Basic Foundational Concepts
Student Book:
Using COBIT® 5
About ISACA

With more than 110,000 constituents in 180 countries, ISACA (www.isaca.org) helps business and IT leaders maximise value and manage risk related to information and technology. Founded in 1969, the nonprofit, independent ISACA is an advocate for professionals involved in information security, assurance, risk management and governance. These professionals rely on ISACA as the trusted source for information and technology knowledge, community, standards and certification. The association, which has 200 chapters worldwide, advances and validates business-critical 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™) credentials. ISACA also developed and continually updates COBIT®, a business framework that helps enterprises in all industries and geographies govern and manage their information and technology.

Disclaimer

ISACA has designed and created Basic Foundational Concepts Student Book: Using COBIT® 5 (the ‘Work’) primarily as an educational resource for governance, security and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, governance, security and assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

© 2014 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

ISACA

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

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

ISACA wishes to recognise:

Author
Krishna Seeburn, PhD, LLM, FBCS, CITP, SMIEEE, CEng, CIA, CFE, CISSP, PMP, Riesling Consulting Group, Mauritius

Board of Directors
Tony Hayes, CEGIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, International President
Allan Boardman, CISA, CISM, CEGIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Vice President
Juan Luis Caraille, CISA, CEGIT, CRISC, RadioShack Mexico, Mexico, Vice President
Ramses Gallego, CISM, CEGIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CEGIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal Raj, CISA, CISM, CEGIT, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., USA, Vice President
Marc Vael, Ph.D., CISA, CISM, CEGIT, CRISC, CISSP, Valuendo, Belgium, Vice President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Past International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Director
Krysten McCabe, CISA, The Home Depot, USA, Director
Jo Stewart-Rattray, CISA, CISM, CEGIT, CRISC, CSEPS, BRM Holdich, Australia, Director

Credentialing Board
Allan Boardman, CISA, CISM, CEGIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Chairman
Bernard Battistin, CISA, CMA, Office of the Auditor General of Canada, Canada
Richard Brisebois, CISA, CGA, Canada
Terry Chrisman, CEGIT, CRISC, GE Money, USA
Erik Friebolin, CISA, CISM, CRISC, CISSP, PCI-QSA, ITIL, USA
Frank Nielsen, CISA, CEGIT, CCIA, CIA, Nordea, Denmark
Hitoshi Ota, CISA, CISM, CEGIT, CRISC, CIA, Mizuho Corporate Bank, Japan
Carmen Ozores Fernandes, CISA, CRISC, Brazil
Steven E. Sizemore, CISA, CIA, CGAP, Texas Health and Human Services Commission, USA

Professional Standards and Career Management Committee
Steven E. Sizemore, CISA, CIA, CGAP, Texas Health and Human Services Commission, USA, Chairman
Christopher Nigel Cooper, CISM, CITP, FBCC, M.Inst.ISP, HP Enterprises Security Services, UK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA, Myers and Stauffer LLC, USA
Alisdair McKenzie, CISA, CISSP, ITCP, IS Assurance Services, New Zealand
Kameswara Rao Namuduri, Ph.D., CISA, CISM, CISSP, University of North Texas, USA
Katsumi Sakagawa, CISA, CRISC, PMP, JIEC Co. Ltd., Japan
Ian Sanderson, CISA, CRISC, FCA, NATO, Belgium
Timothy Smith, CISA, CISSP, CPA, LPL Financial, USA
Todd Weinman, CPS, The Weinman Group, USA

Academic Program Subcommittee
Kameswara Rao Namuduri, Ph.D., CISA, CISM, CISSP, University of North Texas, USA, Chairman
Umesh R. Hodehattedta, Xavier Institute of Management, India
Matthew Liotine, Ph.D., CBIP, CSSBB, MBCI, University of Illinois at Chicago, USA
Joshua Onome Imoniana, Ph.D., CEGIT, Universidade Presbiteriana Mackenzie, Brazil
Nebil Messabia, Canada
Kumar Srikanteswaran, CISA, CMA, PMP, India
Sadir Vanderloopt, CISA, CISM, CCNA, CCSA, NCSA, Sheffield Hallam University, Sweden
Ype van Wijk, RE, RA, University of Groningen, The Netherlands
Hiroshi Yoshida, Ph.D., CEGIT, CRISC, Nagoya Bunri University, Japan
# Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The Purpose of This Document</td>
<td>5</td>
</tr>
<tr>
<td>2.</td>
<td>IT Governance and the Political Dimension</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Emergence of IT Governance</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Political and Legislative Drivers</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>IT Governance Frameworks</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>The Difference Between a Standard and a Framework</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>COBIT, ITIL and ISO/IEC 27000</td>
<td>7</td>
</tr>
<tr>
<td>3.</td>
<td>Core Concepts in COBIT 5</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Governance of Enterprise IT and COBIT 5</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Substantiating the COBIT 5 Principles</td>
<td>9</td>
</tr>
<tr>
<td>4.</td>
<td>Value Creation and Benefits Realisation</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Categories of IT Investment</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Importance of Categorising Investments</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Value Return</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Key Components of the IT Investment Approval Process</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>How Expected Benefits Can be Defined and Quantified</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>How Benefits Can be Realised</td>
<td>20</td>
</tr>
<tr>
<td>5.</td>
<td>Risk</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>COBIT 5 for Risk</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Drivers for Risk</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Risk Perspectives</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>COBIT 5 Enablers</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>COBIT 5 for Risk and Other Frameworks</td>
<td>27</td>
</tr>
<tr>
<td>6.</td>
<td>Information Security</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Key Objectives for Information Security</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Drivers for Information Security</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Benefits of COBIT 5 for Information Security</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Capabilities of COBIT 5 for Information Security</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>COBIT 5 Enablers for Implementing Information Security</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>Implementing Information Security Initiatives</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>COBIT 5 for Information Security and Other Frameworks</td>
<td>31</td>
</tr>
<tr>
<td>7.</td>
<td>Assurance</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Drivers for Assurance</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Assurance Engagement</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Key Concepts in Assurance Methodologies and Techniques</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Components of Assurance Initiatives</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Assurance Techniques</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Critical Hypotheses in an Assurance Assignment</td>
<td>37</td>
</tr>
</tbody>
</table>
Chapter 1. The Purpose of This Document

The goal of this publication is to provide high-quality educational material that can be integrated into courses on information systems, governance and management. It provides an overview of COBIT 5 principles. COBIT 5 is a framework that enables IT to be governed and managed in a holistic manner for the entire enterprise. For details, see Chapter 3, Core Concepts in COBIT 5.

The objective of creating this publication was to develop a learning resource that can be used effectively by students with little or no business experience. As a result, the materials reproduced herein have been condensed by removing material that addresses practical and operational issues that are of concern to business people and information technology (IT) professionals, but may be difficult for students to appreciate and comprehend.

Chapter 2. IT Governance and the Political Dimension provides an overview of IT governance, its emergence, and political and legislative drivers, and it briefly discusses IT governance frameworks, including COBIT 5.

Chapter 3. Core Concepts in COBIT 5 explains the important concepts from COBIT 5 for general use of the framework.

Chapter 4. Value Creation and Benefits Realisation provides an introduction and overview of the concept of how IT can create value for the enterprise.

Chapter 5. Risk presents definitions for risk, risk management, enterprise risk and the risk management process.


Chapter 7. Assurance explains the assurance process, drivers for assurance, techniques for assurance and components of assurance.

1 www.isaca.org/COBIT/Pages/default.aspx
Chapter 2. IT Governance and the Political Dimension

Emergence of IT Governance

IT governance is the process that ensures the efficient use of IT to achieve enterprise strategic objectives and goals. The need for strong IT governance has been recognised since the advent of IT itself. Methods and frameworks to support this have existed for decades, albeit never really attracting a global following or mass media interest. However, this situation changed in the late 1990s and the early years of the twenty-first century. This is relative to massive failure in the governance systems leading to major controversies such as ENRON, Worldcom, etc.

Much of the change occurred as a result of the natural maturing of the IT sector itself. However, much of it was driven by legislation stemming from political situations and decisions.

Political and Legislative Drivers

Often, legislation is passed as a result of public fear or corporate incident. This tendency also applies to the IT sector.

One of the biggest developments of all came in the United States, and it resulted from a series of financial scandals, most notably ENRON and Worldcom. As a reaction to these incidents, a United States federal law, The Sarbanes-Oxley Act of 2002 (SOX), was approved on 30 July 2002. SOX set a new and enhanced standard for all US public company boards, management and accounting firms. By this standard, SOX increased the independence of external auditors and the role of the boards of directors. The perception of stricter formal governance law was enacted in major countries such as Australia, France, Germany, India, Israel, Italy, Japan, South Africa and Turkey. Other countries with seats of multinational companies with a listing in the US stock exchanges (NYSE, NASDAQ) had to comply with this legislation. This realised a world standard for major (listed) companies. This was not specifically directed at IT; however, the implications for IT were immense as it related to understanding the flow of transactions, including IT aspects in sufficient detail to identify points at which a misstatement could arise in the financial statements. The landscape had changed because the need for controls and clarity became a legal requirement. Frameworks (guide books) and methods to support this were now in vogue, indefinitely.

IT Governance Frameworks

Over the years a number of frameworks have emerged. Each has its own strengths and weaknesses, but also, each has its own focus and purpose. Hardly surprising, perhaps, many (but not all) frameworks revolve around, or are documented by, International Organization for Standardization (ISO) standards.

The major frameworks are currently:

- Balanced Scorecard—A framework for measuring enterprise activities in terms of its vision and strategies
- Capability Maturity Model Integration (CMMI)

---

2 http://finance.laws.com/enron-scandal-summary
3 http://finance.laws.com/worldcom
4 http://finance.laws.com/sarbanes-oxley
5 www.iso.org/iso/home.html
The Difference Between a Standard and a Framework

A standard prescribes what to do to comply with the standard; it describes a step-by-step method to complete the process. ISO creates a varied set of standards in many different areas.

A framework is a general guideline that an enterprise can adopt. A framework can include many components, but does not prescribe the steps to be taken. It describes the possible measures to structure and realise the new environment. COBIT is a framework.

COBIT, ITIL and ISO/IEC 27000

COBIT is an IT governance framework and supporting tool set that allows managers to bridge the gap between business objectives, technical issues and business risk. COBIT enables clear policy development and good practice for IT control throughout enterprises. COBIT emphasises regulatory compliance, helps enterprises increase the value attained from IT, enables alignment and provides simple guidelines on the implementation of the COBIT framework.

Attempting to mix the three management specifications—COBIT, ITIL and ISO/IEC 27000—can be daunting, and much work has been done to harmonise them. Think of the three this way: COBIT tells you what to monitor and control, ITIL describes how to go about implementing the processes for doing that, and ISO/IEC 27000 lays out a process for securing those services and addressing legal requirements.

The choice to use a particular framework can be driven by multiple factors. The type of industry or compliance requirements could be deciding factors. Publicly traded companies will probably want to stick with COBIT to more readily comply with Sarbanes Oxley. ISO 27000 is a series of information security frameworks with applicability in any industry. However, it is best used where the enterprise needs to market information security capabilities through the ISO 27000 certification. NIST SP 800-53 is the standard required by U.S. federal agencies but could also be used by any company to build a technology-specific information security plan. The only bad choice among these frameworks is not choosing any of them.

COBIT 5 provides outcome measures at the level of the 37 COBIT 5 processes.

ISO/IEC 27000 is a framework for information security management published by the International Organization for Standardization and the International Electrotechnical Commission. The standard was first published in 2000 and updated in June 2005. It specifies best practices for security in 12 areas and offers guidance on such topics as protecting personal data, internal information and intellectual property.
ITIL was developed by the UK government starting in the 1980s and provides best practices for delivering IT services. The first version was a 48-book collection that was subsequently reduced to 10 books focusing solely on IT process. ITIL 3 is condensed into five books and refines the notion of IT service. Previously, core tenets were divided between service support and service delivery; these are now combined.
Chapter 3. Core Concepts in COBIT 5

The COBIT 5 good-practice framework for governance and management (board level oversight and day to day operational management) of enterprise IT incorporates many widely accepted concepts and theories from general management and academic IT literature. While exploring how the core principles of the framework are derived from insights from theory and literature, guidance is provided here to practitioners who apply COBIT 5 in enterprises.

Governance of Enterprise IT and COBIT 5

Information and related technology have become increasingly crucial in the sustainability, growth and management of value (application of value analysis [value engineering] techniques for improvement of business effectiveness and efficiency) and risk in most enterprises. As a result, IT has moved from a support role to a central position within enterprises. The enhanced role of IT for enterprise value creation includes benefit realisation, risk optimisation, and resource optimisation and is accompanied by an increased emphasis on governance of enterprise IT (GEIT). Enterprise stakeholders and the governing board (the board of directors) wish to ensure that IT fulfills the goals of the enterprise. GEIT is an integral part of overall enterprise (IT) governance.

Substantiating the COBIT 5 Principles

The COBIT 5 framework is built around five core principles, illustrated in figure 1. Each principle is discussed in this section and relates to concepts and insights from professional and academic literature. The following subsections address the COBIT 5 principles and the concepts that are appropriate for the given principle.

1. Meeting Stakeholder Needs—Strategic Business/IT Alignment

COBIT 5 provides all the required processes and other enablers to support stakeholder value creation through the use of IT. In essence, stakeholder value is an informal term that includes all forms of value that determine the health and well-being of the enterprise in the long run. This could include economic value, employee value, customer value, supplier value, channel partner value, alliance partner value, managerial value, and societal value. A core component of IT governance is to achieve strategic alignment of processes and the result of linking an enterprise structure with its strategy and business environment (whether regulatory, physical, etc.) between IT and the rest of the enterprise.

COBIT 5 suggests that enterprises should start with analysing their business/IT strategic alignment through defining and linking enterprise goals and IT-related goals. It is important to note that an enterprise should start with a clear view of its mission and a thorough definition of its supporting strategy and business goals. This then needs to be translated into goals for the IT department, which are the basis for the IT strategy. Finally, the supporting IT processes must be carefully planned to translate the IT strategy into action. For these planning efforts, enterprises may be looking for guidance to identify the set of important business goals and IT goals, and how they interrelate.
**Meeting Stakeholder Needs—The Balanced Scorecard**

To verify whether stakeholder needs are indeed being met, a sound measurement process (feasible, reliable and understandable metrics) should be established. Stakeholder needs can be related to a set of generic enterprise goals. These enterprise goals have been developed using the balanced scorecard dimensions. The enterprise goals are a list of commonly used goals that an enterprise has defined for itself. Although this list is not exhaustive, most enterprise-specific goals can be easily mapped onto one or more of the generic enterprise goals.

To facilitate a broader measurement process, the developers of COBIT 5 have built on the balanced scorecard concepts. As shown in **figure 2**, all enterprise goals and IT-related goals are grouped in the balanced scorecard perspectives with sample outcome metrics to measure each goal. **Figure 3** provides examples of metrics for the customer perspective of the enterprise and IT-related goals.

---

### Figure 2—Enterprise Goals and IT-related Goals

<table>
<thead>
<tr>
<th>APO</th>
<th>Ensure Governance Framework Setting and Maintenance</th>
<th>Ensure Benefits Delivery</th>
<th>Ensure Risk Optimisation</th>
<th>Ensure Resource Optimisation</th>
<th>Ensure Stakeholder Transparency</th>
<th>Manage the IT Management Framework</th>
<th>Manage Strategy</th>
<th>Manage Enterprise Architecture</th>
<th>Manage Innovation</th>
<th>Manage Portfolio</th>
<th>Manage Budget and Costs</th>
<th>Manage Human Resources</th>
<th>Manage Relationships</th>
<th>Manage Service Agreements</th>
<th>Manage Suppliers</th>
<th>Manage Quality</th>
<th>Manage Risk</th>
<th>Manage Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO01</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>APO02</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>APO03</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>APO04</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>APO05</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>APO06</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>APO07</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>APO08</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>APO09</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>APO10</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>APO11</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>APO12</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>APO13</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
</tbody>
</table>

Legend:  
- P = Primary  
- S = Secondary  

Source: COBIT 5, figure 22
Moreover, COBIT 5 provides outcome measures at the level of the 37 detailed COBIT 5 processes. An example providing specific process goals and related metrics is shown in Figure 4 for the process APO13 Manage security. Of course, these process goals and metrics cannot merely be reported to stakeholders—including senior operational management and the governing board—because the stakeholders would be overwhelmed with information. Rather, the process goals and metrics must be consolidated and aggregated in a way that facilitates a usable and comprehensive balanced scorecard for the entire IT-related environment. The balanced scorecard allows the enterprise to determine whether stakeholder needs are being met.

### Figure 4—Example Balanced Scorecard Metrics for the Security Process

<table>
<thead>
<tr>
<th>Process Goal</th>
<th>Related Metrics</th>
</tr>
</thead>
</table>
| 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 |

Source: [COBIT 5: Enabling Processes](#), APO13, page 113

2. Covering the Enterprise End-to-end—IT

COBIT 5 covers all functions and processes within the enterprise. COBIT 5 does not focus only on the IT function, but treats information and related technologies as assets that need to be dealt with just
like any other asset within the enterprise. Business managers should take on responsibility for managing their IT-related assets just as they do for other assets, such as physical plant (refers to the necessary infrastructure used in support and maintenance of a given facility) and financial and human resource assets, within their own organisational units and functions.

A focus on covering the enterprise end-to-end comprises a move from managing IT as a cost to managing IT as an asset.

COBIT 5 covers both IT and IT-related business responsibilities. As a demonstration of this, COBIT 5 provides Responsible, Accountable, Consulted and Informed (RACI) charts for its processes, in which business and IT roles are included. To illustrate this, an example RACI chart for the process APO09 Manage service agreements is shown in Figure 5. This RACI chart indicates that for the service level agreement (SLA)\(^7\) process, both business and IT functions have accountabilities and responsibilities.

### Figure 5 — End-to-end Responsibility in Managing Service Agreements

<table>
<thead>
<tr>
<th>Key Management Practice</th>
<th>Board</th>
<th>CEO of Executive Office</th>
<th>CIO of Corporate Office</th>
<th>Chief Financial Officer</th>
<th>Chief Operating Officer</th>
<th>Business Process Owners</th>
<th>Business/Executive Committee</th>
<th>Portfolio Management Office</th>
<th>Project Management Office</th>
<th>Service Level Management Office</th>
<th>Chief Risk Officer</th>
<th>Risk Management Board</th>
<th>Enterprise Risk Committee</th>
<th>Risk owners</th>
<th>Human Resources</th>
<th>Compliance</th>
<th>Audit</th>
<th>Chief Information Officer</th>
<th>Head of Finance</th>
<th>Head of Human Resources</th>
<th>Head of Operations</th>
<th>Head of IT Administration</th>
<th>Service Manager</th>
<th>Information Security Manager</th>
<th>Business Continuity Manager</th>
<th>Policy Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO09.01 Identify IT services.</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>A</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>APO09.02 Catalogue IT-enabled services.</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>APO09.03 Define and prepare service agreements.</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>APO09.04 Monitor and report service levels.</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>I</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>APO09.05 Review service agreements and contracts.</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>I</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
</tbody>
</table>

Source: COBIT 5: Enabling Processes, APO09 RACI chart, page 93

3. Applying a Single, Integrated Framework

COBIT 5 aligns with other relevant standards and frameworks at a high level and thus can serve as the overarching framework for GEIT.

In its overarching approach, COBIT 5 identifies a set of governance and management enablers that include 37 processes (see Figure 6). At the governance layer, there are five processes in the Evaluate, Direct and Monitor (EDM) domain. These processes set out the responsibilities for evaluating, directing and monitoring the use of IT assets to create value for the enterprise. The EDM domain covers setting the governance framework, establishing responsibilities in terms of benefits (e.g., investment criteria), risk factors (e.g., risk appetite\(^8\)) and resources (e.g., resource optimisation\(^9\)), and maintaining transparency\(^10\) of IT to stakeholders.

---


8. Risk appetite is a method to help guide an enterprise's approach to risk and risk management.


There are four domains defined at the management layer:

1. **Align, Plan and Organise (APO)**—Concerns the identification of how IT can best contribute to the achievement of the business objectives
2. **Build, Acquire and Implement (BAI)**—Makes IT strategy concrete by identifying the requirements for IT and managing the IT investment programme and projects within that programme
3. **Deliver, Service and Support (DSS)**—Refers to the actual delivery of the IT services required to meet strategic and tactical plans
4. **Monitor, Evaluate and Assess (MEA)**—Includes processes that are responsible for the assessment of process performance and conformance, evaluation of internal control adequacy, and monitoring of regulatory compliance

COBIT 5 includes a more thorough and complete involvement of business management in governing and managing IT than earlier COBIT versions. A typical example is the shift of the Manage service

---

9 Resource optimisation is the set of processes and methods to match the available resources (human, machinery, financial) with the needs of the enterprise to achieve established goals. Optimisation consists in achieving desired results within a set timeframe and budget with minimum usage of the resources themselves. The need to optimise resources is particularly evident when the enterprise’s demands tend to saturate and/or exceed the resources currently available.

10 Transparency is the concept of removing all barriers to—and the facilitating of—free and easy public access to corporate information and the laws, rules, social connivance and processes that facilitate and protect those individuals and corporations that freely join, develop and improve the process.
agreements process to the APO domain, recognising the evolution in IT operations with an increasing importance in outsourcing and cloud computing.

4. Enabling a Holistic Approach—Organisational Systems

The fourth principle (enabling a holistic approach) explains that efficient and effective implementation of GEIT requires a holistic approach, taking into account several interacting components—processes, structures and people.

In applying this organisational system theory to GEIT, enterprises are deploying it using a holistic mixture of structures, processes and relational mechanisms. GEIT structures include organisational units and roles responsible for making IT-related decisions and for enabling contacts between business and IT management decision-making functions (e.g., IT steering committee). This can be seen as a form of blueprint for how the governance framework should be structurally organised.

COBIT 5 builds on these insights. A key change in COBIT 5 is the concept of enablers. ‘Enablers’ are defined as factors that individually and collectively influence whether something will work—in this case, governance and management over enterprise IT. The COBIT 5 framework describes seven categories of enablers (see figure 7)—of which Processes; Organisational Structures; and Culture, Ethics and Behavior are closely related to the organisational systems concept. COBIT 5 then complements these organisational systems insights with other important enablers including Principles, Policies and Frameworks; Information; Service, Infrastructure and Applications; and People, Skills and Competencies.

![Figure 7—COBIT 5 Enterprise Enablers](image)

Source: COBIT 5, figure 12


Released in 2012, COBIT 5 builds on and integrates 20 years of development in this field. From its foundation in the IT audit community, COBIT has become a broader and comprehensive IT governance and management framework and continues to establish itself as a generally accepted framework for IT governance.

COBIT 5 states that governance and management are different types of activities. The governance processes are organised following the EDM model (figure 6), as proposed by ISO/IEC 38500. IT governance processes ensure that enterprise objectives are achieved by evaluating stakeholder needs; setting direction through prioritisation and decision making; and monitoring performance, compliance and progress against plans. Based on these governance activities, business and IT
management plans, builds, runs and monitors activities (a COBIT translation of Deming’s Plan, Do, Check, Act [PDCA] cycle) in alignment with the direction set by the governance body to achieve the enterprise objectives.
Chapter 4. Value Creation and Benefits Realisation

There is a strategic value of IT activities; IT governance inherently improves the level and rate of return on IT investments. The IT governance that processes provide helps enterprises to invest wisely, control costs more effectively and adjust priorities based on changing business strategies. IT asset management initiatives must move beyond an inventory management focus to providing critical cost data and analytical capability to help drive the business of IT.

Value is complex, context-specific and dynamic. It is the relative worth or importance of an investment for an enterprise, as perceived by its key stakeholders, expressed in financial and non-financial terms. To be effective and create value, IT needs to be recognised as a strategic business asset, with business executives owning IT-enabled business changes and the management of operational risk.

Benefit is an outcome whose nature and value (expressed in various ways) are considered advantageous by an enterprise.

Successful acquisition and deployment of information technology often require significant allocation of resources and should therefore be subject to the same initial scrutiny ‘before, during and after’ deployment as any other type of investment. No investment, IT included, should be undertaken without full knowledge of the expected cost and anticipated return, as related to risk.

High-risk projects have a higher likelihood of failure. Therefore, to compensate for those that do fail, high-risk projects should carry a higher return expectation.

To maximise the return on IT investments, techniques, such as preparation of formalised, consistent business cases; use of hurdle rates\(^1\); attention to portfolio management; and application of metrics such as internal rate of return (IRR)\(^2\), net present value (NPV)\(^3\) and payback period, can be helpful.

Ensuring that value is obtained from investment in information technology is an essential component of IT governance. It involves selecting investments wisely and managing them throughout their life cycles—from inception to final retirement. As with any facet of governance, without leadership, commitment and support from the top, it is less likely to realise success.

Increasingly, today’s corporations and public sector bodies are becoming dependent on IT, not just to support the traditional activities of the business, but also to enable it to extend into new areas. Within many sectors, that dependence is becoming virtually total. At the same time, expenditure on IT and its supporting activities has grown to the extent that, within many businesses, the level of IT-related costs is second only to that of staff costs.

Categories of IT Investment

IT investments are subject to the same expectation that applies to any other type of corporate

\(^1\) Hurdle Rate is the minimum acceptable rate of return on a capital investment project. The term is usually associated with one particular method of analysis - the net present value method of capital budgeting.

\(^2\) Internal Rate of Return is the rate of return that would make the present value of future cash flows plus the final market value of an investment or business opportunity equal the current market price of the investment or opportunity.

\(^3\) Net Present Value (NPV) is the difference between the present value of the future cash flows from an investment and the amount of investment. Present value of the expected cash flows is computed by discounting them at the required rate of return.
expenditure: the expectation that they will generate a return. Sometimes that return may be easy to measure, and sometimes it will be more difficult; indeed, sometimes it may be impossible.

However, just because it may be difficult, that must never be accepted as an excuse not to make the effort to try to quantify the expected return in the first place. Getting into the habit of spending shareholder funds without having a close eye on the anticipated return will lead to unwise and badly directed spending, which ultimately will lead, at best, to corporate disadvantage or, at worst, to complete corporate failure. This general rule must apply to all types of IT-related spending.

Peter Weill of Sloan Centre for Information Systems Research (CISR) has suggested the following categorisation:

- **Transactional investment**—Provide the information technology to process the basic, repetitive transactions of the business, e.g., mortgage processing, claims processing or account management. Their main purposes are to increase efficiency and reduce costs.
- **Informational investment**—Provide the information for managing and controlling the enterprise. Systems in this category typically include systems for management and financial control, decision making, planning, communication and accounting.
- **Strategic investment**—Usually designed to add real value to the business by increasing competitive advantage, enabling entry into new markets, or otherwise increasing or enhancing revenue streams.
- **Infrastructure investment**—Can be costly and of long duration, but they may not, in themselves, generate any directly quantifiable financial benefits, although the business applications that depend upon the infrastructure will benefit. Examples include implementation of a new or upgraded systems management product or the implementation of a new operating system. Other examples include a new system to support an Internet-enabled banking initiative or a cable TV-enabled insurance marketing channel.

**Importance of Categorising Investments**

It is important to understand the purposes of having a categorisation scheme for IT investments. These include:

- A greater ability to construct and monitor a balanced portfolio of IT investments. It is probable that a healthy, growing enterprise will have investments in all categories. A proper mix is essential to ensure that risk is understood and managed, growth is encouraged, and focus continues to be placed on essential ‘keeping the lights on’ activities as well as the longer term strategic investments.
- The ability to better define risk and return targets for investments. For example, it is probable that a strategic investment will carry a higher risk and, therefore, an expectation of higher return than an informational investment, which will almost certainly be low risk and will, therefore, be undertaken with an expectation of a lower return.

**Value Return**

Once a comprehensive program has been implemented or adopted, it enables:

- A more precise determination of what assets are currently deployed in the enterprisewide IT environment
- The ability to update or replace those assets efficiently
- Identification of underutilised or outdated assets and management of the costs associated with those assets

Armed with this data, enterprises are much better able to optimise the economic value derived from
IT assets. As such, the strides a company makes towards controlling these costs can significantly improve its IT organisation’s overall efficiency and effectiveness by ensuring that it is spending the right amounts on the right things; in essence driving value return.

Within almost all enterprises, whether public or private sector, the demand for IT investment far exceeds the resources (human and financial) available to deliver and maintain it. Difficult decisions have to be made regarding those projects selected for approval and those to be declined or deferred. Within many enterprises, this decision-making process becomes very subjective, often clouded in political uncertainty, and not always based on totally reliable, objective, complete or consistent underlying data and analysis.

Projects must be understood to establish the level of resources that will remain available for discretionary projects. The selection process, therefore, will apply primarily to discretionary projects, i.e., those projects that do not have to be undertaken, but have the potential to deliver real, measurable value to the enterprise if they are delivered successfully.

**Key Components of the IT Investment Approval Process**

The key components of an IT investment approval process include:

- Preparation of a comprehensive business case, which should be considered a living document; updated and revised when necessary during the development and operation to decommission phases; and based upon a consistent corporate standard and agreed-on assumptions (e.g., tax rates and inflation rates)
- An approval board or committee with appropriate representation from both business and IT to ensure that decisions are made with neutral bias and proper transparency of all business case components, particularly including strategic alignment and financial returns
- Proper consideration of key financial metrics on the proposed return from the candidate investments, including key indicators such as net present value (NPV), internal rate of return (IRR) and payback period
- Provision for proper accountability for the delivery of results. If the corporate culture is one in which there is no actual accountability (e.g., no impact on personal bonuses and other incentives), then no one will take seriously the requirement for accurate and reliable financial metrics in the first place. This means that there must be a reliable process to measure the actual returns that are achieved from each investment.
- Definition of appropriate hurdle rates for IT investments
- Assurance that proper project management processes will be followed, including the full involvement of skilled and experienced resources to deliver and manage the project, together with appropriate reporting to a properly qualified and representative project governance board or committee
- Assurance that all parts of the business that will be affected by the outcome of the project are properly involved and will commit the resources necessary to maximise the chances of success
- An understanding of the potential impact on the value return from this investment from previous solutions delivery experience. For example, if IT-related business investments consistently overrun their original budgets by 20 percent, this 20 percent overrun must be factored into the expected return for each business case. This ‘solutions delivery effect’ can often have the effect of turning an expected profitable outcome into a negative one. This is always a useful and essential sanity check on any proposed project. Without building in the expected impact of an overrun, the business case will be overstated. Keeping this constant focus on solutions delivery performance will also help the enterprise improve, perhaps through undertaking the steps necessary to increase its capability maturity model integration (CMMI) level for systems development and implementation. Of course, past experience in other factors
such as time overrun or under delivery of functionality must similarly be factored into the business case.

**How Expected Benefits Can be Defined and Quantified**

A comprehensive business case for any proposed IT-related business investment should have clearly articulated business benefits defined to enable the expected return to be calculated. These benefits usually fall into two main categories: direct and indirect (or soft). The direct benefits usually comprise the quantifiable financial benefits that the new system is expected to generate.

These are usually a combination of:
- Cost savings through, for example, reductions in staff numbers, stockholding cost reduction, lower cost of production, and improved cash flow through quicker billing and cash collection
- Enhanced revenues through, for example, the ability to enter bigger and more diverse markets, or the launch of a new product or service

**How Benefits Can be Realised**

The clarity and precision of anticipated benefits as defined in the business case are key to the actual and demonstrable achievement of value. Experience demonstrates that, within most enterprises, this process is inconsistent and imprecise. This is particularly true of those enterprises (as noted previously) that have no reliable process for ex-post tracking of benefits and the related accountability, feedback and learning processes.

It should become standard practice for enterprises to track the actual benefits achieved from the development and implementation of IT-related business solutions. Only in this way will it be possible to establish the extent to which the investment has paid off and to ensure appropriate accountability.

The tracking of benefits needs to be ongoing from the date of implementation of the project. In the case of larger projects, a reliable picture of the achieved benefits may be possible only many months, or even years, following implementation.

**COBIT 5—Ensuring Benefits Delivery**

It is important that all investment decisions be made with full knowledge of the expected cost and the anticipated return. Ensuring that the right investments are approved implies a need for accurate predictive costing of the total project across its lifetime and robust predictions of the potential return. To ensure that the total process works and becomes part of the culture of the enterprise, it is essential to establish proper tracking mechanisms to determine the actual value delivered and enable accountability.

COBIT 5 proposes using the EDM02 *Ensure benefits delivery* process to look at how best to optimise the value contribution to the enterprise from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs.

This is achieved by securing 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.
IT-related goals include:

- Alignment of IT and business strategy
- 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
- Knowledge, expertise and initiatives for business innovation

Process goals include:

- The enterprise is securing optimal value from its portfolio of approved IT-enabled initiatives, services and assets.
- Optimal value is derived from IT investment through effective value management practices in the enterprise.
- Individual IT-enabled investments contribute optimal value.

The three governance practices that help achieve benefits delivery costs are:

- **Evaluating 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.

- **Direct value optimisation**—Direct value management principles and practices enable optimal value realisation from IT-enabled investments throughout their full economic life cycles.

- **Monitoring 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.

**Figure 8** depicts the activities involved in ensuring the delivery of benefits.

### Figure 8—EDM02 RACI Chart

<table>
<thead>
<tr>
<th>Key Governance Practice</th>
<th>Board</th>
<th>Chief Financial Officer</th>
<th>Chief Operating Officer</th>
<th>Business Executive</th>
<th>Business Process Owners</th>
<th>Strategy Sponsors Committee</th>
<th>Steering Programme/Project Management Office</th>
<th>Value Management Office</th>
<th>Chief Risk Officer</th>
<th>Chief Information Security Officer</th>
<th>Enterprise Risk Committee</th>
<th>Head Human Resources</th>
<th>Compliance</th>
<th>Audit</th>
<th>Chief Information Officer</th>
<th>Head Architect</th>
<th>Head Development</th>
<th>Head IT Operations</th>
<th>Head IT Administrator</th>
<th>Service Management</th>
<th>Information Security Manager</th>
<th>Business Continuity Manager</th>
<th>Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM02.01 Evaluate value optimisation</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>A</td>
<td>Chief Information Officer</td>
<td>Head Architect</td>
<td>Head Development</td>
<td>Head IT Operations</td>
<td>Head IT Administrator</td>
<td>Service Management</td>
<td>Information Security Manager</td>
<td>Business Continuity Manager</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>EDM02.02 Direct value optimisation</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>Chief Information Officer</td>
<td>Head Architect</td>
<td>Head Development</td>
<td>Head IT Operations</td>
<td>Head IT Administrator</td>
<td>Service Management</td>
<td>Information Security Manager</td>
<td>Business Continuity Manager</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>EDM02.03 Monitor value optimisation</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>Chief Information Officer</td>
<td>Head Architect</td>
<td>Head Development</td>
<td>Head IT Operations</td>
<td>Head IT Administrator</td>
<td>Service Management</td>
<td>Information Security Manager</td>
<td>Business Continuity Manager</td>
<td>Privacy Officer</td>
</tr>
</tbody>
</table>

Source: *COBIT 5: Enabling Processes*, EDM02 RACI chart, page 36
Chapter 5. Risk

Every business activity carries both risk and opportunity. It should be ensured that strategic risk, business environment, transaction, investor relations, financial risk, operational risk, compliance risk (legal risk) and other related types of risk of these business activities is assessed, monitored and, if necessary, addressed. Risk is essentially the level of possibility that an action or activity will lead to a loss or to an undesired outcome. The risk may even pay off and not lead to a loss; it may lead to a gain. Uncertainty, on the other hand, is unpredictable. It has too many unknown variables that do not even allow one to estimate what is going to happen.

Risk:
• Reflects the combination of the likelihood of events occurring and the impact those events have on the enterprise
• Is the potential for events and their consequences, which contains both:
  – Opportunities for benefit (upside)
  – Threats to success (downside)

Risk Management

Risk identification, assessment and evaluation is concerned with correctly determining the risk faced by the enterprise and providing recommendations to senior management on how to effectively maintain risk at an acceptable level, including, but not limited to:
• Identifying risk, including emerging risk and risk associated with people, processes, technology, architecture, applications, information, natural factors and physical threats
• Assessing the risk levels associated with each threat, including anticipated risk likelihood and impact and the effectiveness of current and planned controls
• Calculating the risk levels using both quantitative and qualitative metrics and determining the impact of the risk on the ability of the business to meet its goals and objectives

COBIT 5 for Risk

COBIT 5 for Risk discusses IT-related risk. The guidance and principles that are explained throughout COBIT 5 for Risk are applicable to any type of enterprise, whether it operates in a commercial or non-commercial context, in the private or the public sector, as a small, medium or large enterprise.

COBIT 5 for Risk presents two perspectives on how to use COBIT 5 in a risk context: risk function and risk management.

The risk function perspective focuses on what is needed to build and sustain the risk function within an enterprise. The risk management perspective focuses on the core risk governance and management processes of how to optimise risk and how to identify, analyse, respond to and report on risk on a daily basis.

Drivers for Risk

The main drivers for risk include providing:
• Stakeholders with substantiated and consistent opinions over the current state of risk throughout the enterprise
• Guidance on how to manage risk to levels within the enterprise’s risk appetite
• Guidance on how to set up the appropriate risk culture for the enterprise
Wherever possible, quantitative risk assessments enabling stakeholders to consider the cost of mitigation and the required resources against the loss exposure.

To achieve these aims, COBIT 5 for Risk provides:

- Guidance on how to use the COBIT 5 framework to establish the risk governance and management function(s) for the enterprise
- Guidance and a structured approach on how to use the COBIT 5 principles to govern and manage IT risk
- A clear understanding of the alignment of COBIT 5 for Risk with other relevant standards

The target audience for COBIT 5 for Risk includes:

- Risk professionals across the enterprise:
  - Assistance with managing IT risk and incorporating IT risk into ERM
- Boards and executive management:
  - Understanding of their responsibilities and roles with regard to IT risk management
  - The implications of risk in IT to enterprise strategic objectives
  - How to better optimise IT use for successful strategy execution
- IT and business management:
  - Understanding of how to identify and manage IT risk and how to communicate IT risk to business decision makers

Risk Perspectives

As shown in figure 9, there are two risk perspectives: the risk function perspective and the risk management perspective.

Risk Function Perspective

COBIT 5 for Risk provides guidance and describes how each enabler (figure 10) contributes to the overall governance and management of the risk function. For example:

- Which Processes are required to define and sustain the risk function, govern and manage risk
- What Information flows are required to govern and manage risk—e.g., risk universe, risk profile
- The Organisational Structures that are required to govern and manage risk effectively—e.g., enterprise risk committee, risk function
- What People and Skills should be put in place to establish and operate an effective risk function
Risk Management Perspective

*COBIT 5 for Risk* defines seven risk principles, shown in figure 11, to:
- Provide a **systematic, timely and structured approach** to risk management
- Contribute to **consistent, comparable and reliable** results

The risk principles **formalise** and **standardise** policy implementation—both the core IT risk policy and supporting policies—e.g., information security policy, business continuity policy.

These policies provide more detailed guidance on how to put **principles into practice** and how they will **influence decision making** within an enterprise.

*Figure 12*, taken from *COBIT 5 for Risk*, identifies all COBIT 5 processes that are required to support the risk function:
- Key supporting processes—dark pink
- Other supporting processes—light pink
Core risk processes, shown in light blue are also highlighted in Figure 13—these processes support the risk management perspective:

- EDM03 Ensure risk optimisation.
- APO12 Manage risk.

**Figure 12—Supporting Processes for the Risk Function**

**Figure 13—Core Risk Processes**

<table>
<thead>
<tr>
<th>COBIT 5 Process Identification</th>
<th>Reasoning</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM03 Ensure Risk Optimisation</td>
<td>This process covers the understanding, articulation and communication of the enterprise risk appetite and tolerance and ensures identification and management of risk to the enterprise value that is related to IT use and its impact. The goals of this process are to: • Define and communicate risk thresholds and make sure that key IT-related risk is known. • Effectively and efficiently manage critical IT-related enterprise risk. • Ensure IT-related enterprise risk does not exceed risk appetite.</td>
</tr>
<tr>
<td>APO12 Manage Risk</td>
<td>This process covers the continuous identification, assessment and reduction of IT-related risk within levels of tolerances set by enterprise executive management. Management of IT-related enterprise risk should be integrated with overall ERM. The costs and benefits of managing IT-related enterprise risk should be balanced by: • Collecting appropriate data and analysing risk • Maintaining the risk profile of the enterprise and articulating risk • Defining the risk management action portfolio and responding to risk.</td>
</tr>
</tbody>
</table>

**COBIT 5 Enablers**

*COBIT 5 for Risk* provides specific guidance related to all enablers for the effective management of risk (Figure 14):

- The core risk management process(es) used to implement effective and efficient risk management for the enterprise to support stakeholder value.
- **Risk scenarios**, i.e., the key information item needed to identify, analyse and respond to risk; risk scenarios are the concrete, tangible and assessable representation of risk
- How **COBIT 5 enablers** can be used to respond to unacceptable risk scenarios

**Figure 14**—Scope of COBIT 5 for Risk

**Figure 15** is a graphical representation of a sample risk response workflow.

**Figure 15**—Risk Response Workflow

Source: COBIT 5 for Risk, figure 10

Source: COBIT 5 for Risk, figure 43
COBIT 5 for Risk and Other Frameworks

COBIT 5 for Risk—much like COBIT 5 itself—is an umbrella approach for the provisioning of risk governance and management activities. COBIT 5 for Risk is positioned in context with the following risk-related standards:

- ISO 31000:2009—Risk management
- ISO 27005:2011—Information security risk management
- COSO ERM

COBIT 5 for Risk addresses all ISO 31000 principles, through the:

- COBIT 5 for Risk principles and enablers themselves
- Enabler models

In addition, the framework and process model aspects are covered in greater detail by the COBIT 5 for Risk process model. All elements are included in COBIT 5 for Risk and are often expanded on or elaborated in greater detail, specifically for IT risk management:

- ISO 27005:2011—Information security risk management
  - COBIT 5 for Risk addresses all of the components described within ISO 27005. Some of the elements are structured or named differently.
  - COBIT 5 for Risk takes a broader view on IT risk management compared with ISO 27005, which is focused on the management of security-related risk.

  There is a **stronger emphasis** in COBIT 5 for Risk on processes and practices to ensure the alignment with business objectives, the acceptance throughout the enterprise and the completeness of the scope, amongst other factors.

- COSO ERM—COBIT 5 for Risk addresses all of the components defined in COSO ERM. Although COBIT 5 for Risk focuses less on control, it provides **linkages to enablers**—management practices in the COBIT 5 framework. The **essentials with regard to both control and general risk management** as defined in COSO ERM are present in COBIT 5 for Risk, either through the:
  - Principles themselves and the framework's conceptual design
  - Process model and additional guidance provided in the framework
Chapter 6. Information Security

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

COBIT 5 covers information security in the Information enabler as information goals of completeness and accuracy. COBIT 5 for Information Security defines how information security can be applied in real life, using COBIT 5 principles and enablers.

Information security is a business enabler that is strictly bound to stakeholder trust, either by addressing business risk or by creating value for an enterprise. Competitive advantage is one such example. The significance of information and related technologies is increasing in every aspect of business and public life, and the need to mitigate information risk, which includes protecting information and related IT assets from ever-changing threats, is constantly intensifying. Increasing regulation within the business landscape adds to the awareness of the board of directors of the criticality of information security for information and IT-related assets.

Key Objectives for Information Security

The key objectives of information security are:

- **Confidentiality**—Preserving authorised restrictions on access and disclosure, including means for protecting privacy and proprietary information
- **Integrity**—Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
- **Availability**—Ensuring timely and reliable access to and use of information

Drivers for Information Security

In COBIT 5, the processes APO13 Manage security, DSS04 Manage continuity and DSS05 Manage security services provide basic guidance on how to define, operate and monitor a system for general security management. However, the assumption made in this publication is that information security is pervasive throughout the entire enterprise, with information security aspects in every activity and process performed. Therefore, COBIT 5 for Information Security provides the next generation of ISACA’s guidance on the enterprise governance and management of information security.

Breaches in information security can lead to a substantial impact within the enterprise through, for example, financial or operational damages. In addition, the enterprise can be exposed to external impacts such as reputational or legal risk, which can jeopardise customer or employee relations or even endanger the survival of the enterprise.

The need for stronger, better and more systematic approaches for information security is illustrated in the following examples:

- A national critical infrastructure depends on information systems, and successful intrusions can result in a significant impact to economies or human safety.
- Non-public financial information can be used for economic gain.
- Disclosure of confidential information can generate embarrassment to enterprises, cause damage to reputations or jeopardise business relations.
- Intrusion in commercial networks, for example, to obtain credit card or other payment-related data, can lead to substantial reputational and financial damage due to fines, as well as increased scrutiny from regulatory bodies.
Industrial espionage can enable trade secrets to be imitated and increase competition for manufacturing enterprises.

Leakage of national or military intelligence can result in damage to political relationships.

Personal data leaks can result in financial loss and unnecessary efforts to rebuild an individual’s financial reputation.

Significant unplanned costs (both financial and operational) related to containing, investigating and remediating security breaches can impact any enterprise that has suffered a breach.

**Benefits of COBIT 5 for Information Security**

Using COBIT 5 for Information Security brings a number of information security-related capabilities to the enterprise, which can result in a number of enterprise benefits such as:

- Reduced complexity and increased cost-effectiveness due to improved and easier integration of information security standards, good practices and/or sector-specific guidelines
- Increased user satisfaction with information security arrangements and outcomes
- Improved integration of information security in the enterprise
- Informed risk decisions and risk awareness
- Improved prevention, detection and recovery
- Reduced (impact of) information security incidents
- Enhanced support for innovation and competitiveness
- Improved management of costs related to the information security function
- Better understanding of information security

**Capabilities of COBIT 5 for Information Security**

These benefits are obtained by leveraging the COBIT 5 for Information Security capabilities shown in figure 16.

**Figure 16—COBIT 5 for Information Security Capabilities**

<table>
<thead>
<tr>
<th>COBIT 5 for Information Security Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up-to-date view on governance</td>
<td>COBIT 5 for Information Security provides the most up-to-date view on information security governance and management through alignment with COBIT 5, International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 38500 and other IT governance initiatives. During the development of COBIT 5 for Information Security, the most important guidance and standards were analysed. COBIT 5 for Information Security aligns with other major frameworks, standards and models in the marketplace, such as the ISO/IEC 27000 series, the Information Security Forum (ISF) Standard of Good Practice, and BSI. Additionally, ISACA's information security governance offerings, Information Security Governance: Guidance for Information Security Managers and Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition were analysed during the development of COBIT 5 for Information Security.</td>
</tr>
<tr>
<td>Clear distinction between governance and management</td>
<td>COBIT 5 clarifies the roles of governance and management and provides a clear distinction between them, with a revised process model reflecting this distinction and showing how they relate to each other.</td>
</tr>
<tr>
<td>End-to-end view</td>
<td>COBIT 5 for Information Security is a process model that integrates both business and IT functional responsibilities. It provides a clear distinction between information security governance and information security management practices, outlining responsibilities at various levels of the enterprise, encompassing all process steps from the beginning to the end.</td>
</tr>
<tr>
<td>Holistic guidance</td>
<td>The COBIT 5 for Information Security framework brings together comprehensive and holistic guidance on Information Security. Holistic means that attention is paid not only to processes, but to all enablers, including information, structures, culture, policies and their interdependencies.</td>
</tr>
</tbody>
</table>

Source: COBIT 5 for Information Security, figure 3
COBIT 5 Enablers for Implementing Information Security

**COBIT 5 for Information Security** provides specific guidance related to all enablers:

1. Information security Policies, Principles and Frameworks
2. Processes, including information security-specific details and activities
3. Information security-specific Organisational Structures
4. In terms of Culture, Ethics and Behaviour, factors determining the success of information security governance and management
5. Information security-specific Information types
6. Service capabilities required to provide information security functions to an enterprise
7. People, Skills and Competencies specific to information security

### Implementing Information Security Initiatives

Inputs to a policy framework are shown in **figure 17**.

![Figure 17—Policy Framework](image)

Source: *COBIT 5 for Information Security*, figure 10

Considering the enterprise information security context: *COBIT 5 for Information Security* advises that every enterprise needs to define and implement its own information security enablers depending on factors within the enterprise’s environment, such as:

- Ethics and culture relating to information security
- Applicable laws, regulations and policies
- Existing policies and practices
- Information security capabilities and available resources

Additionally, the enterprise’s information security requirements need to be defined based on:

- Business plan and strategic intentions
- Management style
- Information risk profile
- Risk appetite

The approach for implementing information security initiatives will be different for every enterprise, and the context needs to be understood to adapt *COBIT 5 for Information Security* effectively.

Other key areas of importance when implementing *COBIT 5 for Information Security* are:
• Creating the appropriate environment
• Recognising pain points and trigger events
• Enabling change
• Understanding that implementing information security practices is not a one-time event, but is a life cycle

**COBIT 5 for Information Security and Other Frameworks**

COBIT 5 aims to be an umbrella framework to connect to other information security frameworks, good practices and standards.

*COBIT 5 for Information Security* describes the pervasiveness of information security throughout the enterprise and provides an overarching framework of enablers. Other frameworks can be helpful as well because they may elaborate on specific topics. Examples include:

• Business Model for Information Security (BMIS)—ISACA
• Standard of Good Practice for Information Security (ISF)
• ISO/IEC 27000 Series
• NIST SP 800-53a
• Payment Card Industry (PCI)-Data Security Standard (DSS)
Chapter 7. Assurance

Assurance means that, pursuant to an accountability relationship between two or more parties, an IT audit and assurance professional may be engaged to issue a written communication expressing a conclusion about the subject matters to the accountable party. Assurance refers to a number of related activities (assurance engagements) designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter. For example, assurance engagements could include support for audited financial statements; assessment of value provided by IT to the enterprise; reviews of controls; compliance with required standards and practices; and compliance with agreements, licences, legislation and regulations.

Drivers for Assurance

The main drivers for assurance include:
• Providing interested parties (see figure 18) substantiated opinions on governance and management of enterprise IT according to assurance objectives
• Defining assurance objectives in line with enterprise objectives, thus maximising the value of assurance initiatives
• Satisfying regulatory or contractual requirements for enterprises to provide assurance over their IT arrangements

An assurance initiative consists of five components, as illustrated in figure 19.
Assurance Engagement

In conducting an assurance assignment, an accountability relationship exists amongst three parties:

- **Accountable party**—The individual, group or entity (auditee), usually involving management, that is ultimately responsible for subject matter, process or scope
- **User**—Depending on the circumstances, the user could include a variety of stakeholders, such as shareholders, creditors, customers, board of directors, audit committee, legislators or regulators. For some types of assurance activities, the auditee and the user can be identical, e.g., IT management.
- **Auditor**—The assurance professional with overall responsibility for the performance of the assurance engagement and for the issuance of the report on the subject matter

The accountability relationship is a prerequisite for an assurance engagement, and it exists when one party (the auditee) is responsible to another party (the user) for a subject matter, or voluntarily chooses to report to another party on a subject matter. The accountability relationship may arise as a result of an (contractual) agreement or legislation, or because a user can be expected to have a stake in how the accountable party has discharged its responsibility for a subject matter.

Subject Matter

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

Selecting Criteria/Benchmarks

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

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

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

**Executing the Assurance Assignment**

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

**Evaluating the Results**

The process of evaluating the results of audit or assurance testing, after confirmation, to arrive at conclusions and recommendations can be complex. What appears to be a problem may, in fact, be the effect of a problem, not the cause.

Therefore, it is important for the audit and assurance professional to follow the conclusion process, from confirming facts with key individuals in the areas being audited to determining root causes. The individual findings can then be used to provide examples that support higher-level analysis:

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

Audit and assurance professionals should obtain an adequate understanding of the subject matter and its business environment. They should communicate the bigger picture, link the impact of the issues/findings to the overall organisational strategic goals and objectives to tell the ‘the story behind the story’, and communicate value insights. Executives are not very interested in knowing the observations; they need to understand the insights behind the findings (example, the executive summary).

Recommendations from audit and assurance engagements may be reported in a separate report, not as part of the audit or assurance report. The recommendations should be clear, concise and actionable. They should be reviewed and agreed on by management and the auditee or other stakeholders.

Reports should be tailored for a specific audience. Reports to senior management and executives should address issues and concepts, with detailed audit findings used as illustrations of the issue,
problem or result. Reports to middle and line management should contain the same information, but with a different level of detail, to allow them to fully understand the issue and handle the problem. Where appropriate, recommendations should include provision for timely monitoring and follow-up.

Key Concepts in Assurance Methodologies and Techniques

Key concepts:
- The assurance process includes the following steps:
  - Planning assurance
  - Scoping assurance
  - Executing assurance (testing)
- Risk driver
- Value driver

Components of Assurance Initiatives

Assurance initiatives in the realm of IT governance have a dedicated context and objective—to measure or evaluate a specific subject matter that is the responsibility of another party.

To be called an assurance initiative, five components must be present, as shown in figure 20.

Figure 20—Five Components of an Assurance Initiative

There are two types of IT assurance activities or initiatives, each with its own steps.
- For generic assurance, the steps cover the existence and design of proposed control design (assurance controls) as well as the associated responsibilities.
• For specific assurance, the steps test the effective operation of controls and are stated at the control objective level. There are also assurance steps to test the outcomes of control weakness or failure.

There are several testing methods and techniques. They include inquiry, inspection, observation, re-performance, recalculation, analysis and sampling (trace, extract).

According to the International Standards on Auditing (ISA), the assurance professional must obtain an understanding of:
• The control environment
• The entity’s risk assessment process
• The information systems (including the related business processes relevant to financial reporting and communications)
• Control activities and monitoring of controls

The assurance professional should consider the need to obtain audit evidence supporting the effective operation of controls directly related to the management assertions as well as other indirect controls on which these controls depend, such as underlying general IT controls.

In the context of IT, the financial statement assertions that are mandated as regulatory requirements can be translated into the following information processing objectives:
• Completeness
• Accuracy
• Validity
• Restricted access

IT Assurance Road Map

The IT assurance process can be depicted in three phases in the IT assurance road map:
• Planning
• Scoping
• Executing

Assurance Techniques

Typical assurance techniques or activities that are utilised in the different stages and steps of the IT assurance road map are listed in the following planning, scoping and executing phases. Sometimes the step is the activity or technique, and sometimes a technique or activity can be leveraged in several steps.

Planning:
• Perform a quick risk assessment.
• Assess threat, vulnerability and business impact.
• Diagnose operational and project risk.
• Plan risk-based assurance initiatives.
• Identify critical IT processes, based on value drivers.
• Assess process maturity.

Scoping:

---

14 [www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/Pages/default.aspx](www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/Pages/default.aspx)
• Scope and plan assurance initiatives.
• Select the control objectives for critical processes.
• Customise control objectives.

Executing:
• Refine the understanding of the IT assurance subject.
• Refine the scope of the key control objectives for the IT assurance subject.
• Test the effectiveness of the control design of the key control objectives.
• Test the outcome of the key control objectives.
• Document the impact of control weaknesses.
• Develop and communicate overall conclusion and recommendations.
• Report assurance conclusions.

Critical Hypotheses in an Assurance Assignment

There are several critical hypotheses that are inherent in any IS audit or assurance assignment. Some of these include:
• The subject matter is identifiable and subject to audit.
• There is a high probability of successful completion of the project.
• The approach and methodology are free from bias.
• The project is of sufficient scope to meet the IS audit or assurance objectives.
• The project will lead to a report that is objective and that will not mislead the reader.

Formal standards such as ISACA’s Information Technology Assurance Framework (ITAF)\(^\text{15}\), Institute of Internal Auditor’s (IIA) International Professional Practices Framework (IPPF) and the American Institute of Certified Public Accountants’ (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 16 exist and may be referenced when performing assurance assignments, but this assurance publication also covers evaluation activities not governed by internal and/or external audit standards.

\(^{15}\) [www.isaca.org/itaf](http://www.isaca.org/itaf)