use in an incident to enable the enterprise to continue its critical activities.	**From**	**Description**	**Description**	**To**
	APO09.03	OLAs	Incident response actions and communications	DSS02.01
			BCP	Internal
Activities				
1. Define the incident response actions and communications to be taken in the event of disruption. Define related roles and responsibilities, including accountability for policy and implementation.				
2. Develop and maintain operational BCPs containing the procedures to be followed to enable continued operation of critical business processes and/or temporary processing arrangements, including links to plans of outsourced service providers.				
3. Ensure that key suppliers and outsource partners have effective continuity plans in place. Obtain audited evidence as required.				
4. Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity.				
5. Define and document the resources required to support the continuity and recovery procedures, considering people, facilities and IT infrastructure.				
6. Define and document the information backup requirements required to support the plans, including plans and paper documents as well as data files, and consider the need for security and off-site storage.				
7. Determine required skills for individuals involved in executing the plan and procedures.				
8. Distribute the plans and supporting documentation securely to appropriately authorised interested parties and make sure they are accessible under all disaster scenarios.				

Personal Copy of: Dr. David Lanter

DSS04 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS04.04 Exercise, test and review the BCP. Test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated.	**From**	**Description**	**Description**	**To**
			Test objectives	Internal
			Test exercises	Internal
			Test results and recommendations	Internal
Activities				
1. Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP in meeting business risk.				
2. Define and agree on with stakeholders exercises that are realistic, validate continuity procedures, and include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.				
3. Assign roles and responsibilities for performing continuity plan exercises and tests.				
4. Schedule exercises and test activities as defined in the continuity plan.				
5. Conduct a post-exercise debriefing and analysis to consider the achievement.				
6. Develop recommendations for improving the current continuity plan based on the results of the review.				
Management Practice	**Inputs**		**Outputs**	
DSS04.05 Review, maintain and improve the continuity plan. Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plan in accordance with the change control process to ensure that the continuity plan is kept up to date and continually reflects actual business requirements.	**From**	**Description**	**Description**	**To**
			Results of reviews of plans	Internal
			Recommended changes to plans	Internal
Activities				
1. Review the continuity plan and capability on a regular basis against any assumptions made and current business operational and strategic objectives.				
2. Consider whether a revised business impact assessment may be required, depending on the nature of the change.				
3. Recommend and communicate changes in policy, plans, procedures, infrastructure, and roles and responsibilities for management approval and processing via the change management process.				
4. Review the continuity plan on a regular basis to consider the impact of new or major changes to: enterprise organisation, business processes, outsourcing arrangements, technologies, infrastructure, operating systems and application systems.				
Management Practice	**Inputs**		**Outputs**	
DSS04.06 Conduct continuity plan training. Provide all concerned internal and external parties with regular training sessions regarding the procedures and their roles and responsibilities in case of disruption.	**From**	**Description**	**Description**	**To**
	HR	List of personnel requiring training	Training requirements	APO07.03
			Monitoring results of skills and competencies	APO07.03
Activities				
1. Define and maintain training requirements and plans for those performing continuity planning, impact assessments, risk assessments, media communication and incident response. Ensure that the training plans consider frequency of training and training delivery mechanisms.				
2. Develop competencies based on practical training including participation in exercises and tests.				
3. Monitor skills and competencies based on the exercise and test results.				

Personal Copy of: Dr. David Lanter

DSS04 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS04.07 Manage backup arrangements. Maintain availability of business-critical information.	**From**	**Description**	**Description**	**To**
			Test results of backup data	Internal
Activities				
1. Back up systems, applications, data and documentation according to a defined schedule, considering: • Frequency (monthly, weekly, daily, etc.) • Mode of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention) • Type of backup (e.g., full vs. incremental) • Type of media • Automated online backups • Data types (e.g., voice, optical) • Creation of logs • Critical end-user computing data (e.g., spreadsheets) • Physical and logical location of data sources • Security and access rights • Encryption				
2. Ensure that systems, applications, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. Consider requiring return of backups from third parties. Consider escrow or deposit arrangements.				
3. Define requirements for on-site and off-site storage of backup data that meet the business requirements. Consider the accessibility required to back up data.				
4. Roll out BCP awareness and training.				
5. Periodically test and refresh archived and backup data.				
Management Practice	**Inputs**		**Outputs**	
DSS04.08 Conduct post-resumption review. Assess the adequacy of the BCP following the successful resumption of business processes and services after a disruption.	**From**	**Description**	**Description**	**To**
			Post-resumption review report	Internal
			Approved changes to the plans	BAI06.01
Activities				
1. Assess adherence to the documented BCP.				
2. Determine the effectiveness of the plan, continuity capabilities, roles and responsibilities, skills and competencies, resilience to the incident, technical infrastructure, and organisational structures and relationships.				
3. Identify weaknesses or omissions in the plan and capabilities and make recommendations for improvement.				
4. Obtain management approval for any changes to the plan and apply via the enterprise change control process.				

DSS04 Related Guidance	
Related Standard	**Detailed Reference**
BS 25999:2007	Business Continuity Standard
ISO/IEC 20000	6.3 Service continuity and availability management
ISO/IEC 27002:2011	14. Business Continuity Management
ITIL V3 2011	Service Design, 4.6 IT Service Continuity Management

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

DSS05 Manage Security Services	Area: Management Domain: Deliver, Service and Support
Process Description Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges and perform security monitoring.	
Process Purpose Statement Minimise the business impact of operational information security vulnerabilities and incidents.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Networks and communications security meet business needs.	• Number of vulnerabilities discovered • Number of firewall breaches
2. Information processed on, stored on and transmitted by endpoint devices is protected.	• Percent of individuals receiving awareness training relating to use of endpoint devices • Number of incidents involving endpoint devices • Number of unauthorised devices detected on the network or in the end-user environment
3. All users are uniquely identifiable and have access rights in accordance with their business role.	• Average time between change and update of accounts • Number of accounts (vs. number of authorised users/staff)
4. Physical measures have been implemented to protect information from unauthorised access, damage and interference when being processed, stored or transmitted.	• Percent of periodic tests of environmental security devices • Average rating for physical security assessments • Number of physical security-related incidents
5. Electronic information is properly secured when stored, transmitted or destroyed.	• Number of incidents relating to unauthorised access to information

Personal Copy of: Dr. David Lanter

DSS05 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS05.01 Protect against malware.						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Manage network and connectivity security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Manage endpoint security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Manage user identity and logical access.						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS05.05 Manage physical access to IT assets.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Manage sensitive documents and output devices.											I					C	C	A			R					
DSS05.07 Monitor the infrastructure for security-related events.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

DSS05 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
DSS05.01 Protect against malware. Implement and maintain preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	**From**	**Description**	**Description**	**To**
			Malicious software prevention policy	APO01.04
			Evaluations of potential threats	APO12.02 APO12.03
Activities				
1. Communicate malicious software awareness and enforce prevention procedures and responsibilities.				
2. Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).				
3. Distribute all protection software centrally (version and patch-level) using centralised configuration and change management.				
4. Regularly review and evaluate information on new potential threats (e.g., reviewing vendors' products and services security advisories).				
5. Filter incoming traffic, such as email and downloads, to protect against unsolicited information (e.g., spyware, phishing emails).				
6. Conduct periodic training about malware in email and Internet usage. Train users to not install shared or unapproved software.				

Personal Copy of: Dr. David Lanter

DSS05 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS05.02 Manage network and connectivity security. Use security measures and related management procedures to protect information over all methods of connectivity.	**From**	**Description**	**Description**	**To**
	APO01.06	Data classification guidelines	Connectivity security policy	APO01.04
	APO09.03	SLAs	Results of penetration tests	MEA02.08
Activities				
1. Based on risk assessments and business requirements, establish and maintain a policy for security of connectivity.				
2. Allow only authorised devices to have access to corporate information and the enterprise network. Configure these devices to force password entry.				
3. Implement network filtering mechanisms, such as firewalls and intrusion detection software, with appropriate policies to control inbound and outbound traffic.				
4. Encrypt information in transit according to its classification.				
5. Apply approved security protocols to network connectivity.				
6. Configure network equipment in a secure manner.				
7. Establish trusted mechanisms to support the secure transmission and receipt of information.				
8. Carry out periodic penetration testing to determine adequacy of network protection.				
9. Carry out periodic testing of system security to determine adequacy of system protection.				
Management Practice	**Inputs**		**Outputs**	
DSS05.03 Manage endpoint security. Ensure that endpoints (e.g., laptop, desktop, server, and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements of the information processed, stored or transmitted.	**From**	**Description**	**Description**	**To**
	APO03.02	Information architecture model	Security policies for endpoint devices	APO01.04
	APO09.03	• OLAs • SLAs		
	BAI09.01	Results of physical inventory checks		
	DSS06.06	Reports of violations		
Activities				
1. Configure operating systems in a secure manner.				
2. Implement device lockdown mechanisms.				
3. Encrypt information in storage according to its classification.				
4. Manage remote access and control.				
5. Manage network configuration in a secure manner.				
6. Implement network traffic filtering on endpoint devices.				
7. Protect system integrity.				
8. Provide physical protection of endpoint devices.				
9. Dispose of endpoint devices securely.				

Personal Copy of: Dr. David Lanter

DSS05 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS05.04 Manage user identity and logical access. Ensure that all users have information access rights in accordance with their business requirements and co-ordinate with business units that manage their own access rights within business processes.	**From**	**Description**	**Description**	**To**
	APO01.02	Definition of IT-related roles and responsibilities	Approved user access rights	Internal
	APO03.02	Information architecture model	Results of reviews of user accounts and privileges	Internal
Activities				
1. Maintain user access rights in accordance with business function and process requirements. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.				
2. Uniquely identify all information processing activities by functional roles, co-ordinating with business units to ensure that all roles are consistently defined, including roles that are defined by the business itself within business process applications.				
3. Authenticate all access to information assets based on their security classification, co-ordinating with business units that manage authentication within applications used in business processes to ensure that authentication controls have been properly administered.				
4. Administer all changes to access rights (creation, modifications and deletions) to take effect at the appropriate time based only on approved and documented transactions authorised by designated management individuals.				
5. Segregate and manage privileged user accounts.				
6. Perform regular management review of all accounts and related privileges.				
7. Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT infrastructure, system operations, development and maintenance) are uniquely identifiable. Uniquely identify all information processing activities by user.				
8. Maintain an audit trail of access to information classified as highly sensitive.				
Management Practice	**Inputs**		**Outputs**	
DSS05.05 Manage physical access to IT assets. Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	**From**	**Description**	**Description**	**To**
			Approved access requests	Internal
			Access logs	DSS06.03
Activities				
1. Manage the requesting and granting of access to the computing facilities. Formal access requests are to be completed and authorised by management of the IT site, and the request records retained. The forms should specifically identify the areas to which the individual is granted access.				
2. Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities.				
3. Log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site.				
4. Instruct all personnel to display visible identification at all times. Prevent the issuance of identity cards or badges without proper authorisation.				
5. Require visitors to be escorted at all times while on-site. If an unaccompanied, unfamiliar individual who is not wearing staff identification is identified, alert security personnel.				
6. Restrict access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls, and security devices on interior and exterior doors. Ensure that the devices record entry and trigger an alarm in the event of unauthorised access. Examples of such devices include badges or key cards, keypads, closed-circuit television and biometric scanners.				
7. Conduct regular physical security awareness training.				

Personal Copy of: Dr. David Lanter

DSS05 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS05.06 Manage sensitive documents and output devices. Establish appropriate physical safeguards, accounting practices and inventory management over sensitive IT assets, such as special forms, negotiable instruments, special-purpose printers or security tokens.	**From**	**Description**	**Description**	**To**
	APO03.02	Information architecture model	Inventory of sensitive documents and devices	Internal
			Access privileges	Internal
Activities				
1. Establish procedures to govern the receipt, use, removal and disposal of special forms and output devices into, within and out of the enterprise.				
2. Assign access privileges to sensitive documents and output devices based on the least-privilege principle, balancing risk and business requirements.				
3. Establish an inventory of sensitive documents and output devices, and conduct regular reconciliations.				
4. Establish appropriate physical safeguards over special forms and sensitive devices.				
5. Destroy sensitive information and protect output devices (e.g., degaussing of electronic media, physical destruction of memory devices, making shredders or locked paper baskets available to destroy special forms and other confidential papers).				
Management Practice	**Inputs**		**Outputs**	
DSS05.07 Monitor the infrastructure for security-related events. Using intrusion detection tools, monitor the infrastructure for unauthorised access and ensure that any events are integrated with general event monitoring and incident management.	**From**	**Description**	**Description**	**To**
			Security event logs	Internal
			Security incident characteristics	Internal
			Security incident tickets	DSS02.02
Activities				
1. Log security-related events reported by infrastructure security monitoring tools, identifying the level of information to be recorded based on a consideration of risk. Retain them for an appropriate period to assist in future investigations.				
2. Define and communicate the nature and characteristics of potential security-related incidents so they can be easily recognised and their impacts understood to enable a commensurate response.				
3. Regularly review the event logs for potential incidents.				
4. Maintain a procedure for evidence collection in line with local forensic evidence rules and ensure that all staff are made aware of the requirements.				
5. Ensure that security incident tickets are created in a timely manner when monitoring identifies potential security incidents.				

DSS05 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 27002:2011	Code of practice for information security management
NIST SP800-53 Rev 1	Recommended Security Controls for USA Federal Information Systems
ITIL V3 2011	Service Operation, 4.5 Access Management

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

DSS06 Manage Business Process Controls	Area: Management Domain: Deliver, Service and Support
Process Description Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements and manage and operate adequate controls to ensure that information and information processing satisfy these requirements.	
Process Purpose Statement Maintain information integrity and the security of information assets handled within business processes in the enterprise or outsourced.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Coverage and effectiveness of key controls to meet business requirements for processing information are complete.	• Percent of completed inventory of critical processes and key controls • Percent of coverage of key controls within test plans • Number of incidents and audit report findings indicating failure of key controls
2. The inventory of roles, responsibilities and access rights is aligned with authorised business needs.	• Percent of business process roles with assigned access rights and levels of authority • Percent of business process roles with clear separation of duties • Number of incidents and audit findings due to access or separation of duties violations
3. Business transactions are retained completely and as required in logs.	• Percent of completeness of traceable transaction log • Number of incidents where transaction history cannot be recovered

Personal Copy of: Dr. David Lanter

DSS06 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS06.01 Align control activities embedded in business processes with enterprise objectives.		C	C	C	A	R					I	I				C	C	C			C		C	C		C
DSS06.02 Control the processing of information.		R	R	R	A	R					I	I				C	C	C			C		C	C		
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.			R		A	R						I			I	C	C	C			C		C	R		C
DSS06.04 Manage errors and exceptions.				I	I	A										C	C	I			C		R			
DSS06.05 Ensure traceability of information events and accountabilities.					C	A						I				C	C	C			C		C	C		
DSS06.06 Secure information assets.			C	C	C	A					I	I				C	C	C			C			C	C	C

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

DSS06 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
DSS06.01 Align control activities embedded in business processes with enterprise objectives. Continually assess and monitor the execution of the business process activities and related controls, based on enterprise risk, to ensure that the processing controls are aligned with business needs.	**From**	**Description**	**Description**	**To**
	APO01.06	• Data integrity procedures • Data classification guidelines	Results of processing effectiveness reviews	MEA02.04
			Root cause analyses and recommendations	BAI06.01 MEA02.04 MEA02.07 MEA02.08
Activities				
1. Identify and document control activities of key business processes to satisfy control requirements for strategic, operational, reporting and compliance objectives				
2. Prioritise control activities based on the inherent risk to the business and identify key controls.				
3. Ensure ownership of key control activities.				
4. Continually monitor control activities on an end-to-end basis to identify opportunities for improvement.				
5. Continually improve the design and operation of business process controls.				

Personal Copy of: Dr. David Lanter

DSS06 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS06.02 Control the processing of information. Operate the execution of the business process activities and related controls, based on enterprise risk, to ensure that information processing is valid, complete, accurate, timely, and secure (i.e., reflects legitimate and authorised business use).	**From**	**Description**	**Description**	**To**
	BAI05.05	Operation and use plan	Processing control reports	Internal
	BAI07.02	Migration plan		
Activities				
1. Create transactions by authorised individuals following established procedures, including, where appropriate, adequate segregation of duties regarding the origination and approval of these transactions.				
2. Authenticate the originator of transactions and verify that he/she has the authority to originate the transaction.				
3. Input transactions in a timely manner. Verify that transactions are accurate, complete and valid. Validate input data and edit or, where applicable, send back for correction as close to the point of origination as possible.				
4. Correct and resubmit data that were erroneously input without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.				
5. Maintain the integrity and validity of data throughout the processing cycle. Ensure that detection of erroneous transactions does not disrupt processing of valid transactions.				
6. Maintain the integrity of data during unexpected interruptions in business processing and confirm data integrity after processing failures.				
7. Handle output in an authorised manner, deliver to the appropriate recipient and protect the information during transmission. Verify the accuracy and completeness of the output.				
8. Before passing transaction data between internal applications and business/operational functions (inside or outside the enterprise), check for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.				
Management Practice	**Inputs**		**Outputs**	
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority. Manage the business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorise access to any information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	**From**	**Description**	**Description**	**To**
	EDM04.02	Assigned responsibilities for resource management	Allocated roles and responsibilities	APO01.02
	APO11.01	QMS roles, responsibilities and decision rights	Allocated levels of authority	APO01.02
	APO13.01	ISMS scope statement	Allocated access rights	APO07.04
	DSS05.05	Access logs		
Activities				
1. Allocate roles and responsibilities based on approved job descriptions and allocated business process activities.				
2. Allocate levels of authority for approval of transactions, limits and any other decisions relating to the business process, based on approved job roles.				
3. Allocate access rights and privileges based on only what is required to perform job activities, based on pre-defined job roles. Remove or revise access rights immediately if the job role changes or a staff member leaves the business process area. Periodically review to ensure that the access is appropriate for the current threats, risk, technology and business need.				
4. Allocate roles for sensitive activities so that there is a clear segregation of duties.				
5. Provide awareness and training regarding roles and responsibilities on a regular basis so that everyone understands their responsibilities; the importance of controls; and the integrity, confidentiality and privacy of company information in all its forms.				
6. Periodically review access control definitions, logs and exception reports to ensure that all access privileges are valid and aligned with current staff members and their allocated roles.				

Personal Copy of: Dr. David Lanter

DSS06 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS06.04 Manage errors and exceptions. Manage business process exceptions and errors and facilitate their correction. Include escalation of business process errors and exceptions and the execution of defined corrective actions. This provides assurance of the accuracy and integrity of the business information process.	**From**	**Description**	**Description**	**To**
			Evidence of error correction and remediation	MEA02.04
			Error reports and root cause analysis	Internal
Activities				
1. Define and maintain procedures to assign ownership, correct errors, override errors and handle out-of-balance conditions.				
2. Review errors, exceptions and deviations.				
3. Follow up, correct, approve and resubmit source documents and transactions.				
4. Maintain evidence of remedial actions.				
5. Report relevant business information process errors in a timely manner to perform root cause and trending analysis.				
Management Practice	**Inputs**		**Outputs**	
DSS06.05 Ensure traceability of Information events and accountabilities. Ensure that business information can be traced to the originating business event and accountable parties. This enables traceability of the information through its life cycle and related processes. This provides assurance that information that drives the business is reliable and has been processed in accordance with defined objectives.	**From**	**Description**	**Description**	**To**
			Retention requirements	Internal
			Record of transactions	Internal
Activities				
1. Define retention requirements, based on business requirements, to meet operational, financial reporting and compliance needs.				
2. Capture source information, supporting evidence and the record of transactions.				
3. Dispose of source information, supporting evidence and the record of transactions in accordance with the retention policy.				
Management Practice	**Inputs**		**Outputs**	
DSS06.06 Secure information assets. Secure information assets accessible by the business through approved methods, including information in electronic form (such as methods that create new assets in any form, portable media devices, user applications and storage devices), information in physical form (such as source documents or output reports) and information during transit. This benefits the business by providing end-to-end safeguarding of information.	**From**	**Description**	**Description**	**To**
			Reports of violations	DSS05.03
Activities				
1. Apply data classification and acceptable use and security policies and procedures to protect information assets under the control of the business.				
2. Provide acceptable use awareness and training.				
3. Restrict use, distribution and physical access of information according to its classification.				
4. Identify and implement processes, tools and techniques to reasonably verify compliance.				
5. Report to business and other stakeholders on violations and deviations.				

DSS06 Related Guidance	
Related Standard	**Detailed Reference**
None	

Personal Copy of: Dr. David Lanter

Monitor, Evaluate and Assess (MEA)

01 Monitor, evaluate and assess performance and conformance.

02 Monitor, evaluate and assess the system of internal control.

03 Monitor, evaluate and assess compliance with external requirements.

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

MEA01 Monitor, Evaluate and Assess Performance and Conformance	Area: Management Domain: Monitor, Evaluate and Assess
Process Description Collect, validate and evaluate business, IT and process goals and metrics. Monitor that processes are performing against agreed-on performance and conformance goals and metrics and provide reporting that is systematic and timely.	
Process Purpose Statement Provide transparency of performance and conformance and drive achievement of goals.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
15 IT compliance with internal policies	• Number of incidents related to non-compliance to policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices • Frequency of policies review and update
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Goals and metrics are approved by the stakeholders.	• Percent of goals and metrics approved by stakeholders
2. Processes are measured against agreed-on goals and metrics.	• Percent of processes with defined goals and metrics
3. The enterprise monitoring, assessing and informing approach is effective and operational.	• Percent of processes with effectiveness of goals and metrics reviewed and improved • Percent of critical processes monitored
4. Goals and metrics are integrated within enterprise monitoring systems.	• Percent of goals and metrics aligned to enterprise monitoring system
5. Process reporting on performance and conformance is useful and timely.	• Percent of performance reports delivered as scheduled

Personal Copy of: Dr. David Lanter

MEA01 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
MEA01.01 Establish a monitoring approach.		A	R	R	R	I	C		I						C	C	C	R	I	C	C	I	C	I	I	I
MEA01.02 Set performance and conformance targets.		I	I	I	A	R			I						C			C	C	R	R	I	R	I	I	I
MEA01.03 Collect and process performance and conformance data.					C	R			I						C			A		R	R	I	R	I	I	I
MEA01.04 Analyse and report performance.					A	R			C						C	C	C	C	C	R	R	C	R	C	C	C
MEA01.05 Ensure the implementation of corrective actions.	I	I	I	I	C	R			C						C	C	C	A	C	R	R	C	R	C	C	C

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

MEA01 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
MEA01.01 Establish a monitoring approach. Engage with stakeholders to establish and maintain a monitoring approach to define the objectives, scope and method for measuring business solution and service delivery and contribution to enterprise objectives. Integrate this approach with the corporate performance management system.	**From**	**Description**	**Description**	**To**
	EDM05.01	• Reporting and communications principles • Evaluation of enterprise reporting requirements	Monitoring requirements	Internal
			Approved monitoring goals and metrics	Internal
	EDM05.02	Rules for validating and approving mandatory reports		
	EDM05.03	Assessment of reporting effectiveness		
Activities				
1. Identify stakeholders (e.g., management, process owners and users).				
2. Engage with stakeholders and communicate the enterprise requirements and objectives for monitoring, aggregating and reporting, using common definitions (e.g., enterprise glossary, metadata and taxonomy), baselining and benchmarking.				
3. Align and continually maintain the monitoring and evaluation approach with the enterprise approach and the tools to be used for data gathering and enterprise reporting (e.g., business intelligence applications).				
4. Agree on the goals and metrics (e.g., conformance, performance, value, risk), taxonomy (classification and relationships between goals and metrics) and data (evidence) retention.				
5. Agree on a life cycle management and change control process for monitoring and reporting. Include improvement opportunities for reporting, metrics, approach, baselining and benchmarking.				
6. Request, prioritise and allocate resources for monitoring (consider appropriateness, efficiency, effectiveness and confidentiality).				
7. Periodically validate the approach used and identify new or changed stakeholders, requirements and resources.				

Personal Copy of: Dr. David Lanter

MEA01 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
MEA01.02 Set performance and conformance targets. Work with stakeholders to define, periodically review, update and approve performance and conformance targets within the performance measurement system.	**From**	**Description**	**Description**	**To**
	APO01.07	Performance goals and metrics for process improvement tracking	Monitoring targets	All APO All BAI All DSS All MEA
Activities				
1. Define and periodically review with stakeholders the goals and metrics to identify any significant missing items and define reasonableness of targets and tolerances.				
2. Communicate proposed changes to performance and conformance targets and tolerances (relating to metrics) with key due diligence stakeholders (e.g., legal, audit, HR, ethics, compliance, finance).				
3. Publish changed targets and tolerances to users of this information.				
4. Evaluate whether the goals and metrics are adequate, i.e., specific, measurable, achievable, relevant and time-bound (SMART).				
Management Practice	**Inputs**		**Outputs**	
MEA01.03 Collect and process performance and conformance data. Collect and process timely and accurate data aligned with enterprise approaches.	**From**	**Description**	**Description**	**To**
	APO01.07	Process capability assessments	Processed monitoring data	Internal
	APO05.04	Investment portfolio performance reports		
	APO09.04	Service level performance reports		
	APO10.05	Supplier compliance monitoring review results		
	BAI01.06	Results of programme performance reviews		
	BAI04.04	Availability, performance and reports		
	BAI05.05	Success measures and results		
	DSS01.05	Facilities assessment reports		
	DSS02.07	• Request fulfilment status and trends report • Incident status and trends report		
Activities				
1. Collect data from defined processes—automated, where possible.				
2. Assess efficiency (effort in relation to insight provided) and appropriateness (usefulness and meaning) and validate integrity (accuracy and completeness) of collected data.				
3. Aggregate data to support measurement of agreed-on metrics.				
4. Align aggregated data to the enterprise reporting approach and objectives.				
5. Use suitable tools and systems for the processing and format of data for analysis.				

Personal Copy of: Dr. David Lanter

MEA01 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
MEA01.04 Analyse and report performance. Periodically review and report performance against targets, using a method that provides a succinct all-around view of IT performance and fits within the enterprise monitoring system.	**From**	**Description**	**Description**	**To**
			Performance reports	EDM01.03 All APO All BAI All DSS All MEA
Activities				
1. Design process performance reports that are concise, easy to understand, and tailored to various management needs and audiences. Facilitate effective, timely decision making (e.g., scorecards, traffic light reports) and ensure that the cause and effect between goals and metrics are communicated in an understandable manner.				
2. Compare the performance values to internal targets and benchmarks and, where possible, to external benchmarks (industry and key competitors).				
3. Recommend changes to the goals and metrics, where appropriate.				
4. Distribute reports to the relevant stakeholders.				
5. Analyse the cause of deviations against targets, initiate remedial actions, assign responsibilities for remediation, and follow up. At appropriate times, review all deviations and search for root causes, where necessary. Document the issues for further guidance if the problem recurs. Document results.				
6. Where feasible, link achievement of performance targets to the organisational reward compensation system.				
Management Practice	**Inputs**		**Outputs**	
MEA01.05 Ensure the implementation of corrective actions. Assist stakeholders in identifying, initiating and tracking corrective actions to address anomalies.	**From**	**Description**	**Description**	**To**
	EDM05.02	Escalation guidelines	Remedial actions and assignments	All APO All BAI All DSS All MEA
	APO01.08	Non-compliance remedial actions	Status and results of actions	EDM01.03
Activities				
1. Review management responses, options and recommendations to address issues and major deviations.				
2. Ensure that the assignment of responsibility for corrective action is maintained.				
3. Track the results of actions committed.				
4. Report the results to the stakeholders.				

MEA01 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	6.2 Service reporting
ITIL V3 2011	Continual Service Improvement, 4.1 The 7-Step Improvement Process

Personal Copy of: Dr. David Lanter

MEA02 Monitor, Evaluate and Assess the System of Internal Control	Area: Management Domain: Monitor, Evaluate and Assess
Process Description Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organise and maintain standards for internal control assessment and assurance activities.	
Process Purpose Statement Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
15 IT compliance with internal policies	• Number of incidents related to non-compliance to policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices • Frequency of policies review and update
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Processes, resources and information meet enterprise internal control system requirements.	• Percent of processes with assured output meeting targets within tolerances • Percent of processes assured as compliant with internal control targets
2. All assurance initiatives are planned and executed effectively.	• Percent of assurance initiatives following approved assurance programme and plan standards
3. Independent assurance that the system of internal control is operational and effective is provided.	• Percent of processes receiving independent review
4. Internal control is established and deficiencies are identified and reported.	• Number of weaknesses identified by external qualification and certification reports • Number of major internal control breaches • Time between internal control deficiency occurrence and reporting

Personal Copy of: Dr. David Lanter

MEA02 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
MEA02.01 Monitor internal controls.		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
MEA02.02 Review business process controls effectiveness.	I	I	R	I	A	R	I				I	I				R	R	C			C		C	C	C	
MEA02.03 Perform control self-assessments.		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
MEA02.04 Identify and report control deficiencies.		I	C	I	C	R			R		I	I				R	R	A	I	R	R	R	R	R	R	R
MEA02.05 Ensure that assurance providers are independent and qualified.						R										A	A	R								
MEA02.06 Plan assurance initiatives.		A			C	R			C							C	C	R	C	C	C	C	C	C	C	C
MEA02.07 Scope assurance initiatives.				R	R	R			C							C	A	R	C	C	C	C	C	C	C	C
MEA02.08 Execute assurance initiatives.	I	I			C	R			C		I	I				C	A	R	C	C	C	C	C	C	C	C

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

MEA02 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
MEA02.01 Monitor internal controls. Continuously monitor, benchmark and improve the IT control environment and control framework to meet organisational objectives.	**From**	**Description**	**Description**	**To**
	APO12.04	Results of third-party risk assessments	Results of internal control monitoring and reviews	EDM01.03 All APO All BAI All DSS All MEA
	APO13.03	ISMS audit reports	Results of benchmarking and other evaluations	EDM01.03 All APO All BAI All DSS All MEA
	Outside COBIT	Industry standards and good practices		
Activities				
1. Perform internal control monitoring and evaluation activities based on organisational governance standards and industry-accepted frameworks and practices. Include monitoring and evaluation of the efficiency and effectiveness of managerial supervisory reviews.				
2. Consider independent evaluations of the internal control system (e.g., by internal audit or peers).				
3. Identify the boundaries of the IT internal control system (e.g., consider how organisational IT internal controls take into account outsourced and/or offshore development or production activities).				
4. Ensure that control activities are in place and exceptions are promptly reported, followed up and analysed, and appropriate corrective actions are prioritised and implemented according to the risk management profile (e.g., classify certain exceptions as a key risk and others as a non-key risk).				
5. Maintain the IT internal control system, considering ongoing changes in business and IT risk, the organisational control environment, relevant business and IT processes, and IT risk. If gaps exist, evaluate and recommend changes.				
6. Regularly evaluate the performance of the IT control framework, benchmarking against industry accepted standards and good practices. Consider formal adoption of a continuous improvement approach to internal control monitoring.				
7. Assess the status of external service providers' internal controls and confirm that service providers comply with legal and regulatory requirements and contractual obligations.				

Personal Copy of: Dr. David Lanter

MEA02 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
MEA02.02 Review business process controls effectiveness. Review the operation of controls, including a review of monitoring and test evidence, to ensure that controls within business processes operate effectively. Include activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centres, and network operations centres. This provides the business with the assurance of control effectiveness to meet requirements related to business, regulatory and social responsibilities.	**From**	**Description**	**Description**	**To**
	BAI05.06	Compliance audit results	Evidence of control effectiveness	Internal
	BAI05.07	Reviews of operational use		
Activities				
1. Understand and prioritise risk to organisational objectives.				
2. Identify key controls and develop a strategy suitable for validating controls.				
3. Identify information that will persuasively indicate whether the internal control environment is operating effectively.				
4. Develop and implement cost-effective procedures to determine that persuasive information is based on the information criteria.				
5. Maintain evidence of control effectiveness.				
Management Practice	**Inputs**		**Outputs**	
MEA02.03 Perform control self-assessments. Encourage management and process owners to take positive ownership of control improvement through a continuing programme of self-assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.	**From**	**Description**	**Description**	**To**
			Self-assessment plans and criteria	All APO All BAI All DSS All MEA
			Results of self-assessments	Internal
			Results of reviews of self-assessments	EDM01.03 All APO All BAI All DSS All MEA
Activities				
1. Maintain plans and scope and identify evaluation criteria for conducting self-assessments. Plan the communication of results of the self-assessment process to business, IT and general management and the board. Consider internal audit standards in the design of self-assessments.				
2. Determine the frequency of periodic self-assessments, considering the overall effectiveness and efficiency of ongoing monitoring.				
3. Assign responsibility for self-assessment to appropriate individuals to ensure objectivity and competence.				
4. Provide for independent reviews to ensure objectivity of the self-assessment and enable the sharing of internal control good practices from other enterprises.				
5. Compare the results of the self-assessments against industry standards and good practices.				
6. Summarise and report outcomes of self-assessments and benchmarking for remedial actions.				
7. Define an agreed-on, consistent approach for performing control self-assessments and co-ordinating with internal and external auditors.				

Personal Copy of: Dr. David Lanter

MEA02 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
MEA02.04 Identify and report control deficiencies. Identify control deficiencies and analyse and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.	**From**	**Description**	**Description**	**To**
	APO11.05	Root causes of quality delivery failures	Control deficiencies	All APO All BAI All DSS All MEA
	APO12.06	Risk-related root causes		
	DSS06.01	• Root cause analyses and recommendations • Results of processing effectiveness reviews	Remedial actions	All APO All BAI All DSS All MEA
	DSS06.04	Evidence of error correction and remediation		
Activities				
1. Identify, report and log control exceptions, and assign responsibility for resolving them and reporting on the status.				
2. Consider related enterprise risk to establish thresholds for escalation of control exceptions and breakdowns.				
3. Communicate procedures for escalation of control exceptions, root cause analysis, and reporting to process owners and IT stakeholders.				
4. Decide which control exceptions should be communicated to the individual responsible for the function and which exceptions should be escalated. Inform affected process owners and stakeholders.				
5. Follow up on all exceptions to ensure that agreed-on actions have been addressed.				
6. Identify, initiate, track and implement remedial actions arising from control assessments and reporting.				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
MEA02.05 Ensure that assurance providers are independent and qualified. Ensure that the entities performing assurance are independent from the function, groups or organisations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.			Results of assurance provider evaluations	Internal
Activities				
1. Establish adherence to applicable codes of ethics and standards (e.g., Code of Professional Ethics of ISACA) and (industry- and geography-specific) assurance standards, e.g., IT Audit and Assurance Standards of ISACA and the International Auditing and Assurance Standards Board's (IAASB's) International Framework for Assurance Engagements (IAASB Assurance Framework).				
2. Establish independence of assurance providers.				
3. Establish competency and qualification of assurance providers.				
Management Practice	**Inputs**		**Outputs**	
MEA02.06 Plan assurance initiatives. Plan assurance initiatives based on enterprise objectives and strategic priorities, inherent risk, resource constraints, and sufficient knowledge of the enterprise.	**From**	**Description**	**Description**	**To**
	BAI01.05	Programme audit plans	High-level assessments	Internal
	DSS01.02	Independent assurance plans	Assurance plans	EDM01.03 All APO All BAI All DSS All MEA
			Assessment criteria	Internal
Activities				
1. Determine the intended users of the assurance initiative output and the object of the review.				
2. Perform a high-level risk assessment and/or assessment of process capability to diagnose risk and identify critical IT processes.				
3. Select, customise and reach agreement on the control objectives for critical processes that will be the basis for the control assessment.				

Personal Copy of: Dr. David Lanter

MEA02 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
MEA02.07 Scope assurance initiatives. Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.	**From**	**Description**	**Description**	**To**
	APO11.05	Root causes of quality delivery failures	Assurance review scope	Internal
	APO12.06	Risk-related root causes	Engagement plan	Internal
	DSS06.01	Root cause analyses and recommendations	Assurance review practices	Internal
	MEA03.04	Reports of non-compliance issues and root causes		
Activities				
1. Define the actual scope by identifying the enterprise and IT goals for the environment under review, the set of IT processes and resources, and all the relevant auditable entities within the enterprise and external to the enterprise (e.g., service providers), if applicable.				
2. Define the engagement plan and resource requirements.				
3. Define practices for gathering and evaluating information from process(es) under review to identify controls to be validated, and current findings (both positive assurance and any deficiencies) for risk evaluation.				
4. Define practices to validate control design and outcomes and determine whether the level of effectiveness supports acceptable risk (required by organisational or process risk assessment).				
5. Where control effectiveness is not acceptable, define practices to identify residual risk (in preparation for reporting).				
Management Practice	**Inputs**		**Outputs**	
MEA02.08 Execute assurance initiatives. Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risk.	**From**	**Description**	**Description**	**To**
	APO11.05	Root causes of quality delivery failures	Refined scope	All APO All BAI All DSS All MEA
	APO12.04	Risk analysis and risk profile reports for stakeholders	Assurance review results	EDM05.01 EDM05.03 All APO All BAI All DSS All MEA
	APO12.06	Risk-related root causes		
	DSS05.02	Results of penetration tests		
	DSS06.01	Root cause analyses and recommendations	Assurance review report	EDM05.03 All APO All BAI All DSS All MEA
	MEA03.03	Identified compliance gaps		
Activities				
1. Refine the understanding of the IT assurance subject.				
2. Refine the scope of key control objectives for the IT assurance subject.				
3. Test the effectiveness of the control design of the key control objectives.				
4. Alternatively/additionally test the outcome of the key control objectives.				
5. Document the impact of control weaknesses.				
6. Communicate with management during execution of the initiative so that there is a clear understanding of the work performed and agreement on and acceptance of the preliminary findings and recommendations.				
7. Supervise the assurance activities and make sure the work done is complete, meets objectives and is of an acceptable quality.				
8. Provide management with a report (aligned with the terms of reference, scope and agreed-on reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.				

MEA02 Related Guidance	
Related Standard	**Detailed Reference**
None	

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter

MEA03 Monitor, Evaluate and Assess Compliance with External Requirements	Area: Management Domain: Monitor, Evaluate and Assess
Process Description Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.	
Process Purpose Statement Ensure that the enterprise is compliant with all applicable external requirements.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. All external compliance requirements are identified.	• Average time lag between identification of external compliance issues and resolution • Frequency of compliance reviews
2. External compliance requirements are adequately addressed.	• Number of critical non-compliance issues identified per year • Percent of process owners signing off, confirming compliance

MEA03 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
MEA03.01 Identify external compliance requirements.					A	R										R	R	R								R
MEA03.02 Optimise response to external requirements.		R	R	R	A	R	I		R							R	R	R	I	R	R	R	R	R	R	R
MEA03.03 Confirm external compliance.	I	R	R	R	R	R	I	I	C							A	I	R	C	C	C	C	C	C	C	R
MEA03.04 Obtain assurance of external compliance.	I	I	I	I	C	C	I		C							C	A	R	C	C	C	C	C	C	C	C

Note: Some governance and management practices produce outputs that serve as inputs to many practices. Those outputs are detailed in **figure 11**. Please refer to **figure 11** to ensure completeness when working with the practices that follow.

Personal Copy of: Dr. David Lanter

MEA03 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
MEA03.01 Identify external compliance requirements. On a continuous basis, identify and monitor for changes in local and international laws, regulations and other external requirements that must be complied with from an IT perspective.	**From**	**Description**	**Description**	**To**
	Outside COBIT	Legal and regulatory compliance requirements	Compliance requirements register	Internal
			Log of required compliance actions	Internal
Activities				
1. Assign responsibility for identifying and monitoring any changes of legal, regulatory and other external contractual requirements relevant to the use of IT resources and the processing of information within the business and IT operations of the enterprise.				
2. Identify and assess all potential compliance requirements and the impact on IT activities in areas such as data flow, privacy, internal controls, financial reporting, industry-specific regulations, intellectual property, health and safety.				
3. Assess the impact of IT-related legal and regulatory requirements on third-party contracts related to IT operations, service providers and business trading partners.				
4. Obtain independent counsel, where appropriate, on changes to applicable laws, regulations and standards.				
5. Maintain an up-to-date log of all relevant legal, regulatory and contractual requirements, their impact and required actions.				
6. Maintain a harmonised and integrated overall register of external compliance requirements for the enterprise.				
Management Practice	**Inputs**		**Outputs**	
MEA03.02 Optimise response to external requirements. Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and good practice guidance for adoption and adaptation.	**From**	**Description**	**Description**	**To**
			Updated policies, principles, procedures and standards	APO01.07 APO01.08
			Communications of changed compliance requirements	EDM01.01 All APO All BAI All DSS All MEA
Activities				
1. Regularly review and adjust policies, principles, standards, procedures and methodologies for their effectiveness in ensuring necessary compliance and addressing enterprise risk using internal and external experts, as required.				
2. Communicate new and changed requirements to all relevant personnel.				
Management Practice	**Inputs**		**Outputs**	
MEA03.03 Confirm external compliance. Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements.	**From**	**Description**	**Description**	**To**
	BAI05.06	Compliance audit results	Identified compliance gaps	MEA02.08
	BAI09.05	Results of installed licence audits	Compliance confirmations	EDM01.03
	BAI10.05	Licence deviations		
	DSS01.04	Insurance policy reports		
Activities				
1. Regularly evaluate organisational policies, standards, procedures and methodologies in all functions of the enterprise to ensure compliance with relevant legal and regulatory requirements in relation to the processing of information.				
2. Address compliance gaps in policies, standards and procedures on a timely basis.				
3. Periodically evaluate business and IT processes and activities to ensure adherence to applicable legal, regulatory and contractual requirements.				
4. Regularly review for recurring patterns of compliance failures. Where necessary, improve policies, standards, procedures, methodologies, and associated processes and activities.				

Personal Copy of: Dr. David Lanter

MEA03 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
MEA03.04 Obtain assurance of external compliance. Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.	**From**	**Description**	**Description**	**To**
	EDM05.02	Rules for validating and approving mandatory reports	Compliance assurance reports	EDM01.03
	EDM05.03	Assessment of reporting effectiveness	Reports of non-compliance issues and root causes	EDM01.03 MEA02.07
Activities				
1. Obtain regular confirmation of compliance with internal policies from business and IT process owners and unit heads.				
2. Perform regular (and, where appropriate, independent) internal and external reviews to assess levels of compliance.				
3. If required, obtain assertions from third-party IT service providers on levels of their compliance with applicable laws and regulations.				
4. If required, obtain assertions from business partners on levels of their compliance with applicable laws and regulations as they relate to intercompany electronic transactions.				
5. Monitor and report on non-compliance issues and, where necessary, investigate the root cause.				
6. Integrate reporting on legal, regulatory and contractual requirements at an enterprisewide level, involving all business units.				

MEA03 Related Guidance	
Related Standard	**Detailed Reference**
None	

Personal Copy of: Dr. David Lanter

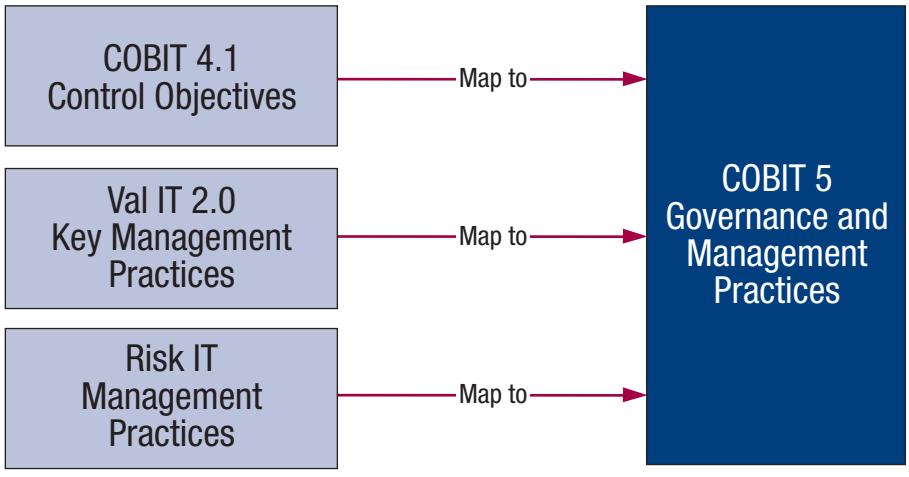
Page intentionally left blank

Personal Copy of: Dr. David Lanter

Appendix A
Mapping Between COBIT 5 and Legacy ISACA Frameworks

Figure 13 shows the ISACA frameworks included in COBIT 5.

Figure 13—ISACA Frameworks Included in COBIT 5



The mapping of COBIT 4.1, Val IT and Risk IT components to COBIT 5 is shown in **figures 14**, **15** and **16**.

Figure 14—COBIT 4.1 Control Objectives Mapped to COBIT 5

COBIT 4.1 Control Objective		Covered in COBIT 5 by:
AC1	Source Data Preparation and Authorisation	DSS06.02; DSS06.03; BAI03.02; BAI03.03; BAI03.05; BAI03.07
AC2	Source Data Collection and Entry	DSS06.02
AC3	Accuracy, Completeness and Authenticity Checks	DSS06.02
AC4	Processing Integrity and Validity	DSS06.02
AC5	Output Review, Reconciliation and Error Handling	DSS06.02
AC6	Transaction Authentication and Integrity	DSS06.02
PO1.1	IT Value Management	EDM02
PO1.2	Business-IT Alignment	APO02.01
PO1.3	Assessment of Current Capability and Performance	APO02.02
PO1.4	IT Strategic Plan	APO02.03-05
PO1.5	IT Tactical Plans	APO02.05
PO1.6	IT Portfolio Management	APO05.05
PO2.1	Enterprise Information Architecture Model	APO03.02
PO2.2	Enterprise Data Dictionary and Data Syntax Rules	APO03.02
PO2.3	Data Classification Scheme	APO03.02
PO2.4	Integrity Management	APO01.06
PO3.1	Technological Direction Planning	APO02.03; APO04.03
PO3.2	Technical Infrastructure Plan	APO02.03-05; APO04.03-05
PO3.3	Monitor Future Trends and Regulations	EDM01.01; APO04.03
PO3.4	Technology Standards	APO03.05
PO3.5	IT Architecture Board	APO01.01
PO4.1	IT Process Framework	APO01.03; APO01.07
PO4.2	IT Strategy Committee	APO01.01
PO4.3	IT Steering Committee	APO01.01
PO4.4	Organisational Placement of the IT Function	APO01.05

Personal Copy of: Dr. David Lanter

Figure 14—COBIT 4.1 Control Objectives Mapped to COBIT 5 *(cont.)*		
COBIT 4.1 Control Objective		**Covered in COBIT 5 by:**
P04.5	IT Organisational Structure	APO01.01
P04.6	Establishment of Roles and Responsibilities	APO01.02
P04.7	Responsibility for IT Quality Assurance	APO11.01
P04.8	Responsibility for Risk, Security and Compliance	Deleted—these specific roles are no longer explicitly specified as a practice.
P04.9	Data and System Ownership	APO01.06
P04.10	Supervision	APO01.02
P04.11	Segregation of Duties	APO01.02
P04.12	IT Staffing	APO07.01
P04.13	Key IT Personnel	APO07.02
P04.14	Contracted Staff Policies and Procedures	APO07.06
P04.15	Relationships	APO01.01
P05.1	Financial Management Framework	APO06.01
P05.2	Prioritisation Within IT Budget	APO06.02
P05.3	IT Budgeting	APO06.03
P05.4	Cost Management	APO06.04-05
P05.5	Benefit Management	APO05.06
P06.1	IT Policy and Control Environment	APO01.03
P06.2	Enterprise IT Risk and Control Framework	EDM03.02; APO01.03
P06.3	IT Policies Management	APO01.03; APO01.08
P06.4	Policy, Standards and Procedures Rollout	APO01.03; APO01.08
P06.5	Communication of IT Objectives and Direction	APO01.04
P07.1	Personnel Recruitment and Retention	APO07.01; APO07.05
P07.2	Personnel Competencies	APO07.03
P07.3	Staffing of Roles	APO01.02; APO07.01
P07.4	Personnel Training	APO07.03
P07.5	Dependence Upon Individuals	APO07.02
P07.6	Personnel Clearance Procedures	APO07.01; APO07.06
P07.7	Employee Job Performance Evaluation	APO07.04
P07.8	Job Change and Termination	APO07.01
P08.1	Quality Management System	APO11.01
P08.2	IT Standards and Quality Practices	APO11.02
P08.3	Development and Acquisition Standards	APO11.02; APO11.05
P08.4	Customer Focus	APO11.03
P08.5	Continuous Improvement	APO11.06
P08.6	Quality Measurement, Monitoring and Review	APO11.04
P09.1	IT Risk Management Framework	EDM03.02; APO01.03
P09.2	Establishment of Risk Context	APO12.03
P09.3	Event Identification	APO12.01; APO12.03
P09.4	Risk Assessment	APO12.02; APO12.04
P09.5	Risk Response	APO12.06
P09.6	Maintenance and Monitoring of a Risk Action Plan	APO12.04-05
P010.1	Programme Management Framework	BAI01.01
P010.2	Project Management Framework	BAI01.01
P010.3	Project Management Approach	BAI01.01

Personal Copy of: Dr. David Lanter

Figure 14—COBIT 4.1 Control Objectives Mapped to COBIT 5 *(cont.)*		
COBIT 4.1 Control Objective		**Covered in COBIT 5 by:**
PO10.4	Stakeholder Commitment	BAI01.03
PO10.5	Project Scope Statement	BAI01.07
PO10.6	Project Phase Initiation	BAI01.07
PO10.7	Integrated Project Plan	BAI01.08
PO10.8	Project Resources	BAI01.08
PO10.9	Project Risk Management	BAI01.10
PO10.10	Project Quality Plan	BAI01.09
PO10.11	Project Change Control	BAI01.11
PO10.12	Project Planning of Assurance Methods	BAI01.08
PO10.13	Project Performance Measurement, Reporting and Monitoring	BAI01.06; BAI01.11
PO10.14	Project Closure	BAI01.13
AI1.1	Definition and Maintenance of Business Functional and Technical Requirements	BAI02.01
AI1.2	Risk Analysis Report	BAI02.03
AI1.3	Feasibility Study and Formulation of Alternative Courses of Action	BAI02.02
AI1.4	Requirements and Feasibility Decision and Approval	BAI02.04
AI2.1	High-level Design	BAI03.01
AI2.2	Detailed Design	BAI03.02
AI2.3	Application Control and Auditability	BAI03.05
AI2.4	Application Security and Availability	BAI03.01-03; BAI03.05
AI2.5	Configuration and Implementation of Acquired Application Software	BAI03.03; BAI03.05
AI2.6	Major Upgrades to Existing Systems	BAI03.10
AI2.7	Development of Application Software	BAI03.03-04
AI2.8	Software Quality Assurance	BAI03.06
AI2.9	Applications Requirements Management	BAI03.09
AI2.10	Application Software Maintenance	BAI03.10
AI3.1	Technological Infrastructure Acquisition Plan	BAI03.04
AI3.2	Infrastructure Resource Protection and Availability	BAI03.03; DSS02.03
AI3.3	Infrastructure Maintenance	BAI03.10
AI3.4	Feasibility Test Environment	BAI03.07-08
AI4.1	Planning for Operational Solutions	BAI05.05
AI4.2	Knowledge Transfer to Business Management	BAI08.01-04
AI4.3	Knowledge Transfer to End Users	BAI08.01-04
AI4.4	Knowledge Transfer to Operations and Support Staff	BAI08.01-04
AI5.1	Procurement Control	BAI03.04
AI5.2	Supplier Contract Management	APO10.01; APO10.03
AI5.3	Supplier Selection	APO10.02
AI5.4	IT Resources Acquisition	APO10.03
AI6.1	Change Standards and Procedures	BAI06.01-04
AI6.2	Impact Assessment, Prioritisation and Authorisation	BAI06.01
AI6.3	Emergency Changes	BAI06.02
AI6.4	Change Status Tracking and Reporting	BAI06.03
AI6.5	Change Closure and Documentation	BAI06.04
AI7.1	Training	BAI05.05
AI7.2	Test Plan	BAI07.01; BAI07.03

Personal Copy of: Dr. David Lanter

Figure 14—COBIT 4.1 Control Objectives Mapped to COBIT 5 *(cont.)*		
COBIT 4.1 Control Objective		**Covered in COBIT 5 by:**
AI7.3	Implementation Plan	BAI07.01
AI7.4	Test Environment	BAI07.04
AI7.5	System and Data Conversion	BAI07.02
AI7.6	Testing of Changes	BAI07.05
AI7.7	Final Acceptance Test	BAI07.05
AI7.8	Promotion to Production	BAI07.06
AI7.9	Post-implementation Review	BAI07.08
DS1.1	Service Level Management Framework	APO09.01-05
DS1.2	Definition of Services	APO09.01-02
DS1.3	Service Level Agreements	APO09.03
DS1.4	Operating Level Agreements	APO09.03
DS1.5	Monitoring and Reporting of Service Level Achievements	APO09.04
DS1.6	Review of Service Level Agreements and Contracts	APO09.05
DS2.1	Identification of All Supplier Relationships	APO10.01
DS2.2	Supplier Relationship Management	APO10.03
DS2.3	Supplier Risk Management	APO10.04
DS2.4	Supplier Performance Monitoring	APO10.05
DS3.1	Performance and Capacity Planning	BAI04.03
DS3.2	Current Performance and Capacity	BAI04.01-02
DS3.3	Future Performance and Capacity	BAI04.01
DS3.4	IT Resources Availability	BAI04.05
DS3.5	Monitoring and Reporting	BAI04.04
DS4.1	IT Continuity Framework	DSS04.01-02
DS4.2	IT Continuity Plans	DSS04.03
DS4.3	Critical IT Resources	DSS04.04
DS4.4	Maintenance of the IT Continuity Plan	DSS04.02; DSS04.05
DS4.5	Testing of the IT Continuity Plan	DSS04.04
DS4.6	IT Continuity Plan Training	DSS04.06
DS4.7	Distribution of the IT Continuity Plan	DSS04.03
DS4.8	IT Services Recovery and Resumption	DSS04.03
DS4.9	Offsite Backup Storage	DSS04.07
DS4.10	Post-resumption Review	DSS04.08
DS5.1	Management of IT Security	APO13.01; APO13.03
DS5.2	IT Security Plan	APO13.02
DS5.3	Identity Management	DSS05.04
DS5.4	User Account Management	DSS05.04
DS5.5	Security Testing, Surveillance and Monitoring	DSS05.07
DS5.6	Security Incident Definition	DSS02.01
DS5.7	Protection of Security Technology	DSS05.05
DS5.8	Cryptographic Key Management	DSS05.03
DS5.9	Malicious Software Prevention, Detection and Correction	DSS05.01
DS5.10	Network Security	DSS05.02
DS5.11	Exchange of Sensitive Data	DSS05.02
DS6.1	Definition of Services	APO06.04
DS6.2	IT Accounting	APO06.01

Personal Copy of: Dr. David Lanter

Figure 14—COBIT 4.1 Control Objectives Mapped to COBIT 5 *(cont.)*		
COBIT 4.1 Control Objective		**Covered in COBIT 5 by:**
DS6.3	Cost Modelling and Charging	APO06.04
DS6.4	Cost Model Maintenance	APO06.04
DS7.1	Identification of Education and Training Needs	APO07.03
DS7.2	Delivery of Training and Education	APO07.03
DS7.3	Evaluation of Training Received	APO07.03
DS8.1	Service Desk	Deleted—ITIL 3 does not refer to Service Desk as a process.
DS8.2	Registration of Customer Queries	DSS02.01-03
DS8.3	Incident Escalation	DSS02.04
DS8.4	Incident Closure	DSS02.05-06
DS8.5	Reporting and Trend Analysis	DSS02.07
DS9.1	Configuration Repository and Baseline	BAI10.01-02; BAI10.04; DSS02.01
DS9.2	Identification and Maintenance of Configuration Items	BAI10.03
DS9.3	Configuration Integrity Review	BAI10.04-05; DSS02.05
DS10.1	Identification and Classification of Problems	DSS03.01
DS10.2	Problem Tracking and Resolution	DSS03.02
DS10.3	Problem Closure	DSS03.03-04
DS10.4	Integration of Configuration, Incident and Problem Management	DSS03.05
DS11.1	Business Requirements for Data Management	DSS01.01
DS11.2	Storage and Retention Arrangements	DSS04.08; DSS06.04
DS11.3	Media Library Management System	DSS04.08
DS11.4	Disposal	DSS05.06; DSS06.05-06
DS11.5	Backup and Restoration	DSS04.08
DS11.6	Security Requirements for Data Management	DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
DS12.1	Site Selection and Layout	DSS01.04-05; DSS05.05
DS12.2	Physical Security Measures	DSS05.05
DS12.3	Physical Access	DSS05.05
DS12.4	Protection Against Environmental Factors	DSS01.04
DS12.5	Physical Facilities Management	DSS01.05
DS13.1	Operations Procedures and Instructions	DSS01.01
DS13.2	Job Scheduling	DSS01.01
DS13.3	IT Infrastructure Monitoring	DSS01.03
DS13.4	Sensitive Documents and Output Devices	DSS05.06
DS13.5	Preventive Maintenance for Hardware	BAI09.02
ME1.1	Monitoring Approach	MEA01.01
ME1.2	Definition and Collection of Monitoring Data	MEA01.02-03
ME1.3	Monitoring Method	MEA01.03
ME1.4	Performance Assessment	MEA01.04
ME1.5	Board and Executive Reporting	MEA01.04
ME1.6	Remedial Actions	MEA01.05
ME2.1	Monitoring of Internal Control Framework	MEA02.01-02
ME2.2	Supervisory Review	MEA02.01
ME2.3	Control Exceptions	MEA02.04
ME2.4	Control Self-assessment	MEA02.03
ME2.5	Assurance of Internal Control	MEA02.06-08
ME2.6	Internal Control at Third Parties	MEA02.01

Personal Copy of: Dr. David Lanter

Figure 14—COBIT 4.1 Control Objectives Mapped to COBIT 5 *(cont.)*		
COBIT 4.1 Control Objective		**Covered in COBIT 5 by:**
ME2.7	Remedial Actions	MEA02.04
ME3.1	Identification of External Legal, Regulatory and Contractual Compliance Requirements	MEA03.01
ME3.2	Optimisation of Response to External Requirements	MEA03.02
ME3.3	Evaluation of Compliance With External Requirements	MEA03.03
ME3.4	Positive Assurance of Compliance	MEA03.04
ME3.5	Integrated Reporting	MEA03.04
ME4.1	Establishment of an IT Governance Framework	EDM01
ME4.2	Strategic Alignment	Deleted—In COBIT 5, alignment is considered to be the result of all governance and management activities.
ME4.3	Value Delivery	EDM02
ME4.4	Resource Management	EDM04
ME4.5	Risk Management	EDM03
ME4.6	Performance Measurement	EDM01.03; EDM02.03; EDM03.03; EDM04.03
ME4.7	Independent Assurance	MEA02.05-07; MEA02-08

Figure 15—Val IT 2.0 Key Management Practices Covered by COBIT 5		
Val IT 2.0 Key Management Practice		**Covered in COBIT 5 by:**
VG1.1	Develop an understanding of the significance of IT and the role of governance.	EDM01.01
VG1.2	Establish effective reporting lines.	EDM01.01
VG1.3	Establish a leadership forum.	EDM01.02; APO01.01
VG1.4	Define value for the enterprise.	EDM02.02
VG1.5	Ensure alignment and integration of business and IT strategies with key business goals.	APO02.01
VG2.1	Define the value governance framework.	EDM01.02
VG2.2	Assess the quality and coverage of current processes.	APO01.07
VG2.3	Identify and prioritise process requirements.	APO01.07
VG2.4	Define and document the processes.	APO01.07
VG2.5	Establish, implement and communicate roles, responsibilities and accountabilities.	APO01.02
VG2.6	Establish organisational structures.	EDM01.02; APO01.02
VG3.1	Define portfolio types.	EDM02.02
VG3.2	Define categories (within portfolios).	EDM02.02
VG3.3	Develop and communicate evaluation criteria (for each category).	EDM02.02
VG3.4	Assign weightings to criteria.	EDM02.02
VG3.5	Define requirements for stage-gates and other reviews (for each category).	EDM02.02
VG4.1	Review current enterprise budgeting practices.	APO06.03
VG4.2	Determine value management financial planning practice requirements.	APO06.01
VG4.3	Identify changes required.	APO06.01
VG4.4	Implement optimal financial planning practices for value management.	APO06.01
VG5.1	Identify key metrics.	EDM02.03
VG5.2	Define information capture processes and approaches.	EDM02.03
VG5.3	Define reporting methods and techniques.	EDM02.03
VG5.4	Identify and monitor performance improvement actions.	EDM02.03
VG6.1	Implement lessons learned.	EDM02.03
PM1.1	Review and ensure clarity of the business strategy and goals.	APO05.01

Personal Copy of: Dr. David Lanter

Figure 15—Val IT 2.0 Key Management Practices Covered by COBIT 5 *(cont.)*		
Val IT 2.0 Key Management Practice		**Covered in COBIT 5 by:**
PM1.2	Identify opportunities for IT to influence and support the business strategy.	APO05.01
PM1.3	Define an appropriate investment mix.	APO05.01
PM1.4	Translate the business strategy and goals into IT strategy and goals.	APO05.01
PM2.1	Determine overall investment funds.	APO05.02
PM3.1	Create and maintain an inventory of business human resources.	APO07.01
PM3.2	Understand the current and future demand (for business human resources).	APO07.01
PM3.2	Identify shortfalls (between current and future business human resource demand).	APO07.01
PM3.4	Create and maintain tactical plans (for business human resources).	APO07.01
PM3.5	Monitor, review and adjust (business function allocation and staffing).	APO07.05
PM3.6	Create and maintain an inventory of IT human resources.	APO07.05
PM3.7	Understand the current and future demand (for IT human resources).	APO07.05
PM3.8	Identify shortfalls (between current and future IT human resource demand).	APO07.05
PM3.9	Create and maintain tactical plans (for IT human resources).	APO07.05
PM3.10	Monitor, review and adjust (IT function allocation and staffing).	APO07.05
PM4.1	Evaluate and assign relative scores to programme business cases.	APO05.03
PM4.2	Create an overall investment portfolio view.	APO05.03
PM4.3	Make and communicate investment decisions.	APO05.03
PM4.4	Specify stage-gates and allocate funds to selected programmes.	APO05.03
PM4.5	Adjust business targets, forecasts and budgets.	APO05.03
PM5.1	Monitor and report on investment portfolio performance.	APO05.04
PM6.1	Optimise investment portfolio performance.	APO05.04
PM6.2	Reprioritise the investment portfolio.	APO05.04
IM1.1	Recognise investment opportunities.	APO05.03
IM1.2	Develop the initial programme concept business case.	BAI01.02
IM1.3	Evaluate the initial programme concept business case.	APO05.03
IM2.1	Develop a clear and complete understanding of the candidate programme.	BAI01.02
IM2.2	Perform analysis of the alternatives.	BAI01.02
IM3.1	Develop the programme plan.	BAI01.04
IM4.1	Identify full life-cycle costs and benefits.	BAI01.04
IM4.2	Develop a benefits realisation plan.	BAI01.04
IM4.3	Perform appropriate reviews and obtain sign-offs.	BAI01.03-04
IM5.1	Develop the detailed programme business case.	BAI01.02
IM5.2	Assign clear accountability and ownership.	BAI01.02
IM5.3	Perform appropriate reviews and obtain sign-offs.	BAI01.02-03
IM6.1	Plan projects, and resource and launch the programme.	BAI01.05
IM6.2	Manage the programme.	BAI01.05
IM6.3	Track and manage benefits.	BAI01.05
IM7.1	Update operational IT portfolios.	APO05.05
IM8.1	Update the business case.	BAI01.04
IM9.1	Monitor and report on programme (solution delivery) performance.	BAI01.06
IM9.2	Monitor and report on business (benefit/outcome) performance.	BAI01.06
IM9.3	Monitor and report on operational (service delivery) performance.	BAI01.06
IM10.1	Retire the programme.	BAI10.14

Personal Copy of: Dr. David Lanter

Figure 16—Risk IT Key Management Practices Covered by COBIT 5		
Risk IT Key Management Practice		**Covered in COBIT 5 by:**
RG1.1	Perform enterprise IT risk assessment.	EDM03.01; APO12.02-03
RG1.2	Propose IT risk tolerance thresholds.	EDM03.01
RG1.3	Approve IT risk tolerance.	EDM03.01-02
RG1.4	Align IT risk policy.	EDM03.01-02
RG1.5	Promote IT risk-aware culture.	EDM03.02
RG1.6	Encourage effective communication of IT risk.	EDM03.03
RG2.1	Establish and maintain accountability for IT risk management.	EDM03.02
RG2.2	Co-ordinate IT risk strategy and business risk strategy.	EDM03.01-02
RG2.3	Adapt IT risk practices to enterprise risk practices.	EDM03.01-02
RG2.4	Provide adequate resources for IT risk management.	EDM04.01; APO07.01; APO07.03
RG2.5	Provide independent assurance over IT risk management.	EDM03.03
RG3.1	Gain management buy-in for the IT risk analysis approach.	EDM01.01-02; EDM03.02
RG3.2	Approve IT risk analysis.	EDM03.01
RG3.3	Embed IT risk considerations in strategic business decision making.	EDM03.01
RG3.4	Accept IT risk.	EDM03.01
RG3.5	Prioritise IT risk response activities.	EDM03.02
RE1.1	Establish and maintain a model for data collection.	APO12.01
RE1.2	Collect data on the operating environment.	APO12.01
RE1.3	Collect data on risk events.	APO12.01
RE1.4	Identify risk factors.	APO12.01
RE2.1	Define IT risk analysis scope.	APO12.02
RE2.2	Estimate IT risk.	APO12.02
RE2.3	Identify risk response options.	APO12.02
RE2.4	Perform a peer review of IT risk analysis.	APO12.02
RE3.1	Map IT resources to business processes.	APO12.02
RE3.2	Determine business criticality of IT resources.	APO12.03
RE3.3	Understand IT capabilities.	APO12.03
RE3.4	Update IT risk scenario components.	APO12.03
RE3.5	Maintain the IT risk register and IT risk map.	APO12.03
RE3.6	Develop IT risk indicators.	APO12.03
RR1.1	Communicate IT risk analysis results.	APO12.04
RR1.2	Report IT risk management activities and state of compliance.	APO12.04
RR1.3	Interpret independent IT assessment findings.	APO12.04
RR 1.4	Identify IT-related opportunities.	APO12.04
RR2.1	Inventory controls.	APO12.05
RR2.2	Monitor operational alignment with risk tolerance thresholds.	APO12.05
RR2.3	Respond to discovered risk exposure and opportunity.	APO12.05
RR2.4	Implement controls.	APO12.05
RR2.5	Report IT risk action plan progress.	APO12.05
RR3.1	Maintain incident response plans.	APO12.06
RR3.2	Monitor IT risk.	APO12.06
RR3.3	Initiate incident response.	APO12.06
RR3.4	Communicate lessons learned from risk events.	APO12.06

Personal Copy of: Dr. David Lanter

Appendix B
Detailed Mapping Enterprise Goals—IT-related Goals

The COBIT 5 goals cascade is explained in chapter 2. **Figure 17** contains:
- In the columns, all 17 generic enterprise goals defined in COBIT 5, grouped by BSC dimension
- In the rows, all 17 IT-related goals, also grouped in IT BSC dimensions
- A mapping of 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.

The table was created based on the following inputs:
- Research by the University of Antwerp Management School IT Alignment and Governance Research Institute
- Additional reviews and expert opinions obtained during the development and review process of COBIT 5

Personal Copy of: Dr. David Lanter

When using the table in figure 17, please consider the remarks made in chapter 2 on how to use the COBIT 5 goals cascade.

Figure 17—Mapping COBIT 5 Enterprise Goals to IT-related Goals

			Enterprise Goal																
			Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	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 Goal	Financial					Customer					Internal					Learning and Growth	
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05	Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07	Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S
Internal	09	IT agility	S	P	S			S		P			P		S	S		S	P
	10	Security of information, processing infrastructure and applications			P	P			P								P		
	11	Optimisation of IT assets, resources and capabilities	P	S						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 delivering benefits, on time, on budget, and meeting requirements and quality standards	P	S	S			S				S		S	P				
	14	Availability of reliable and useful information for decision making	S	S	S	S			P		P		S						
	15	IT compliance with internal policies			S	S											P		
Learning and Growth	16	Competent and motivated business and IT personnel	S	S	P			S		S						P		P	S
	17	Knowledge, expertise and initiatives for business innovation	S	P				S		P	S		S		S			S	P

Personal Copy of: Dr. David Lanter

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

Figure 18 contains:
- In the columns, all 17 generic IT-related goals defined in chapter 2, grouped in IT BSC dimensions
- In the rows, all 37 COBIT 5 processes, grouped by domain
- A mapping of 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.

The table was created based on the following inputs:
- Research by the University of Antwerp Management School IT Alignment and Governance Research Institute
- Additional reviews and expert opinions obtained during the development and review process of COBIT 5

When using the table in figure 18, please consider the remarks made in chapter 2 on how to use the COBIT 5 goals cascade.

Figure 18—Mapping COBIT 5 IT-related Goals to Processes

			IT-related Goal																	
			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 risk	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, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
COBIT 5 Process			Financial						Customer		Internal							Learning and Growth	
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Ensure Benefits Delivery	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Ensure Risk Optimisation	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Ensure Resource Optimisation	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Ensure Stakeholder Transparency	S	S	P			P	P						S	S	S		S

Personal Copy of: Dr. David Lanter

Figure 18—Mapping COBIT 5 IT-related Goals to Processes *(cont.)*

			IT-related Goal																
			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 risk	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, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	COBIT 5 Process		Financial						Customer		Internal							Learning and Growth	
Align, Plan and Organise	APO01	Manage the IT Management Framework	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Manage Strategy	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Manage Enterprise Architecture	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Manage Innovation	S			S	P			P	P		P	S		S			P
	APO05	Manage Portfolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Manage Budget and Costs	S		S	S	P	P	S	S			S		S				
	APO07	Manage Human Resources	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Manage Relationships	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Manage Service Agreements	S			S	S	S	P	S	S	S	S		S	P	S		
	APO010	Manage Suppliers		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO011	Manage Quality	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO012	Manage Risk		P		P		P	S	S	S	P			P	S	S	S	S
	APO013	Manage Security		P		P		P	S	S		P				P			
Build, Acquire and Implement	BAI01	Manage Programmes and Projects	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Manage Requirements Definition	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Manage Solutions Identification and Build	S			S	S		P	S			S	S	S	S			S
	BAI04	Manage Availability and Capacity				S	S		P	S	S		P		S	P			S
	BAI05	Manage Organisational Change Enablement	S		S		S		S	P	S		S	S	P				P
	BAI06	Manage Changes			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Manage Change Acceptance and Transitioning				S	S		S	P	S			P	S	S	S		S
	BAI08	Manage Knowledge	S				S		S	S	P	S	S			S		S	P
	BAI09	Manage Assets		S		S		P	S		S	S	P			S	S		
	BAI10	Manage Configuration		P		S		S		S	S	S	P			P	S		

Personal Copy of: Dr. David Lanter

Figure 18—Mapping COBIT 5 IT-related Goals to Processes *(cont.)*

			IT-related Goal																
			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 risk	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, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	COBIT 5 Process		**Financial**						**Customer**		**Internal**							**Learning and Growth**	
Deliver, Service and Support	DSS01	Manage Operations		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Manage Service Requests and Incidents				P			P	S		S				S	S		S
	DSS03	Manage Problems		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Manage Continuity	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Manage Security Services	S	P		P			S	S		P	S	S		S	S		
	DSS06	Manage Business Process Controls		S		P			P	S		S	S	S		S	S	S	S
Monitor, Evaluate and Assess	MEA01	Monitor, Evaluate and Assess Performance and Conformance	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Monitor, Evaluate and Assess the System of Internal Control		P		P		S	S	S		S				S	P		S
	MEA03	Monitor, Evaluate and Assess Compliance With External Requirements		P		P	S		S			S					S		S

Personal Copy of: Dr. David Lanter

Page intentionally left blank

Personal Copy of: Dr. David Lanter