ISACA®
Trust in, and value from, information systems

COBIT® 5

Enabling Information

COBIT® 5
AN ISACA® FRAMEWORK

ISACA®

With more than 110,000 constituents in 180 countries, ISACA (*www.isaca.org*) helps business and IT leaders maximize value and manage risk related to information and technology. Founded in 1969, the non-profit, 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 *COBIT® 5: Enabling Information* (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 judgment to the specific governance of enterprise IT (GEIT), assurance, risk and security circumstances presented by the particular systems or information technology environment.

Copyright

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

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

COBIT® 5: Enabling Information
ISBN 978-1-60420-350-9
1

Acknowledgements

ISACA wishes to recognise:

COBIT 5 IRM Task Force
Steven De Haes, Ph.D., University of Antwerp—Antwerp Management School, Belgium, Chairman
Charles Betz, AT&T, USA
Martin Douglas, CA(SA), ITIL, UK
Patrick Stachtchenko, CISA, CGEIT, CRISC, CA, Stachtchenko & Associates SAS, France

Development Team
Stefanie Grijp, PwC, Belgium
Bart Peeters, CISA, PwC, Belgium
Dirk Steuperaert, CISA, CGEIT, CRISC, IT In Balance BVBA, Belgium

Workshop Participants
Floris Ampe, CISA, CGEIT, CRISC, CIA, ISO 27001, PwC, Belgium
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Peter De Bruyne, CISA, CGEIT, ITIL, ING, Belgium
Yalcin Gerek, CISA, CGEIT, CRISC, ITIL Expert, PRINCE2, TAC A.S., Turkey
Jurgen Van De Sompel, CGEIT, Belgium
Tichaona Zororo, CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance of IT (Pty) Ltd., South Africa

Expert Reviewers
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Goutama Bachtiar, BCIP, BCP, HPCP, Global Innovations and Technology Platform, Indonesia
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Joanne De Vito De Palma, BCMM, The Ardent Group, USA
Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Austria
Ivo Horner, Australia
John Jasinski, CISA, CGEIT, ISO20K, ITIL Expert, SSBB, ITSMBP, USA
Masatoshi Kajimoto, CISA, CRISC, Japan
Joanna Karczewska, CISA, ASKOT NIP: 113-078-77-89, Poland
John W. Lainhart IV, CISA, CISM, CGEIT, CRISC, IBM Global Business Services, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Patricia Prandini, CISA, CRISC, Direccion De Aplicaciones, Argentina
Salomon Rico, CISA, CISM, CGEIT, Deloitte Mexico, Mexico
Paras Kesharichand Shah, CISA, CGEIT, CRISC, CA, Australia
Mark Smalley, Smalley.IT, The Netherlands
Jurgen Van De Sompel, CGEIT, Belgium
Greet Volders, CGEIT, Voquals, Belgium
Tichaona Zororo, CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance of IT (Pty) Ltd., South Africa

ISACA Board of Directors
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, International President
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Vice President
Juan Luis Carselle, CISA, CGEIT, CRISC, RadioShack Mexico, Mexico, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal Raj, CISA, CISM, CGEIT, 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, CGEIT, 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, CGEIT, CRISC, CSEPS, BRM Holdich, Australia, Director

Acknowledgements *(cont.)*

Knowledge Board
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Thomas E. Borton, CISA, CISM, CRISC, CISSP, Cost Plus, USA
Philip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK

Framework Committee
Steven A. Babb, CGEIT, CRISC, Betfair, UK, Chairman
David Cau, ISO, ITIL, MSP, PRINCE2, France
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Frank J. Cindrich, CGEIT, CIPP, CIPP/G, Deloitte & Touche LLP, USA
Joanne De Vito De Palma, BCMM, The Ardent Group, USA
Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Austria
Katherine McIntosh, CISA, Central Hudson Gas & Electric Corp., USA
Andre Pitkowski, CGEIT, CRISC, APIT Informatica, Brazil
Paras Kesharichand Shah, CISA, CGEIT, CRISC, CA, Australia

Table of Contents

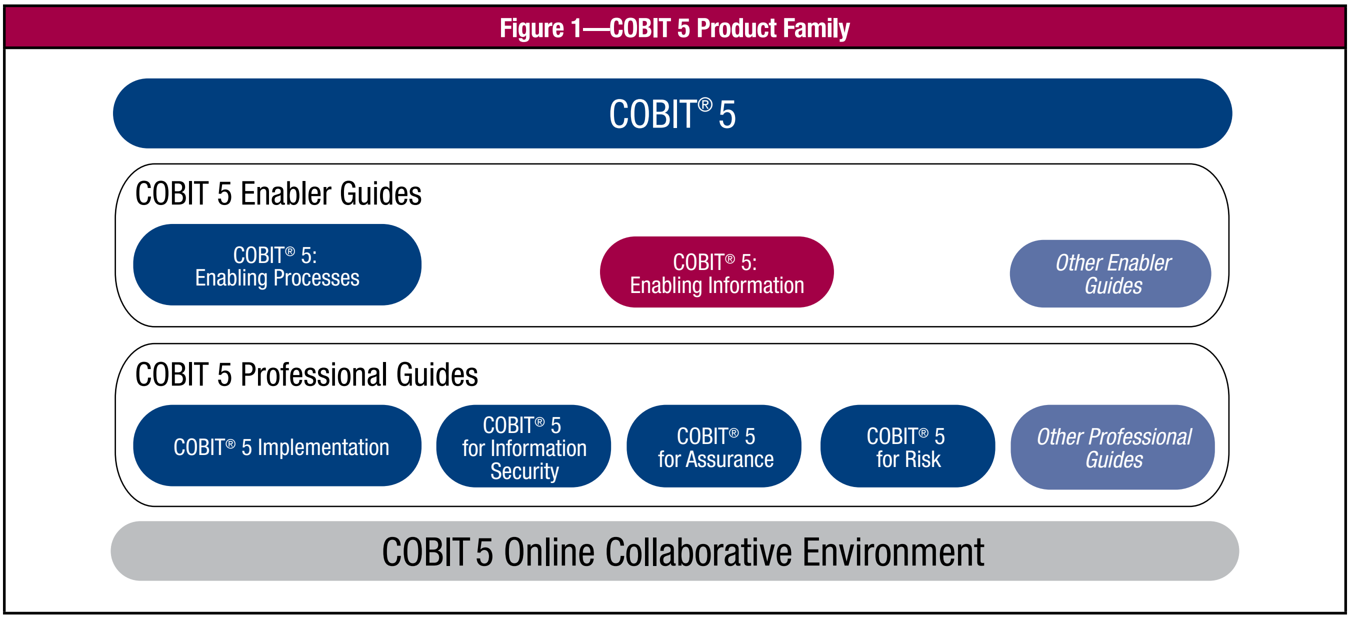
List of Figures

Chapter 1
Introduction

1.1 *COBIT 5: Enabling Information* in the COBIT 5 Product Family

COBIT 5 is a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise information technology (IT). *COBIT 5: Enabling Information* supports and enhances the COBIT 5 framework family of products (**figure 1**) by focusing on the Information enabler. This guide addresses the information model attributes and life cycle that are introduced in the COBIT 5 framework. *COBIT 5: Enabling Information* is a reference guide for structured thinking about **information** and typical **information governance and management issues**.

Figure 1—COBIT 5 Product Family


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

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

The COBIT 5 product family includes the following products:

- COBIT 5 (the framework)
- COBIT 5 enabler guides, in which governance and management enablers are discussed in detail. These include:
  - *COBIT 5: Enabling Processes*
  - ***COBIT 5: Enabling Information***
  - 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 (in development)

1.2 Benefits of *COBIT 5: Enabling Information*

The main benefit of this publication is that it provides COBIT 5 users with a reference guide for structured thinking about **information** and typical **information governance and management issues** in any type of organisation. This structured thinking can be applied throughout the life cycle of information, from conception and design, through building information systems, securing information, using and providing assurance over information, and to the disposal of information.

This guide provides information practitioners with the following three key benefits:

- A comprehensive information model, based on the generic COBIT 5 enabler model, that comprises all aspects of information, e.g., stakeholders, goals (quality), life cycle stages and good practices (information attributes). The model allows practitioners to effectively consider and develop relevant, usable information models from a governance and management point of view.
- Guidance on how to use an established governance and management framework (COBIT 5) to address common information governance and management issues, e.g., big data, master data management, information disintermediation and privacy, and how COBIT 5 principles and concepts, especially the enablers, can address these issues.
- An understanding of the reasons information needs to be managed and governed in an appropriate way and the criticality of information that is contained within a given context.

This guide assists enterprises with information issues and challenges, such as:

- Disparate, uncoordinated data sets are implicated in increasing cost and risk from missed project deadlines, lack of transparency and operational failures.
- Records management, legal and IT teams need a common base reference to coordinate activities, because records retention and legal discovery are of growing concern and cost to managers, and security classifications overlap with record classifications.
- The number of data elements with multiple compliance dimensions is increasing. How can an enterprise maintain appropriate practices to comply with relevant global and regional legislation and regulatory and compliance requirements, such as:
  - Payment Card Industry (PCI)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Health Information Technology for Economic and Clinical Health (HITECH) Act
  - Gramm-Leach-Bliley (GLB) Act
  - European Union (EU) Directive on Data Protection

  Specifically, how are such practices operationalised in terms of data and information management? Enterprises are experiencing increasing difficulty in maintaining control of their data to comply with legal and regulatory requirements. What needs to be done to address this issue?
- Information is increasingly being recognised as an asset or resource that delivers benefits to the enterprise when the enterprise meets necessary quality goals. However, identifying, defining and prioritising these goals against the cost of quality are always a challenge.

The intent of this guide is to provide readers with a better understanding of information governance and management issues and improve their ability to generate benefits and manage information-related risk. This guide supports readers in their efforts to use information-centric thinking about their enterprises.

1.3 Target Audience for This Guide

Figure 2 shows that the target audience for this publication includes a broad range of business and IT professionals, because all work with information as a resource and/or assets.

Figure 2—Target Audience and Benefits of *COBIT 5: Enabling Information*

Stakeholder	Stakeholder-specific Benefits of Using *COBIT 5: Enabling Information*
Board of directors and executive management (Chief executive officer [CEO], Chief operations officer [COO], Chief financial officer [CFO])	• Basic understanding of the meaning of information governance and management, based on COBIT 5 principles, and the assertion that a comprehensive model exists for describing and dealing with all aspects of information • Better understanding of information as a valued asset/resource and an enabler and facilitator
Business process owners, business process architects	• Basic understanding of the meaning of information governance and management, based on COBIT 5 principles, and the assertion that a comprehensive model exists for describing and dealing with all aspects of information • Well-defined overview of information items required to run specific business processes
Information architects, information solution builders, information managers, IT architects, IT developers	• A COBIT 5-oriented model for describing, specifying and designing all aspects of information that support all information-based processes and information systems, whether automated or not • Ability to identify the information items that need to be managed through the applications that are being developed

Figure 2—Target Audience and Benefits of *COBIT 5: Enabling Information (cont.)*

Stakeholder	Stakeholder-specific Benefits of Using COBIT 5: Enabling Information
Chief information officer [CIO] and IT management, technology service providers (internal and external), application managers	• Understanding of a model for information items that is needed to manage the IT function • Better understanding of all business information items that need to be managed through information systems
IT operations	Understanding of the criticality of information contained within a given service
IT security, continuity professionals	• Understanding of the criticality of information contained within a given service • Understanding of how the information model provides the necessary components to define and manage information security concepts as they pertain to confidentiality, integrity and availability • Understanding of how their enterprise organisations fit in the overall information quality management
Assurance professionals	Guidance about the information items that need to comply with quality criteria when planning and executing assurance assignments
External audit	• Understanding of information accuracy, currency and reliability • Understanding of the completeness and security of transactions • Understanding of how information may have material impact on business performance
Records management professionals, knowledge managers	Ability to capitalise on a structured way of thinking about information and use it to facilitate understanding with IT and business groups
Data governance and management professionals	A model for describing, specifying and designing key aspects of information that support information-based processes and information systems, whether automated or not
Government and regulators	• Basic understanding of the meaning of information governance and management, based on COBIT 5 principles, and the assertion that a comprehensive model exists for describing and dealing with all aspects of information • Well-defined base reference on which to base their legislative and regulatory directives
Education	Basic understanding of the meaning of information governance and management, based on COBIT 5 principles, and the assertion that a comprehensive model exists for describing and dealing with all aspects of information, both of which can be taught to students
Privacy professionals	A model for analysing and reporting on aspects of information that support information-based processes and information systems, whether automated or not
Compliance and risk professionals	A model for analysing and reporting on aspects of information that support information-based processes and information systems, whether automated or not
Data owners	A model for describing, specifying and designing key aspects of information that support information-based processes and information systems, whether automated or not

1.4 Prerequisite Knowledge

COBIT 5: Enabling Information builds on COBIT 5 (the framework). Relevant key concepts of COBIT 5 are repeated and elaborated on in this guide, making it a fairly stand-alone guide—in essence, not requiring any prerequisite knowledge of COBIT 5. However, an understanding of COBIT 5 principles, concepts and structure at the foundation level will accelerate and improve comprehension of the contents of this guide. If readers wish to know more about COBIT 5, beyond what is required to address information governance and management business goals and issues, they are referred to the COBIT 5 framework publication.

In addition, *COBIT 5: Enabling Information* refers to:

- The COBIT 5 process reference model and the COBIT 5 governance and management processes that are described therein. If readers wish to know more about COBIT 5 processes, perhaps to implement or improve some of them as part of addressing an information-related issue, they are referred to the *COBIT 5: Enabling Processes* guide.
- The other COBIT 5 enablers that are discussed in the COBIT 5 framework publication

Finally, readers can find more information on information risk management, information security and providing assurance over information in the corresponding COBIT 5 professional guides: *COBIT 5 for Risk*, *COBIT 5 for Information Security* and *COBIT 5 for Assurance*.

1.5 Document Overview and Scope

COBIT 5: Enabling Information addresses fundamental questions and issues about information as an enterprise asset or governance/management enabler. This guide also discusses information governance and information management practices and enabler arrangements. **Figure 3** shows these questions, explains how and where *COBIT 5: Enabling Information* addresses them or if the topic is out of the scope of this guide, and defines key concepts.

Figure 3—COBIT 5: Enabling Information Overview and Frequently Asked Questions

Common Questions	Guidance in This Publication
What is data? What is information?	**Data** can be defined as something that is, or represents, a fact. This can be in many forms (e.g., text, numbers, graphics, sound, video). **Information** is data in context. Context means providing a meaning to the data, defending the format in which the data are presented and the relevance of the data within a certain usage context.
Why is information important?	Information is used at every level of the enterprise, i.e., at operational, management and governance levels. Information is one of the enablers of every business function reliant on IT, including IT itself. As such, information contributes to the achievement of overall enterprise objectives. Chapter 2 explains how the COBIT 5 goals cascade is a useful tool for analysing and illustrating this dependency.
What types of information does this guide consider?	This guide is applicable to all types of information. Because no universal classification or model exists for all enterprise information, this guide proposes a simple model to distinguish different levels of information, as described in chapter 3, in section 3.1 COBIT 5 Information Model Overview and section 3.1.4.1 Good Practices. Section 2.1.2 explains Principle 2: Covering the Enterprise End-to-end.
What is the difference between information governance and information management and how does this guide help me?	Based on definitions from COBIT 5 and Data Management Body of Knowledge (DMBOK) frameworks, information governance and management can be described as follows. **Information governance** ensures that: • Stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives, which are to be achieved through the acquisition and management of information resources. • Direction is set for information management capabilities through prioritisation and decision making. • Performance and compliance of the information resource are monitored against agreed-on direction and objectives. **Information management** plans, builds, runs and monitors the practices, projects and capabilities that acquire, control, protect, deliver and enhance the value of data and information assets, in alignment with the direction set by the data and information governance body. Section 2.1.5 further distinguishes the terms.
How can one guide deal with all types of information?	Information and data management have been topics of both study and practice for many decades, and a number of principles and good practices have been identified that persist regardless of the type of information. Chapter 3 includes a rich and yet sufficiently high-level model for information that is capable of dealing with all types of information.
Are there any related standards?	DAMA-DMBOK is a complete guide for data management practitioners, from business analysts through technical operations. The Open Group's TOGAF has extensive coverage of data architecture, which is one of the essential pillars of enterprise architecture. The Object Management Group has more prescriptive standards for data management syntax (metamodels), such as Semantics of Business Vocabulary and Business Rules, Common Warehouse Metamodel, Common Terminology Services and Ontology Definition Metamodel. ISO 15489 is a standard for records management that includes setting policies and standards; assigning responsibilities and authorities; establishing and promulgating procedures and guidelines; providing a range of services relating to the management and use of records; designing, implementing and administering specialised systems for managing records; and integrating records management into business systems and processes. Appendix A provides details about the DAMA-DMBOK framework and ISO 15489-1:2001 and compares them to COBIT 5.
What topics about information are not included in this guide?	Many topics are deliberately not included in this document because they require a level of detail beyond its scope, such as: solutions architecture, logical and physical data modelling at a practice level; solutions design, including choice of database management system (DBMS); implementation and operation of DBMS; detailed business practices to help govern and manage information.

To provide a structured approach to the information in this guide, COBIT 5: Enabling Information is divided into four chapters and three appendices. Following is a brief description of each section and how those sections are interconnected:

- **Chapter 1**—Introduction
- **Chapter 2**—Applies the COBIT 5 principles to information. This chapter:
  - Demonstrates the relationship between information and enterprise goals using the COBIT 5 goals cascade.
  - Differentiates information types, distinguishing between business information and IT-related information and illustrating both.
  - Differentiates information governance and management.
  - Demonstrates how **information** fits in to the overall holistic view of an enterprise and its constituent parts and introduces the COBIT 5 enabler concept.
- **Chapter 3**—Elaborates on the information model that is presented in the COBIT 5 framework publication by presenting multiple examples of how to apply the model to all aspects of information governance and management.
- **Chapter 4**—Elaborates on a number of typical information governance and management issues that enterprises encounter, explains the issues and their relevance in the enterprise context, and suggests how COBIT 5 and its enablers can help to address the issues.
- **Appendix A**—Reference to relevant other guidance
- **Appendix B**—Comprehensive list of information items that are related to all business processes
- **Appendix C**—Comprehensive list of IT-related information items, their key quality criteria and related metrics

COBIT 5: Enabling Information focuses on governance and management of information at a high level and is **<u>not</u>** intended to:

- Assist organisations with technical or operational guidance on how to build a complete data set, information items and artefacts or databases, or how to operate storage systems. These items are dependent on specific enterprise policies, information standards and software specifications.
- Be comprehensive in any specific area of business, e.g., industry-specific data models that facilitate exchange of data or information

Note: Although structured thinking may lead to the development of good information-related practices, process practices are not the focus of this guide. Processes are documented in *COBIT 5: Enabling Processes*.

Page intentionally left blank

Chapter 2
COBIT 5 Principles Applied to Information

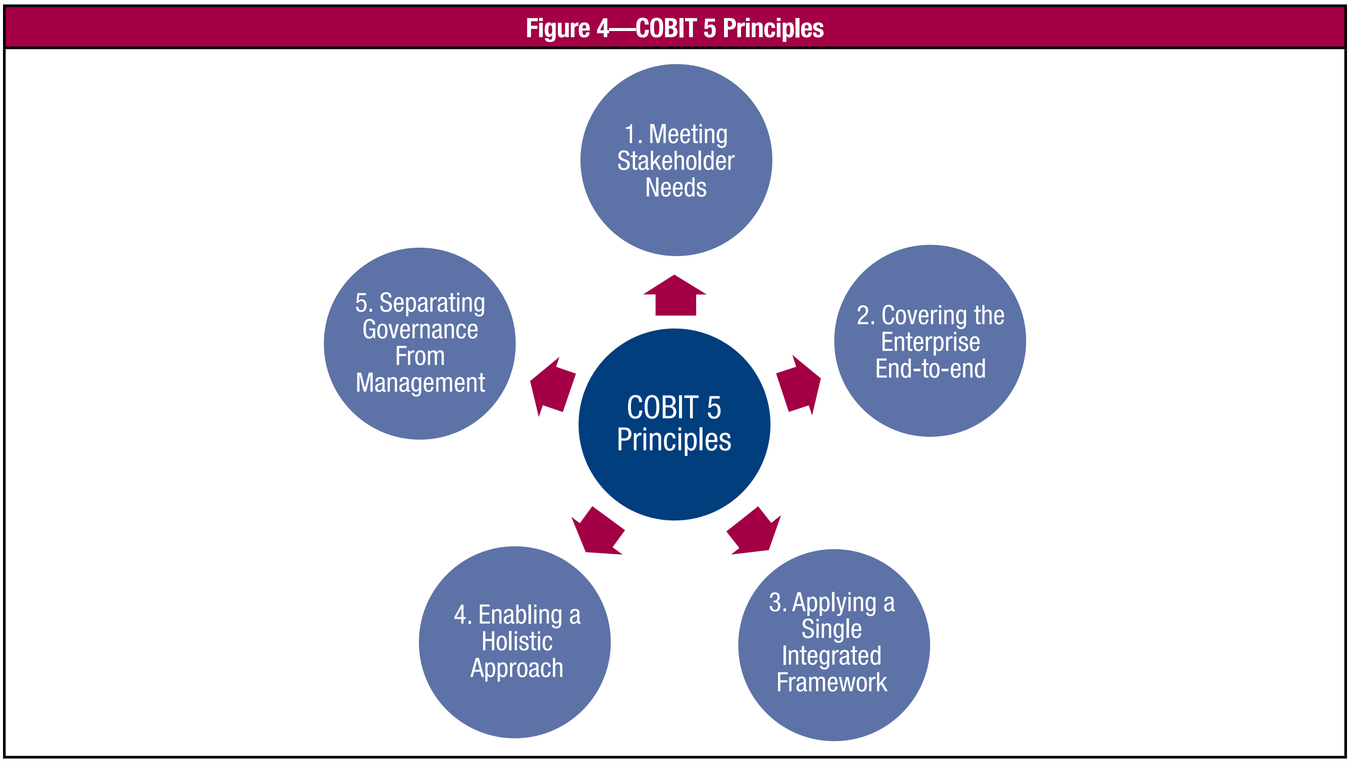
This chapter explains how the COBIT 5 principles are applied to information and includes:

- The COBIT 5 goals cascade, to explain value creation and how it relates to information and the other enablers
- Information, an enabler for the overall enterprise during the complete value chain, which is illustrated with example information items for business processes and the IT function
- Information governance and information management explanations

2.1 COBIT 5 Principles

COBIT 5 is based on five principles, as shown in **figure 4**. This guide applies the COBIT 5 principles to information.

Figure 4—COBIT 5 Principles


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

Principle 1: Meeting Stakeholder Needs—Enterprises exist to create value for their stakeholders by maintaining a balance between the realisation of benefits, the optimisation of risk and the use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customise COBIT 5 to suit its own context through the goals cascade[1], translating high-level enterprise goals into manageable, specific, IT-related goals and mapping these to specific enabler goals.

COBIT 5: Enabling Information provides an information-centric view of the enterprise. Information should ultimately support the goal of any enterprise—deliver value for its stakeholders—which translates to enterprise goals that should be achieved. The COBIT 5 goals cascade translates enterprise goals into more tangible enabler goals, in this case, information quality goals.

Principle 2: Covering the Enterprise End-to-end—COBIT 5 integrates governance of enterprise IT into enterprise governance:

- It 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 addressed, just like any other asset, by everyone in the enterprise.
- It considers all IT-related governance and management enablers to be enterprisewide and end-to-end, i.e., inclusive of everything and everyone—internal and external—that is relevant to governance and management of enterprise information.

[1] The goals cascade is based on research performed by the University of Antwerp Management School IT Alignment and Governance Institute in Belgium.

COBIT 5: Enabling Information provides a single model to structure information that is applicable to all types of information used by the enterprise, including information used by business functions, information internal to the IT function and external information.

Principle 3: Applying a Single, Integrated Framework—There are many IT-related standards and good practices, each providing guidance on a subset of IT activities. COBIT 5 aligns with other relevant standards and frameworks at a high level, and thus can serve as the overarching framework for governance and management of enterprise IT.

COBIT 5: Enabling Information aligns with the COBIT 5 framework and the information model included in COBIT 5. It is a unique framework that not only provides effective information governance and management, but also provides a single model for information that is applicable to all types of information used within the enterprise.

Principle 4: Enabling a Holistic Approach—Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines seven categories of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise:
- Principles, Policies and Frameworks
- Processes
- Organisational Structures
- Culture, Ethics and Behaviour
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

COBIT 5: Enabling Information focuses on information. In this guide, the Information enabler is discussed and illustrated in substantially more detail than in the COBIT 5 framework publication. All the other enablers also support the Information enabler.

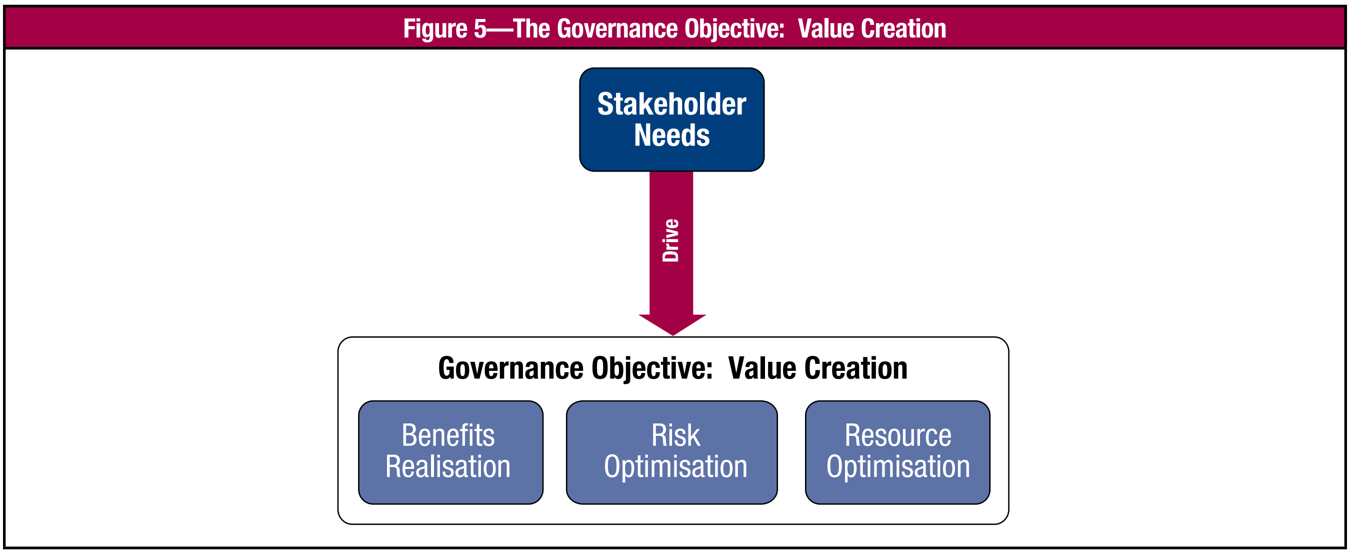
Principle 5: Separating Governance From Management—The COBIT 5 framework makes a clear distinction between governance and management, i.e., they encompass different types of activities, require different organisational structures and serve different purposes.

COBIT 5: Enabling Information distinguishes between information governance and information management in section 2.1.5 Separating Governance From Management, later in this chapter.

2.1.1 Meeting Stakeholder Needs

Enterprises exist to create value for their stakeholders. Consequently, any enterprise—commercial or not—has value creation as a governance objective. **Value creation means realising benefits at an optimal resource cost while optimising risk.** (See **figure 5.**) Benefits can take many forms, e.g., financial for commercial enterprises and high-quality public service for government entities.

Figure 5—The Governance Objective: Value Creation



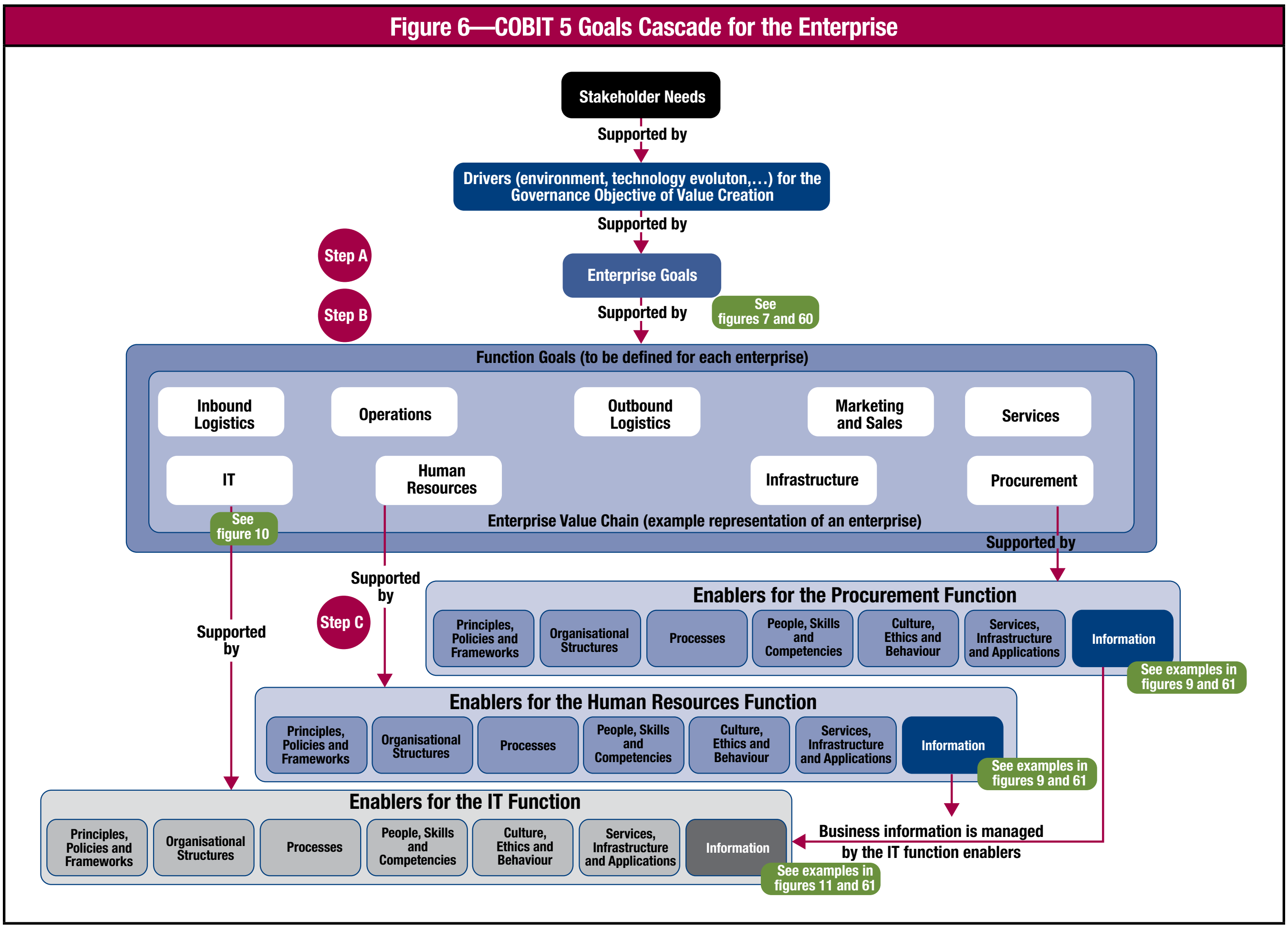
Enterprises have many stakeholders, and 'creating value' means different—and sometimes conflicting—things to each of them. Governance is about negotiating and deciding amongst different stakeholders' value interests. By consequence, the governance system should consider all stakeholders when making benefit, risk and resource assessment decisions. For each decision, the following questions should be asked:

- For whom are the benefits?
- Who bears the risk?
- What resources are required?

Stakeholder needs must be transformed into the 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 the enterprise to set specific goals at every level and in every area, in support of the overall goals and stakeholder requirements.

Figure 6 shows an extension of the generic COBIT 5 goals cascade. The three steps in the goals cascade are explained in the following paragraphs.

Figure 6—COBIT 5 Goals Cascade for the Enterprise


Stakeholder Needs
Supported by
Drivers (environment, technology evoluton,…) for the Governance Objective of Value Creation
Supported by
Step A
Enterprise Goals
Step B
Supported by
See figures 7 and 60
Function Goals (to be defined for each enterprise)
Inbound Logistics
Operations
Outbound Logistics
Marketing and Sales
Services
IT
Human Resources
Infrastructure
Procurement
See figure 10
Enterprise Value Chain (example representation of an enterprise)
Supported by
Supported by
Step C
Supported by
Enablers for the Procurement Function
Principles, Policies and Frameworks
Organisational Structures
Processes
People, Skills and Competencies
Culture, Ethics and Behaviour
Services, Infrastructure and Applications
Information
See examples in figures 9 and 61
Enablers for the Human Resources Function
Principles, Policies and Frameworks
Organisational Structures
Processes
People, Skills and Competencies
Culture, Ethics and Behaviour
Services, Infrastructure and Applications
Information
See examples in figures 9 and 61
Enablers for the IT Function
Principles, Policies and Frameworks
Organisational Structures
Processes
People, Skills and Competencies
Culture, Ethics and Behaviour
Services, Infrastructure and Applications
Information
Business information is managed by the IT function enablers
See examples in figures 11 and 61

STEP A. GOVERNANCE OBJECTIVE INFLUENCES ENTERPRISE GOALS

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

Stakeholder needs can be related to a set of generic enterprise goals. These enterprise goals have been developed using the balanced scorecard (BSC)[2] 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.

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

COBIT 5 defines 17 generic goals, as shown in **figure 7**, which includes the following information:

- BSC dimension under which the enterprise goal fits
- Enterprise goals
- 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.)

Enterprises must define their own enterprise-specific goals based on their stakeholders' needs.

Figure 7—Generic Enterprise Goals (COBIT 5 Framework)

BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	EG01. Stakeholder value of business investments	P		S
	EG02. Portfolio of competitive products and services	P	P	S
	EG03. Managed business risk (safeguarding of assets)		P	S
	EG04. Compliance with external laws and regulations		P	
	EG05. Financial transparency	P	S	S
Customer	EG06. Customer-oriented service culture	P		S
	EG07. Business service continuity and availability		P	
	EG08. Agile responses to a changing business environment	P		S
	EG09. Information-based strategic decision making	P	P	P
	EG10. Optimisation of service delivery costs	P		P
Internal	EG11. Optimisation of business process functionality	P		P
	EG12. Optimisation of business process costs	P		P
	EG13. Managed business change programmes	P	P	S
	EG14. Operational and staff productivity	P		P
	EG15. Compliance with internal policies		P	
Learning and Growth	EG16. Skilled and motivated people	S	P	P
	EG17. Product and business innovation culture	P		

STEP B. ENTERPRISE GOALS DRIVE FUNCTION GOALS

Achievement of **enterprise goals** requires a number of successful outcomes of underlying business functions, which are represented by the **function goals**. Functions can include any business function, e.g., in the value chain representation of an enterprise, this includes any component of the value chain as illustrated in **figure 6**.

STEP C. FUNCTION GOALS DRIVE ENABLER GOALS

Achieving **business-function-related goals** requires the successful application and use of a number of enablers. Enablers are those things that influence the likelihood of achieving something. **Figure 6** shows the enablers for three of the nine business functions: procurement function, human resources function and IT function. The enabler concept is valid for any business function, and it is explained in detail in the COBIT 5 framework. For each enabler, a set of specific relevant goals can be defined in support of the business function goals.

In the goals cascade, all enablers—in this case, Information—should serve one or more enterprise goals and thus contribute to the overall value delivery of the enterprise. Chapter 3 further elaborates on the enablers.

2.1.2 Covering the Enterprise End-to-end

While different domains may have specialised vocabularies (some quite technical), information is relevant to the entire enterprise, throughout all business functions.

The goals cascade in **figure 6** shows:

- The business functions procurement, human resources and IT further expanded, illustrating that functions are supported by all enabler types.
- The interconnection that is relevant in the context of information. For example, any information enabling the operations function or the procurement function also requires the IT-function enablers, i.e., procurement and operations need information provided and processed by the technology function.

- The IT function, while supporting other business functions also requires its own enablers, which include information. These are information items[3] of a different nature compared to business information, i.e., they are IT-specific information items, but they should be considered. Examples include IT asset registries, change records and trouble tickets.

Each process in the value chain is supported by the same categories of enablers, including the Information enabler. In the case of non-IT processes, the information items may be based in traditional 'business' domains, such as sales, logistics and marketing. Note that all of these areas may have their own specialised, in-depth, technical terminology not readily understandable by generalists. These business information items are usually managed and supported by IT, i.e., by the COBIT 5 IT-related enablers, as discussed previously.

Figure 6 illustrates that the key COBIT 5 concepts—goals cascade and enablers—not only apply to IT-related processes and goals, but to any other business process and its related goals. Hence, the COBIT 5 information model can serve any type of information generated, processed, communicated, etc., by the enterprise.

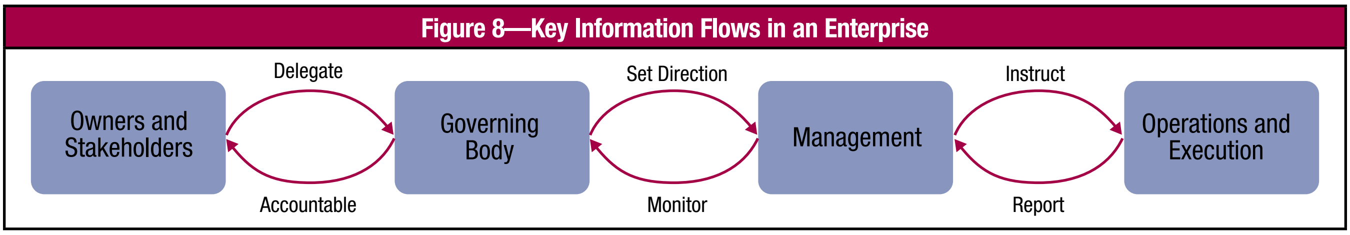
Information is not only a resource for business functions, but also is often a part of the primary product/service that the enterprise produces, i.e., the output of a business process.

2.1.2.1 Specific (Business) Information Items Supporting Business Function Goals

The term 'information' covers a widely varying spectrum. One way to understand this wide spectrum is to look at the key use of an information item in relation to the overall enterprise.

Figure 8 shows the purpose of communication of information between the key areas of responsibility in an enterprise. This flow of information can be applied to any functional area in the enterprise, e.g., any business process, and the IT area.

Figure 8—Key Information Flows in an Enterprise



The figure also shows the **types** of information items flowing between the enterprise levels, e.g., the governing body requires adequate information items to support its effort to set the direction for management.

Figure 9 shows examples of the business information items that support the goals achievement of the expanded human resources and procurement value-chain functions (shown in **figure 6**) and identifies whether the information items concern the governing body, management, or operations and execution enterprise levels. Information can relate to any of the communication streams depicted in **figure 8**, e.g., operational information generated/used during operations and execution. (Information items that support the goals achievement of IT function are discussed in section 2.1.2.2 and shown in **figure 11**.)

Note: Appendix B contains a comprehensive table of the business information items that support the goals achievement of all the value-chain functions shown in **figure 6** and identifies the enterprise levels between which the information items flow during communication.

[3] An information item is any individual enterprise information asset or governance and management enabler that has a specific defined set of attributes. The COBIT 5 inputs and outputs, i.e., process work products or artefacts, can be considered information items when being viewed through information enabler attributes. Other examples of information items can be found in appendices B and C. See appendix H in the COBIT 5 framework for the complete COBIT 5 glossary.

Figure 9—Examples of Information Items in Information Flows That Support the Enterprise Value Chain Goals

Functional Area	Key (Business) Information Items Required to Support Achievement of the Enterprise Goals		
	Governing Body	**Management**	**Operations and Execution**
Human resources (goals)	• Reporting on allocation and effectiveness of resources and capabilities • Budget communications • Request fulfilment status and trends report • Guiding principles for allocation of resources and capabilities • Success measures and results • Salary information (human cost allocation status of each department or business unit)	• Remedial actions to address resource management deviations • Operation and use plan • Root causes of quality delivery failures • Budget allocations • Resource budget and plan • IT budget and plan • Communication of resourcing strategies • Skills and competencies matrix turnover ratios • Salary information (salary tables, human cost analysis) • 360-degree review feedback results	• Approved resources plan • Skills and competencies matrix • Incident status and trends report • Salary information • Performance reports • 360-degree review feedback results
Procurement (goals)	• Business cases • Legal and regulatory requirements • Information on required production goods and services • Information on required maintenance, repairs and operations supplies • Sourcing strategy	• Legal and regulatory requirements • Contractual requirements • Supplier information • Requests for information • Requests for proposals • Tenders • Warranties • Contract terms • Sourcing strategy	• Supplier information • Requests for information • Requests for proposals • Proposals • Warranties • Contract terms

Excerpt from appendix B, figure 71

2.1.2.2 IT-related Information Items Supporting IT Function Goals

Figure 6 shows that the enterprise IT function is also supported by the seven enablers, including Information. Achievement of enterprise goals requires a number of IT-related outcomes, which are represented by the IT-related goals. 'IT-related' means information and related technology. The IT-related goals are structured according to the dimensions of the IT balanced scorecard (IT BSC). The information items that are required to support the achievement of the IT-related goals are related to (and often internal to) the IT function. A comprehensive set of 17 generic and high-level IT-related goals are defined in the COBIT 5 framework and are listed in **figure 10**. Enterprises must define their own enterprise-specific goals that are based on their stakeholders' needs.

Figure 10—Generic IT-related Goals

IT BSC Dimension	Information and Related Technology Goal
Financial	ITG01. Alignment of IT and business strategy
	ITG02. IT compliance and support for business compliance with external laws and regulations
	ITG03. Commitment of executive management for making IT-related decisions
	ITG04. Managed IT-related business risk
	ITG05. Realised benefits from IT-enabled investments and services portfolio
	ITG06. Transparency of IT costs, benefits and risk
Customer	ITG07. Delivery of IT services in line with business requirements
	ITG08. Adequate use of applications, information and technology solutions
Internal	ITG09. IT agility
	ITG10. Security of information, processing infrastructure and applications
	ITG11. Optimisation of IT assets, resources and capabilities
	ITG12. Enablement and support of business processes by integrating applications and technology into business processes
	ITG13. Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	ITG14. Availability of reliable and useful information for decision making
	ITG15. IT compliance with internal policies
Learning and Growth	ITG16. Competent and motivated business and IT personnel
	ITG17. Knowledge, expertise and initiatives for business innovation

The COBIT 5 enabler model builds on seven interconnected and interrelated enablers (see section 2.1.4 Enabling a Holistic Approach). Therefore, the Information enabler does not stand on its own but is linked to the other enablers, as in the following examples:

- Processes require information as inputs to process, and deliver information as outputs.
- Services, infrastructure and applications provide the means by which information is processed.
- People deal with information continually, in business processes and in IT processes.

The COBIT 5 process descriptions in the *COBIT 5: Enabling Processes* guide list the inputs and outputs associated with each process practice. **These inputs and outputs are a set of information items required to support the IT-related goals.**

Figure 11 shows examples of how each IT-related goal can be supported by specific (IT-related) information items. The table contains sample information items that support the generic IT-related goals from the COBIT 5 framework and:

- Illustrative quality criteria (explained in chapter 3) for the information item
- Potential metrics that can be used to assess the information quality

Appendix C contains a comprehensive table of the IT-related goals and the key information items that support the achievement of those goals. **Figure 11** illustrates an excerpt of the appendix C table.

Note: The key information items that are required to achieve the IT-related goal, even when satisfying all quality criteria, are not sufficient. Goal achievement depends on all the other related enablers, as well.

The table is not complete and aims to illustrate the thought process that can be applied to use the goals cascade for the Information enabler.

Figure 11—Information Items Supporting IT-related Goals

Generic IT-related Goals		Key Information Items to Support Achievement of the IT-related Goal	Illustrative Quality Criteria	Related Metrics
ITG01	Alignment of IT and business strategy	IT strategy plan	• Currency	Time since last update of the IT strategic plan
		Enterprise strategy	• Completeness	Percentage of IT-related goals that are translated into potential IT-enabled investment programmes (road map)
		Investment types and criteria	• Reputation, • Believability • Relevancy	Benchmark investment portfolio composition against industry (industry analyst reports)
		Performance reports	• Accuracy • Currency • Concise representation	Ease of reading and understanding by stakeholders
			• Relevance • Completeness	Stakeholder satisfaction with scope of the planned portfolio of programmes and services
ITG02	IT compliance and support for business compliance with external laws and regulations	• IT-related compliance requirements register • Compliance assurance reports	• Accuracy • Completeness • Currency	Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss
			• Accuracy • Completeness • Currency • Concise representation • Interpretability	Number of IT-related non-compliance issues reported to the board of directors or causing public comment or embarrassment
			• Accuracy • Completeness • Currency • Concise representation • Interpretability	Number of non-compliance issues relating to contractual agreements with IT service providers
			• Accuracy • Completeness • Currency	Coverage of compliance assessments
Excerpt from appendix C, figure 72				

Note: See appendix C for a comprehensive table of the typical information items that support the achievement of all 17 IT-related goals from the COBIT 5 goals cascade.

2.1.3 Applying a Single Integrated Framework

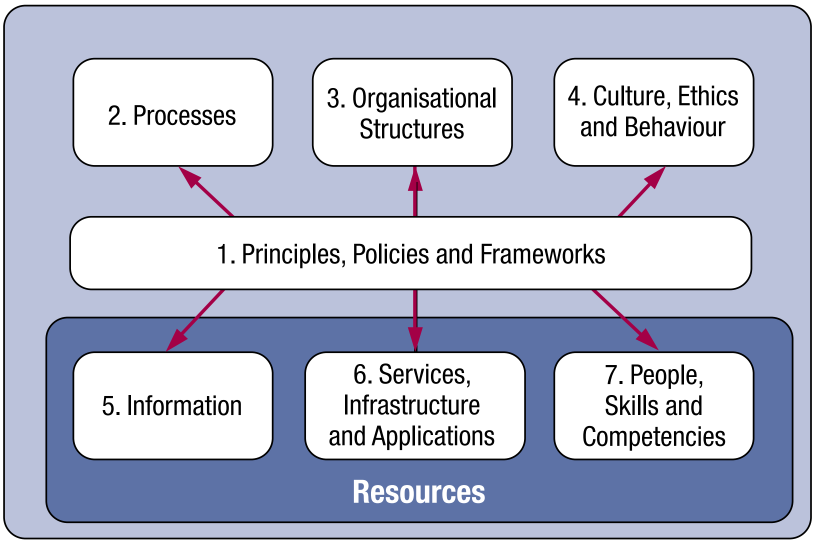
COBIT 5: Enabling Information aligns with the COBIT 5 framework and the information model included in COBIT 5, providing a unique framework that not only provides effective information governance and information management, but also overall governance and management of enterprise IT.

Another significant framework in the information management area is the Data Management Body of Knowledge (DMBOK), sponsored by the Data Management Association International (DAMA), the primary professional organisation that specialises in the area of data and information management. *COBIT 5: Enabling Information* does not provide the same amount of detail when compared to DMBOK, but the key concepts in both frameworks align well, and at no place do the frameworks contradict each other—they can be considered complementary. More information on how both frameworks compare and complement each other can be found in appendix A.

2.1.4 Enabling a Holistic Approach

Efficient and effective governance and management of enterprise IT requires a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are factors that, individually and collectively, influence whether something will work—in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve. The COBIT 5 framework defines seven categories of enablers, as shown in **figure 12**.

Figure 12—COBIT 5 Enablers


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

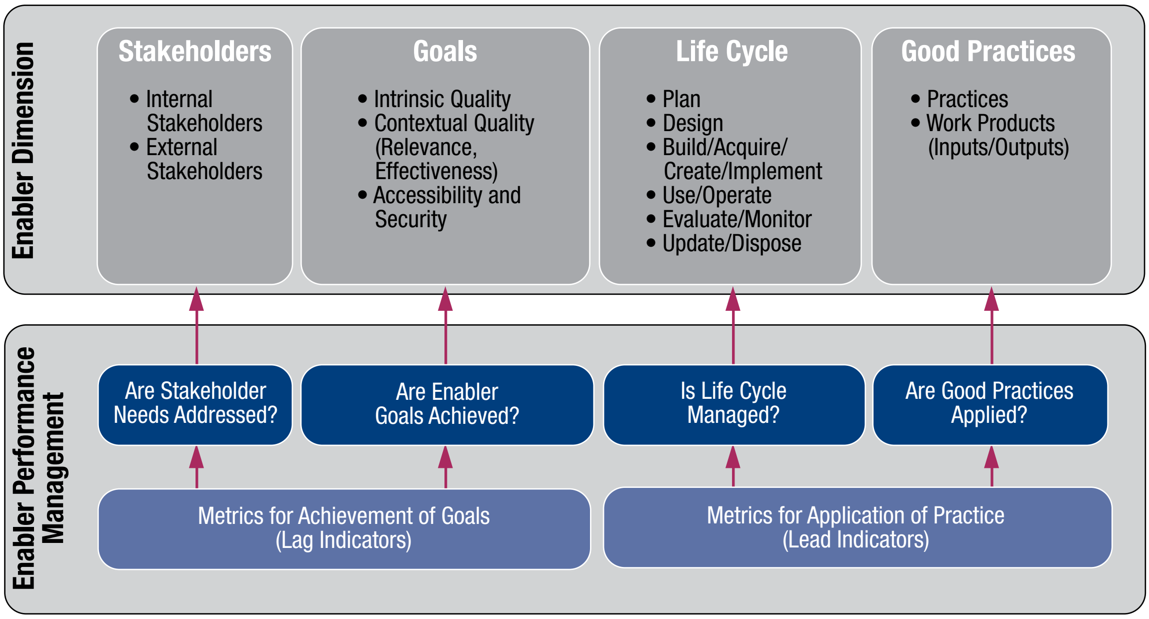
2.1.4.1 THE COBIT 5 ENABLER MODEL

The COBIT 5 enablers, as introduced in **figure 12**, can be applied in practical situations and can be used to implement effective and efficient information governance and information management in the enterprise.

All enablers defined in COBIT 5 have a set of common dimensions that are illustrated in the COBIT 5 enabler model (**figure 13**). These dimensions:

- Provide a simple and structured way to deal with enablers.
- Allow enterprises to manage their complex interactions.
- Facilitate successful outcomes of the enablers.

Figure 13—COBIT 5 Generic Enabler Model


Enabler Dimension
Stakeholders
• Internal Stakeholders
• External Stakeholders
Goals
• Intrinsic Quality
• Contextual Quality (Relevance, Effectiveness)
• Accessibility and Security
Life Cycle
• Plan
• Design
• Build/Acquire/ Create/Implement
• Use/Operate
• Evaluate/Monitor
• Update/Dispose
Good Practices
• Practices
• Work Products (Inputs/Outputs)
Enabler Performance Management
Are Stakeholder Needs Addressed?
Are Enabler Goals Achieved?
Is Life Cycle Managed?
Are Good Practices Applied?
Metrics for Achievement of Goals (Lag Indicators)
Metrics for Application of Practice (Lead Indicators)

2.1.4.2 DIMENSIONS OF THE GENERIC ENABLER MODEL

The four common dimensions for enablers are:

- **Stakeholders**—Each enabler has stakeholders, which are parties who play an active role and/or have an interest in the enabler. For example, processes have different parties who execute process activities and/or who have an interest in the process outcomes; organisational structures have stakeholders—each with their own roles and interests—that are part of the structures. Stakeholders can be internal or external to the organisation, all having their own—sometimes conflicting—interests and needs. Stakeholders' needs translate to enterprise goals, which in turn translate to IT-related goals for the enterprise.
- **Goals**—Each enabler has a number of goals, which are expected outcomes. Enablers provide value by the achievement of these goals. The enabler goals are the final step in the COBIT 5 goals cascade. Goals can be further divided into different categories:
  - Intrinsic quality—The extent to which enablers provide accurate, objective and reputable results
  - Contextual quality—The extent to which enablers and their outcomes are fit for purpose given the context in which they operate. For example, outcomes should be relevant, complete, current, appropriate, consistent, understandable, easy to use and agile.
  - Access and security—The extent to which enablers are accessible—available when and if needed—and secured, i.e., access is restricted to those entitled and needing it
- **Life cycle**—Each enabler has a life cycle, from inception through an operational/useful life until disposal. This applies to information, structures, processes and policies, etc. The phases of the life cycle consist of:
  - Plan (includes concepts development and concepts selection)
  - Design
  - Build/acquire/create/implement
  - Use/operate
  - Evaluate/monitor
  - Update/dispose
- **Good practices**—For each of the enablers, good practices can be defined. Good practices support the achievement of the enabler goals, provide examples or suggestions on how to best implement the enabler, and provide the required work products or inputs and outputs. After these good practices are properly tuned and successfully integrated within the enterprise, they can become, through follow up of the changing business needs and proper monitoring, best practices for the enterprise.

In chapter 3, the Information enabler model is explained in more detail and illustrated with several examples.

2.1.5 Separating Governance From Management

The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organisational structures and serve different purposes. The COBIT 5 view on this key distinction between governance and management is explained in the following paragraphs.

2.1.5.1 INFORMATION GOVERNANCE AND INFORMATION MANAGEMENT DEFINED

The term data governance and management and the term information governance and management are very often used interchangeably or are used to describe very similar activities. This guide focuses on the distinction between governance and management, not on the less clear difference between data and information. Hence, this guide uses the terms information governance and information management.

2.1.5.2 INFORMATION GOVERNANCE

COBIT 5 defines governance as:

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

This definition reflects the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 38500-based definition of governance, with the three key activities evaluate, direct and monitor represented. Monitoring in the governance context means ensuring that monitoring outcomes are achieved in support of the provided direction and the expected objectives.

DMBOK defines data governance as:

> *Data governance is the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets. The data governance function guides how all other data management functions are performed. Data governance is high-level, executive data stewardship.*[4]

The COBIT 5 and DMBOK definitions are not entirely aligned, in that some **governance** activities in the DMBOK definition are considered **management** activities in COBIT 5, e.g., planning is a management activity in COBIT 5, whereas monitoring and enforcement, which, depending on the context, can be management or governance activities.

Based on the previous descriptions and staying aligned with the overall COBIT 5 definition of governance, information governance can be described as follows.

Information governance ensures that:
- Stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives, which are to be achieved through the acquisition and management of information resources.
- Direction is set for information management capabilities through prioritisation and decision making.
- Performance and compliance of the information resource are monitored against agreed-on direction and objectives.

Information governance activities include:
- Communicating information strategies, policies, standards, architecture and metrics
- Tracking and enforcing regulatory compliance and conformance to information policies, standards, architecture and procedures
- Sponsoring, tracking and overseeing the delivery and operational execution of information management programmes
- Providing an understanding, based on stakeholder needs, of the decisions and priorities associated with information resources

2.1.5.3 INFORMATION MANAGEMENT

Information management is encountered as one or more specific areas of practice in many organisations, with various names, such as data architecture, data management, data administration, database administration, data warehousing, data/information governance, business intelligence (BI) and analytics, information architecture, information resource management, enterprise architecture, enterprise content management, and/or records management.

For the purpose of this guide, information management encompasses the management of structured and unstructured data, in electronic, paper or other media formats. It may encompass portions of knowledge management as a formalised organisational capability.

COBIT 5 defines management as:

> *Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.*

[4] Data Management Association International (DAMA), *The DAMA Guide to the Data Management Body of Knowledge* (DMBOK), USA, 2009

In this definition, 'monitoring' represents monitoring that management activities are occurring as expected, in alignment with the plan, build and run activities.

DMBOK defines data management as:

> *The planning and execution of policies, practices, and projects that acquire, control, protect, deliver, and enhance the value of data and information assets.*[5]

Both definitions are aligned, although the COBIT 5 definition emphasises that management has to align with the direction set by the governance body.

Based on the previous descriptions, and staying aligned with the overall COBIT 5 definition of management, information management can be described as follows.

Information management plans, builds, runs and monitors the practices, projects and capabilities that acquire, control, protect, deliver and enhance the value of data and information assets, in alignment with the direction set by the information governance body.

[5] Data Management Association International (DAMA), *The DAMA Guide to the Data Management Body of Knowledge* (DMBOK), USA, 2009

Page intentionally left blank

Chapter 3
The COBIT 5 Information Model

In chapter 2, it was established that information is relevant throughout any enterprise, for any business process. From this, the following questions arise:

- How should enterprises deal with information?
- What do information practitioners need to consider to make information valuable for the enterprise?

These questions are addressed by the COBIT 5 information model. This model was originally developed in the COBIT 5 framework publication and covers all information types in any size and type of enterprise. **Figure 14** lists the practical uses of this model for different information stakeholders.

Figure 14—Practical Use of the Information Model

Practical Use of the Information Model for Stakeholders	Board of Directors and Executive Management (CEO, COO, CFO)	CIO and IT Senior Management	Business Process Owners	Enterprise Architects, Data Stewards	IT Architect, IT Solutions Development	IT Operations	IT Security, Continuity and Privacy Professionals	Internal Audit and Compliance, Risk Management
Define and assign accountability and responsibility during different life cycle stages of information, e.g., during planning, design, build, use, monitoring, storage and disposal of sensitive information	✔	✔	✔					
Define quality criteria for information across a range of different quality goals, e.g., relevancy, completeness, restricted access	✔	✔	✔	✔				
Define all attributes of information items required for efficient and effective design, development and use of information by business functions		✔	✔	✔	✔			
Understand which information items (and their criticality) are managed through the applications that are being operated and supported				✔	✔	✔		✔
Understand which information items are managed through the applications that are being operated and supported and ensure they are managed according to their materiality/criticality			✔	✔	✔	✔	✔	✔
Relate security and availability requirements to the wider concept of quality criteria for information across a range of 15 quality goals				✔	✔	✔	✔	✔
Define all attributes of information items required for efficient and effective protection of information							✔	✔

3.1 COBIT 5 Information Model Overview

The COBIT 5 Information Model (**figure 15**) is based on the generic COBIT 5 enabler model (as explained in chapter 2). In this chapter, each of the four enabler dimensions for the Information enabler is discussed in detail and illustrated with examples.

3.1.1 Stakeholders

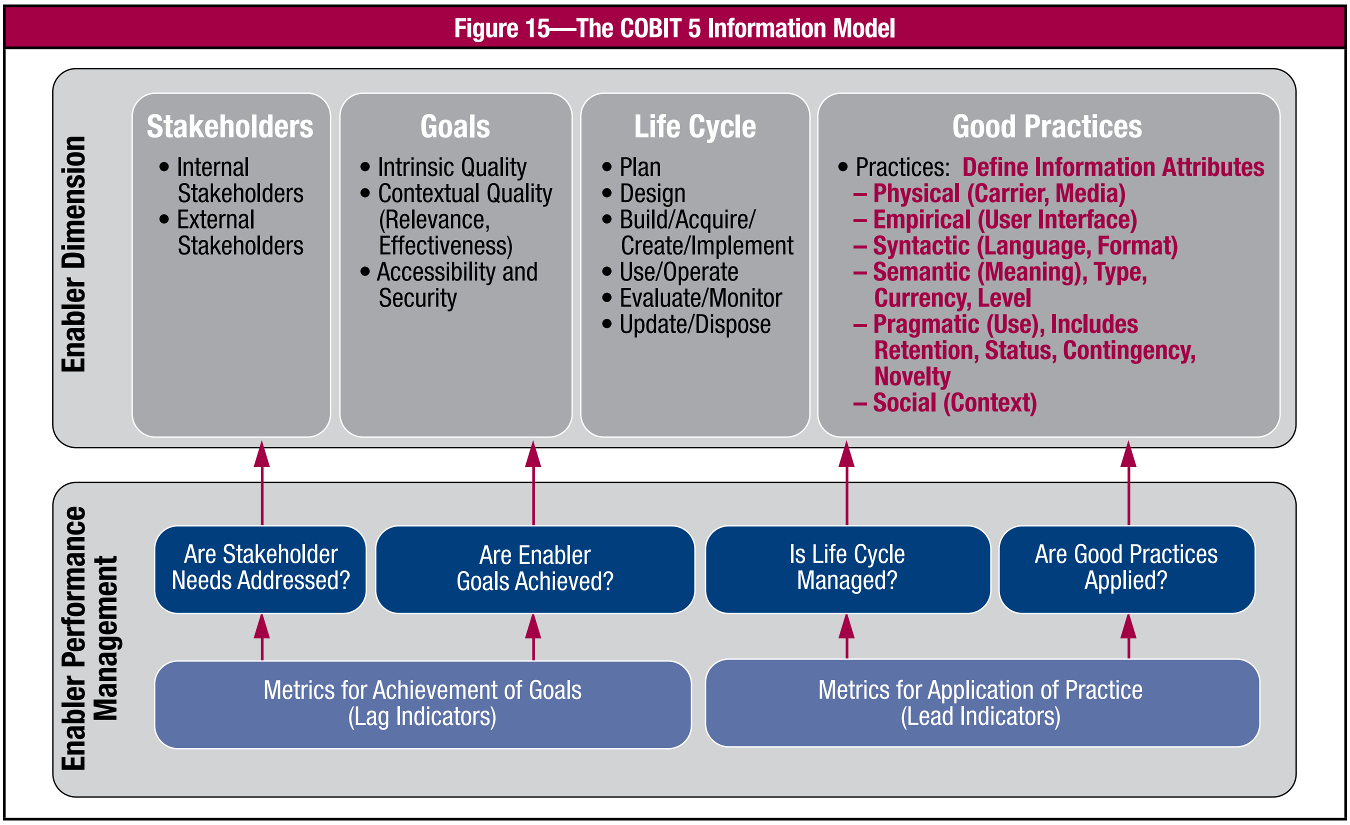
Stakeholders can be internal or external to the enterprise. The generic model suggests that, apart from identifying the stakeholders, their stakes need to be identified, i.e., why they care or are interested in the information.

Stakeholders can be categorised by their roles in dealing with information, ranging from detailed roles, e.g., specific data or information roles like architect, owner, steward, trustee, supplier, beneficiary, modeller, quality manager, or security manager, to more general roles, e.g., distinguishing amongst information producers, information custodians and information consumers, as follows:

- Information producer—Responsible for creating the information[6]
- Information custodian—Responsible for storing and maintaining the information
- Information consumer—Responsible for using the information

[6] In this context, it should be noted that the concept 'information owner' is often used. 'Information producer' includes the data owner, who is ultimately accountable in the enterprise for the existence of the information item type, and other roles that create actual information items.

Figure 15—The COBIT 5 Information Model


Enabler Dimension
Stakeholders
• Internal Stakeholders
• External Stakeholders
Goals
• Intrinsic Quality
• Contextual Quality (Relevance, Effectiveness)
• Accessibility and Security
Life Cycle
• Plan
• Design
• Build/Acquire/ Create/Implement
• Use/Operate
• Evaluate/Monitor
• Update/Dispose
Good Practices
• Practices: Define Information Attributes
– Physical (Carrier, Media)
– Empirical (User Interface)
– Syntactic (Language, Format)
– Semantic (Meaning), Type, Currency, Level
– Pragmatic (Use), Includes Retention, Status, Contingency, Novelty
– Social (Context)
Enabler Performance Management
Are Stakeholder Needs Addressed?
Are Enabler Goals Achieved?
Is Life Cycle Managed?
Are Good Practices Applied?
Metrics for Achievement of Goals (Lag Indicators)
Metrics for Application of Practice (Lead Indicators)

These categorisations refer to specific activities regarding the information resource. Activities depend on the life cycle phase of the information. Therefore, to find a categorisation of roles that has an appropriate level of granularity for the information model and to ensure internal consistency, the information life cycle dimension of the information model can be used.

This means that information stakeholder roles can be defined in terms of information life cycle phases, for example:
- Information planners
- Information acquirers
- Information users

The information stakeholder dimension is not an entirely independent dimension; different life cycle phases have different stakeholders. An additional feature of this approach of defining stakeholder roles in terms of information cycle phases is the frequently used and suggested concepts of 'information demand' and 'information supply'.[7]

Whereas the relevant roles depend on the information life cycle phase, the stakes can be related to information goals. The actual stakeholders, i.e., the persons or organisational structures that assume the stakeholder roles include the entire enterprise, e.g., staff, customers, auditors, internal or external IT service providers, business partners and regulators.

3.1.1.1 Stakeholder Information Items and Their Relationships to Information Stakeholders

The following examples contain some stakeholder information items and their relationships to information stakeholders. They identify and describe the stakeholders during the different stages in an information item's life cycle as it flows through an enterprise. Examples are provided for the following stakeholder information items:
- Customer data—See **figure 16**.
- The IT strategy—See **figure 17**.
- Supply chain software specification document—See **figure 18**.
- Hospital patient records—See **figure 19**.

[7] It is suggested by some that these two concepts are equivalent to the 'business' and the 'IT' side of an organisation, but this guide does not completely accept that approach. The present information determines the demanding party and the supplier. The business side can be the demander for some information, but, at the same time, the supplier of other information. The IT function provides IT services, e.g., the use of applications and associated data sources, to the business, from which the business derives information. So there is a demand-supply-use relationship between the business (demand/use) and IT (supply), with respect to IT services, but not with regard to information (other than information about IT services). Within the business, there is demand, supply and use of information. The IT function also needs information to support its own activities, which have demand, supply and use of information.

Figure 16—Customer Data Information Stakeholders

Stakeholder	Internal/External	Description/Stake
• Sales and marketing • Other enterprise functions	I	• Customer data is perhaps the most valuable data to the modern enterprise and can take various forms depending on use. Both marketing and sales are primary stakeholders, but virtually any constituent function of an enterprise may come in contact with customer data in some form. • Customer data origination occurs in multiple forms. Daily data entry by various organisational functions may capture customer or prospective customer data via various channels and related to various functions: marketing, sales, receivables or support.
Information architect	I	• It is rare that an enterprise can design customer data from the beginning, as virtually any enterprise from inception has a need to track customer data in some form. More typical of this particular data subject are substantial integration and reconciliation problems: reconciling marketing with sales data, sales data with accounts receivable and accounts receivable with customer service. • Master data management approaches may constitute an important part of an integrated data architecture design, intended to bring disparate customer data repositories into alignment. Data quality metrics are essential.
Information security	I	The security classification of customer data is critical. Some of the most critical customer data, (usually personally identifiable data or health-related data) is regulated and can be very damaging to both the enterprise and its customers if mishandled.
Data owners	I	Data owners monitor the customer data for target quality levels to be achieved.
Audit	I/E	• Auditors are concerned with both the security and proper disposal of customer data; they perform testing to ensure compliance with both external regulations and internal policies. • Auditors are also concerned with other criteria, e.g., effectiveness, efficiency and relevancy.
Customers	I/E	Customers have the right to ask details about their customer data, request changes and request disposal.
Privacy regulators	E	Regulators take interest in customer data from a data privacy and security perspective.
Data brokers	E	Prospective customer data may be purchased from data brokers.

Figure 17—IT Strategy Information Stakeholders

Stakeholder	Internal/External	Description/Stake
Board of directors	I	Defines the enterprise goals and objectives, which serve as the basis for the IT strategy, IT goals and objectives.
CIO	I	Defines the IT strategy and road map, based on enterprise goals and objectives.
IT management	I	The IT strategy defines priorities and sets direction for the IT services and activities to be performed and managed by IT.
Enterprise architects	I	The enterprise architects use the IT strategy as an input when looking for innovation opportunities and aligning the enterprise architecture.
Users	I	The IT strategy should be communicated to all users to create awareness and understanding of IT objectives and priorities.
Audit	I/E	Auditors perform testing to ensure compliance with both external regulations and internal policies and need information on the IT strategy of the organisation as an input for these checks.
Suppliers	I/E	Suppliers might be interested to see how the services that they deliver fit into the IT strategy of the organisation and how they can deliver value to the business through IT.
Customers	E	Customers might have an interest in the IT strategy of the organisation, e.g., when security of transactions is highly important, online services are delivered to the customer or innovative services are expected to be launched.

Figure 18—Supply Chain Software Specification Document Information Stakeholders

Stakeholder	Internal/External	Description/Stake
Supply chain management	I	Supply chain management needs to be involved when defining business specifications and functionalities for new software tools that are developed. These specifications need to be documented in the specification document.
Enterprise and information architects	I	Enterprise and information architects need to be involved when defining technical software specifications to ensure that the design aligns with the enterprise architecture.
External IT development sourcing partners	E	External developers need to fine tune the software design based on the business and technical specifications and needs that were defined by supply chain management and IT.
Users	I/E	Users of the supply chain software need this information item to be able to understand the specifications and functionalities of the new software and use it.
External supply chain partners	E	External partners often have interfaces or dependencies with the supply chain of the organisation. They need to be aware of the use of new software and restrictions or opportunities that come with it.
Audit	I/E	Audit needs to be aware of the software specifications to understand how the business process is supported, which dependencies exist and what results are achieved.

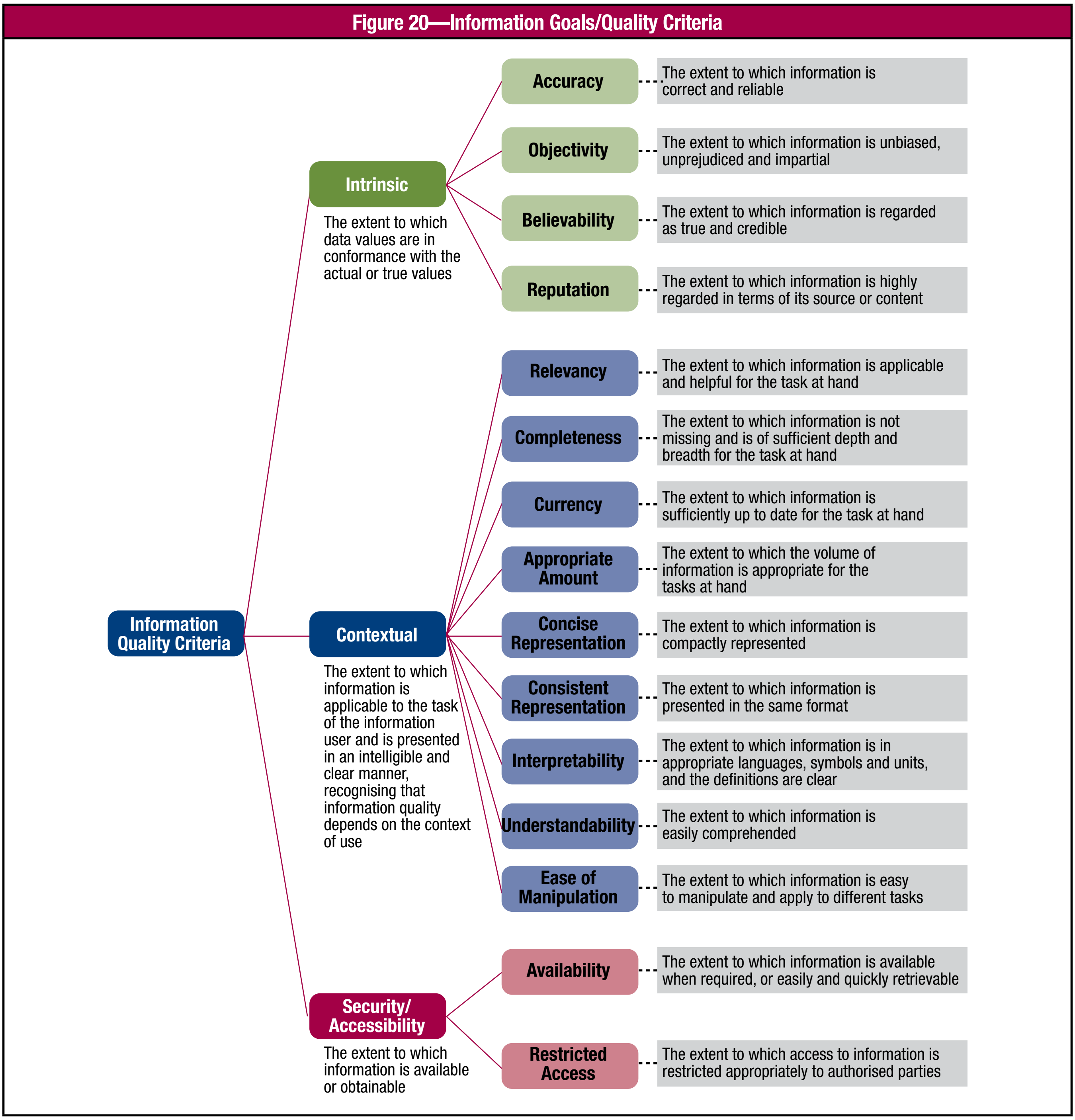
Figure 19—Hospital Patient Medical Records Information Stakeholders

Stakeholder	Internal/External	Description/Stake
Medical doctors	I	Medical doctors provide input to a medical record of a patient, to support optimal care and satisfy all legal and contractual requirements.
IT architects, IT development	I	IT architects design the patient medical records within the IT systems and define interfaces to the required applications. IT development builds or acquires a technical solution, with or without support from external providers.
Data steward	I	The data steward ensures transparency regarding data use; participation of individuals in the use of health data; adherence to privacy and confidentiality policies, principles and practices; ensures proper administration or administrative, technical and physical safeguards; and provides accountability, enforcement and remediation mechanisms as needed.
Information security	I	Information security needs to ensure that patient medical records are secure (supporting accurate, reliable and available-when-needed information requirements) and that information is adapted, stored and disposed of in compliance with policies and regulations.
Medical and quality assurance staff	I	Medical staff and quality assurance staff test the solution to determine whether it meets all quality criteria and requirements. In operations, they need to ensure that quality of input remains adequate. Medical staff decide when information can be disposed of, if at all, which depends on applicable legal and contractual requirements.
IT operations	I	IT operations ensure that the systems and information remain operational.
Patients	E	The well-being of patients depends on adequacy of the medical records. Patients have an interest in secure, accurate and reliable medical records that are available when needed.
Insurance companies (life, health)	E	Insurance companies process personal and medical records information to provide insurance benefits to their customers as and when appropriate.
Regulators	E	Regulators take interest in patient medical records from a data privacy and security perspective.

3.1.2 Goals

The goals of information are expressed as quality criteria to be achieved. The criteria are divided into three subdimensions of quality: intrinsic, contextual and security/accessibility. Each subdimension is divided further into several quality criteria, which are defined in **figure 20**.

Figure 20—Information Goals/Quality Criteria



Information Quality Criteria

- **Intrinsic**: The extent to which data values are in conformance with the actual or true values
  - **Accuracy**: The extent to which information is correct and reliable
  - **Objectivity**: The extent to which information is unbiased, unprejudiced and impartial
  - **Believability**: The extent to which information is regarded as true and credible
  - **Reputation**: The extent to which information is highly regarded in terms of its source or content
- **Contextual**: The extent to which information is applicable to the task of the information user and is presented in an intelligible and clear manner, recognising that information quality depends on the context of use
  - **Relevancy**: The extent to which information is applicable and helpful for the task at hand
  - **Completeness**: The extent to which information is not missing and is of sufficient depth and breadth for the task at hand
  - **Currency**: The extent to which information is sufficiently up to date for the task at hand
  - **Appropriate Amount**: The extent to which the volume of information is appropriate for the tasks at hand
  - **Concise Representation**: The extent to which information is compactly represented
  - **Consistent Representation**: The extent to which information is presented in the same format
  - **Interpretability**: The extent to which information is in appropriate languages, symbols and units, and the definitions are clear
  - **Understandability**: The extent to which information is easily comprehended
  - **Ease of Manipulation**: The extent to which information is easy to manipulate and apply to different tasks
- **Security/ Accessibility**: The extent to which information is available or obtainable
  - **Availability**: The extent to which information is available when required, or easily and quickly retrievable
  - **Restricted Access**: The extent to which access to information is restricted appropriately to authorised parties

3.1.2.1 Information Quality Goals Example

Figure 21 lists all quality goals and subgoals and their descriptions and briefly discusses them or provides a short example.

Figure 21—Information Goals/Quality Criteria Discussion and Examples

Quality Goal/Subgoal	Description: The extent to which…	Example(s)
Intrinsic/accuracy	information is correct and reliable.	• Customer data: Is the customer's address accurate? • Medical records: Is the patient's medical history correct? Has it been validated?
Intrinsic/objectivity	information is unbiased, unprejudiced and impartial.	Objectivity is a very important quality goal for information items that serve as the basis for enterprise decision making. Examples are business cases, risk assessments and audit reports. Example: One could assume that customer data information includes creditworthiness or reputation of the customer. This information should be objective and not merely based on individual evaluations or judgement.
Intrinsic/believability	information is regarded as true and credible.	Believability often relates to highly aggregated information, typically in a governance flow. Examples: Risk analysis, competitive analysis and market forecast are typical information items where believability is a key quality goal.
Intrinsic/reputation	information is highly regarded in terms of its source or content.	Reputation might severely compromise an information item's value, e.g., in the case of an information source with poor reputation, the information will less likely be used to its full potential. Example outcome of poor reputation: 'I do not trust the CRM system because it is not in alignment with the accounts receivable system. You have to manually find the customer in both places and change the address in both places, and the name might not even be the same'.
Contextual/relevancy	information is applicable and helpful for the task at hand.	Relevancy is an important attribute of the planning and architecture processes. The distinction needs to be made between relevant and irrelevant data, always considering the context/purpose of the information. Include information that serves a purpose, and avoid including information 'because we can'. Example outcome of information that is not relevant: 'I do not know why we are collecting and maintaining customer pet name; it is not used in any report and has only 0.01% completeness in the database'.
Contextual/ completeness	information is not missing and is of sufficient depth and breadth for the task at hand.	Completeness is one of the most frequently quantified data quality metrics. It could be enforced via system mechanisms, but risk increases if the requirement for completeness causes value eroding delays in record entry. Example: Capture only the customer name and phone number if they are a sales prospect. To ask for their address at that time may be inappropriate. Example outcomes of missing information: • 'The system requires me to enter the customer address, but sometimes the sales team does not provide it, so the order just sits there on my desk while I chase down the address. Sometimes this slows down the entire process'. • 'It is optional to add zip code; it always has been. It might have made sense a long time ago, but nowadays there is no good reason to not have a zip code. We run a data quality report and still about 5 percent of records do not have zip codes. We cannot bulk mail to those people. We periodically scrub the addresses against the postal service master, but a few months later, there we are again with incomplete records'.
Contextual/currency	information is sufficiently up to date for the task at hand.	Information that is not up to date might indicate delay in processes, but can also cause delay in processes, operational errors or decisions that are made on the wrong basis. Examples: • 'We have customer records that have not shown any activity for ten years. We know that the older the record, the more likely we no longer have a correct address'. • 'If an incident is logged in the IT service desk, we start to track how long it remains open. Anything that is open longer than 36 hours, with no updates, is flagged. Usually those indicate a data-entry follow-up failure'.
Contextual/appropriate amount	the volume of information is appropriate for the task at hand.	The quantity of data presented has two aspects: the number of records presented and the number of attributes per record, all relative to the purpose at hand. Example outcome of inappropriate amount: 'That report has all the data you need, but it is impossible to figure out without going through page after page of stuff you do not need'. Example outcome of appropriate amount: 'It is a huge data set, but we are using state of the art visualisation techniques so you can really see what is going on and where the hot spots are'.
Contextual/ concise representation	information is compactly represented.	Usually, the decision of how much data to present is a matter of usability engineering, screen design and/or report design. Example outcome of representation that is not concise: 'I cannot stand the customer screen design in that old ERP system. The developers put 50 attributes on a screen and it is impossible to get anything done'.

Figure 21—Information Goals/Quality Criteria Discussion and Examples *(cont.)*

Quality Goal/Subgoal	Description: The extent to which…	Example(s)
Contextual/ consistent representation	information is presented in the same format.	Consistency is often an issue when data is replicated across two repositories. Example outcome of inconsistent representation: 'We get a feed from the general ledger of the account codes. It is only updated monthly, but they can add a new code any time; so, we sometimes do not have the code that people want to enter'. Example of inconsistent representation: date format is different between data repositories, e.g., DD/MM/YY, MM/DD/YY.
Contextual/ interpretability	information is in appropriate languages, symbols and units and the definitions are clear.	Internationalisation is a key requirement for modern enterprise software. Example outcome of in sufficient interpretability: 'The system is outdated. It does not even support Unicode, and we have international customers whose names we cannot properly represent without that'.
Contextual/ understandability	information is easily comprehended.	A system can be 'correct' in terms of data structure and yet still be hard to understand. Example outcome of poor understandability: 'Because of the many codes/abbreviations used, it is really hard to figure out the customer history'.
Contextual/ease of manipulation	information is easy to manipulate and apply to different tasks.	Interacting with the data is the primary concern of usability engineering. Example outcome of difficult manipulation: 'The customer data screens are OK to look at, but updating them is way too labour intensive. You have to click about five times on various buttons to update even the simplest thing. Also, it is not easy to extract customer information and to process it in other applications'.
Security/accessibility/ availability	information is available when required, or easily and quickly retrievable.	If the system is down or degraded, the user cannot access the data. Example outcome of poor availability: 'The customer database crashed and we have not been able to restore a backup. Our business operations are starting to lose serious money'.
Security/accessibility/ restricted access	information is restricted appropriately to authorised parties.	Data access must be controlled and available only to the appropriate and authorised personnel. Example of appropriate information restriction: 'While any operator can see the customer's address, we only allow senior customer service operators and above to see the customer's tax ID number and bank account number'.

3.1.2.2 INFORMATION QUALITY GOALS MAPPED TO SECURITY CIA

The basic information security concept of confidentiality, integrity and availability (CIA) is globally accepted among security professionals. COBIT 5 covers the CIA criteria in the information enabler as information goals. **Figure 22** shows how CIA maps to the COBIT 5 information quality criteria, as defined in the information model.

Figure 22—Information Quality Criteria Mapped to Security CIA

Security (CIA)	COBIT 5 Information Quality Criteria
Confidentiality	Restricted access
Integrity	The combination of: • Completeness • Accuracy
Availability	Timely and reliable access

3.1.3 Life Cycle

The full life cycle of information needs to be considered, and different approaches may be required for information in different phases of the life cycle.

Figure 23—Information Life Cycle

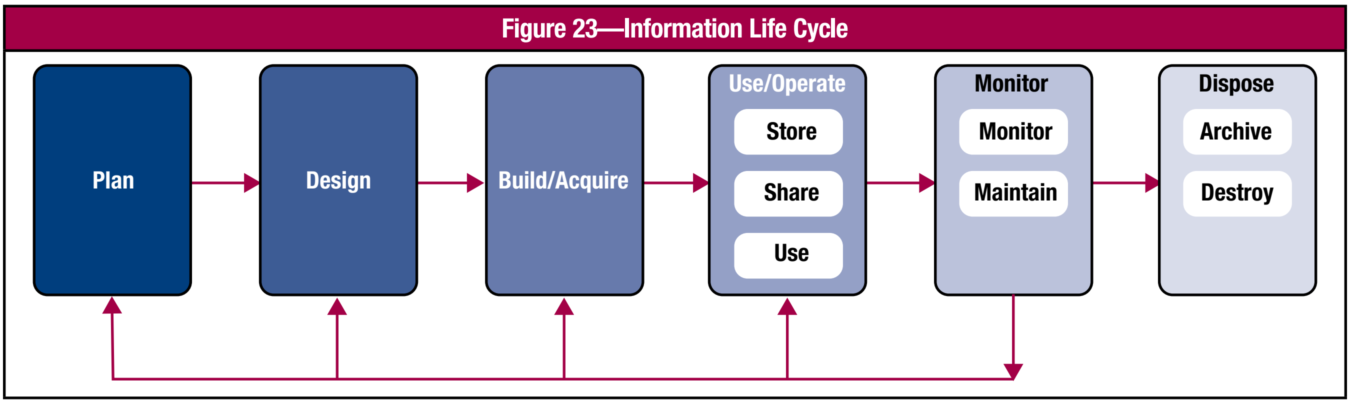
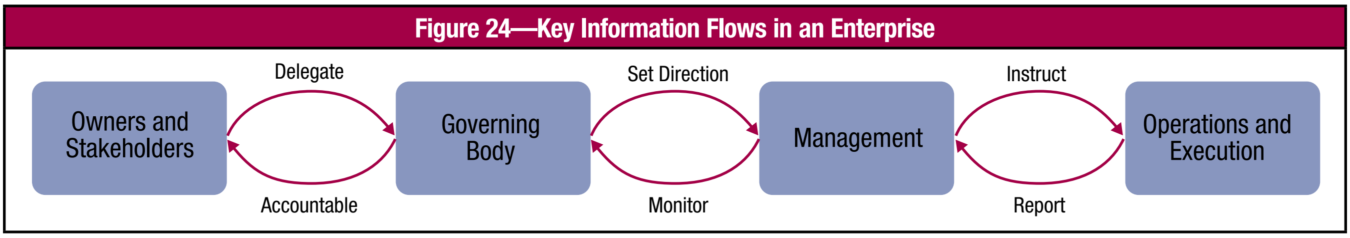


Figure 23 shows how the COBIT 5 Information enabler distinguishes the life cycle phases:

- **Plan**—The phase in which the creation, acquisition and use of the information resource is prepared. Activities in this phase include understanding information use in the respective business processes, determining the value of the information asset and its associated classification, identifying objectives, and planning the information architecture.
- **Design**—The phase in which more detailed work is done in specifying how the information will look and how systems processing the information will have to work. Activities in this phase may refer to the development of standards and definitions (e.g., data definitions, data collection, access, storage procedures and metadata characteristics).
- **Build/acquire**—The phase in which the information resource is acquired. Activities in this phase may refer to the creation of data records, the purchase of data and the loading of external files.
- **Use/operate**—This phase includes:
  - Store—The phase in which information is held electronically or in hard copy (or even just in human memory). Activities in this phase may refer to the storage of information in electronic form (e.g., electronic files, databases, data warehouses) or as hard copy (e.g., paper documents).
  - Share—The phase in which information is made available for use through a distribution method. Activities in this phase may refer to the processes involved in getting the information to places where it can be accessed and used (e.g., distributing documents by email). For electronically held information, this life cycle phase may largely overlap with the store phase (e.g., sharing information through database access, file/document servers).
  - Use—The phase in which information is used to accomplish (IT-related and thus enterprise) goals. Activities in this phase may refer to all kinds of information usage (e.g., managerial decision making, running automated processes), and also include activities such as information retrieval and converting information from one form to another.

  Information use as defined in the information model can be thought of as the purposes for which enterprise stakeholders need information when assuming their roles, fulfilling their activities and interacting with each other. There are many types of information and many different ways to classify information as well. The interactions between stakeholders require information flows. The COBIT 5 framework provides the flow of information between governance and management roles, as shown in **figure 24**.

Figure 24—Key Information Flows in an Enterprise



  Information can relate to any of the communication streams depicted in figure 24, including operational information generated/used during operations and execution.

  Investments in information and related technology are based on business cases which include cost-benefit analysis. Costs and benefits refer not only to tangible, measurable factors, but they also take into account intangible factors such as competitive advantage, customer satisfaction and technology uncertainty. It is only when the information resource is applied or used that an enterprise generates benefits from it, so the value of information is determined solely through its use (internally or by selling it), and information has no intrinsic value. It is only through putting information into action that value can be generated.
- **Monitor**—The phase in which it is ensured that the information resource continues to work properly (i.e., to be valuable). Activities in this phase may refer to keeping information up to date as well as other kinds of information management activities (e.g., enhancing, cleansing, merging, removing duplicate information data in data warehouses).
- **Dispose**—The phase in which the information resource is transferred or retained for a defined period, destroyed, or handled as part of an archive as needed. Activities in this phase may refer to information retention, archiving or destroying.

3.1.3.1 LIFE CYCLE EXAMPLES

Figure 25 describes the overall life cycle of the information category supplier information.

Figure 25—Example Information Life Cycle for Supplier Information

Life Cycle Stage	Description
Plan	Consider overall business requirements—through defined stakeholder value proposals, business strategy and objectives, business model, and corresponding sourcing strategy—to plan management of supplier information (identification, collection, declaration, classification, storage, disposal, etc.). For example: Supplier information will be collected by the procurement department and stored in the supplier management system.
Design	Design the supplier information elements: carrier, media, access channel, code language, type, currency, retention period, contingency and use contexts, etc. For example: Business has designed a common integrated automated supplier system that requires suppliers to input their information in a specified standard format directly on an online system.
Build/acquire	Build/acquire the supplier information elements (supplier database, supplier management system, payment methods, etc.). For example: Business has set up a project management team to acquire and implement a new sourcing software application or an e-invoicing module. In the case of integrated systems with the supplier systems, the supplier's ISMS may be reviewed at this time.
Use/operate: store, share, use	Consider/utilise supplier information to perform the business sourcing activities, such as: • Ranking suppliers • Selecting suppliers based on set criteria • Pay suppliers—debit/credit • Update (delete, add and maintain) supplier information For example: Analytics over suppliers—through consolidating supplier network information relative to total purchases the business has identified an opportunity to negotiate supplier price reductions.
Monitor	Continuously check and evaluate/assess the elements of the supplier information to ensure continuous alignment with business sourcing and overall strategy. These elements include, for example: • Carrier (soft copy, hard copy) • Media • Access channel • Code language • Type • Currency • Retention period • Contingency • Use contexts For example: Business has decided to not accept supplier information in hard copy, effective with the next business cycle.
Dispose	Dispose of the information, as identified during the supplier information design, taking into account the regulatory and business retention requirements. For example: Business requires disposal of supplier records that are over 10 years old (retention period determined in the design phase).

Figure 26 describes the life cycle of the information item retention requirements, i.e., a policy document describing the requirements for business information retention.

Figure 26—Example Information Life Cycle for Retention Requirements

Life Cycle Stage	Description
Plan	Establish the need for formalised records retention. Determine the scope, approach, and relationship to enterprise policy. Scope and initiate implementation initiative(s). For example: A project is defined to detail retention requirements and implement the new policy within the enterprise.
Design	Determine the detailed structure for records taxonomy. Determine the technology requirements and design for supporting retention requirements. For example: An archiving functionality is designed to ensure that required information is stored for the minimum-defined retention period.
Build/acquire	Build and implement according to the retention requirements specifications. This includes developing and implementing operational procedures, technology solutions, etc. For example: Operational procedures for information archiving and automatic disposal after retention period are implemented.
Use/operate: store, share, use	Apply the operational procedures and technology solutions to comply with retention requirements. For example: Operational procedures for information archiving and automatic disposal after retention period are in use.
Monitor	Monitor whether retention requirements are: • Still aligned with legal and regulatory requirements • Retention requirements are complied with For example: Monitor if no supplier information is being disposed within the regulatory retention period.
Dispose	Records management data, itself, should be kept, effective-dated (full audit trail), in perpetuity, because the enterprise may be legally liable to report on its retention schedules for any given point in time, for any data topic that the enterprise has ever managed. For example: If the enterprise kept customer data for life + 7 years between 1990 and 2000, and reduced this to life + 5 years for 2001 and after, the effective retention time in effect for 1990 to 2000 may still be needed, in case of litigation involving that time frame.

Figure 27 describes the life cycle phases of IT change management data and change requests.

Figure 27—Example Information Life Cycle for IT Change Management Data

Life Cycle Stage	Description
Plan	Change Management is typically implemented as a standard process. Part of the process design is specifying the scope, characteristics and location of IT change data or change requests. For example: The enterprise architecture should define the existence and integration of one or more change data repositories (independent of particular implementation). If multiple repositories are specified, master data management principles should be employed to determine which repositories are authorised to originate change data (system of record [SOR]) and which repositories must simply replicate the change data from the authorised systems of record. If multiple systems will originate change data (e.g., a mainframe environment maintains a separate repository) the specific business rules by which the data will be integrated in the various repositories must be defined.
Design	Specify the logical change data in terms of the change process requirements. Specific questions include: • Which data attributes are associated with the change? • What other data entities may be relevant to changes? Establish the record class[8], if appropriate, and define the retention period. Assess the potential sensitivity of change data. In general, the change process seeks to inform all stakeholders of a planned change. Often, change data is widely available to IT personnel. However, consider whether wide availability could be a point of vulnerability. Knowing that a system is being changed could enable a successful exploit. Other changes might be related to confidential strategic or security-related initiatives and should only be reported on a need-to-know basis. Define change reporting, as appropriate. Identify data quality metrics reflecting the process architecture and KPIs. See process BAI06 *Manage changes* in the *COBIT 5: Enabling Processes* guide. For example: • Should a change be related to the project that drives the initiative, to associated releases, to service requests, to work orders, to configuration items? • Should change data be accessible to the entire organisation, all IT personnel, selected groups, etc.? • Should a change classification be applied to restrict access? The change data may be widely shared by other systems, such as project and release management, and may also be important to the IT data warehouse or similar analytic capabilities. Conversely, the project system may provide project IDs and names for easy association with changes, and, similarly, for releases, incidents, and other primary IT data entities. Reporting might be established for changes without associated configuration items, changes whose approval window has been exceeded, changes with no sponsoring project or related incident, etc.
Build/acquire	The logical change data specification that was designed implies requirements to the acquisition and implementation process. For example: Access to categories of change data needs to be configured in the appropriate systems to ensure restricted access of confidential or strategic information.
Use/operate: store, share, use	Provide training on appropriate use of the change system and compliance with change design requirements (setup, storage, etc.). Ensure that interfaces to upstream and downstream systems are functional. The change system is, itself, a production application and subject to the change process, as well as other operational processes and practices, such as monitoring, capacity management, service level management, and so forth. For example: Change data should be entered according to the change process documentation, which should clearly specify which data is required, recommended and optional. The system should be designed, as much as possible, to support the user in meeting the process requirements. Required change data should be enforced via constraints on data entry or at least exception reporting.
Monitor	Monitor change data quality and compliance with design requirements. Report on exceptions, both for remediation and root cause analysis (continuous improvement). The change process should be a top priority for IT continuous improvement. For example: Monitor compliance with completion and approval deadlines. Take appropriate action if stakeholders do not comply with the process.
Dispose	Change data should have a defined retention period and be disposed of accordingly. Its susceptibility and importance to legal discovery may be of interest to discuss amongst the change management staff, the legal counsel and the records management staff. Note that long horizon retention of some summary change data (e.g., success/failure rates) might be advisable for tracking IT service quality over time. For example: Detail-level change request information is retained for three years and is afterwards disposed of according to the standard disposal process. Aggregate change reporting may be retained indefinitely for historical purposes.

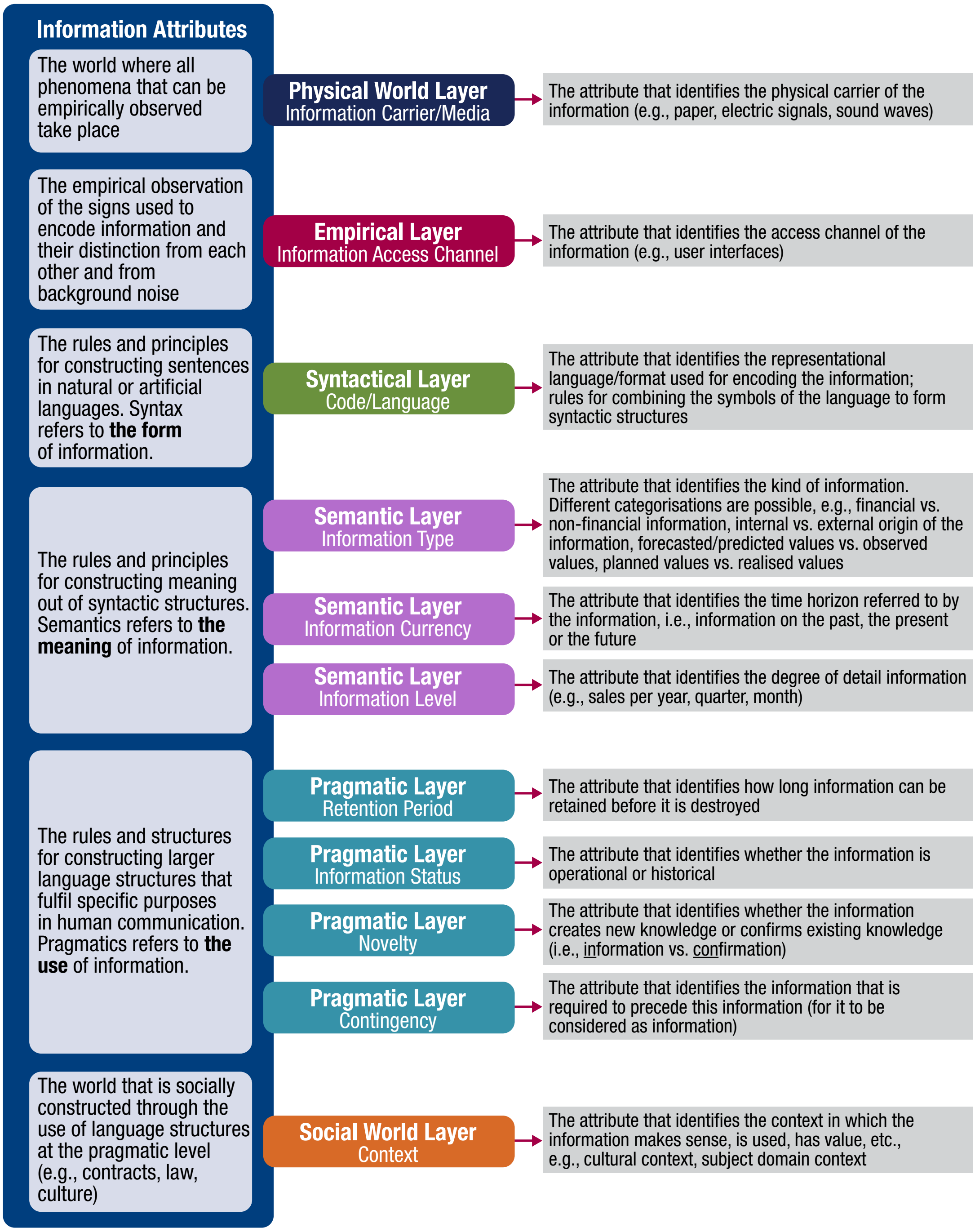
[8] Considering record class codes as a data subject in their own right introduces the concept of metadata, i.e., data about data. This can be a difficult concept to grasp, but is an essential component of information governance and management.

3.1.4 Good Practices

The concept of information is understood differently in different disciplines, such as economics, communication theory, information science, knowledge management and information systems. Therefore, there is no universally agreed-on definition for information. The nature of information, however, can be clarified through defining and describing its properties.

The scheme shown in **figure 28** is proposed to structure the different properties: It consists of six levels, or layers, to define and describe properties of information. These six levels present a continuum of attributes, ranging from the physical world of information, where attributes are linked to information technologies and media for information capturing, storing, processing, distribution and presentation, to the social world of information use, sense-making and action.

Figure 28—Information Attributes



Information Attributes

The world where all phenomena that can be empirically observed take place

Physical World Layer Information Carrier/Media → The attribute that identifies the physical carrier of the information (e.g., paper, electric signals, sound waves)

The empirical observation of the signs used to encode information and their distinction from each other and from background noise

Empirical Layer Information Access Channel → The attribute that identifies the access channel of the information (e.g., user interfaces)

The rules and principles for constructing sentences in natural or artificial languages. Syntax refers to **the form** of information.

Syntactical Layer Code/Language → The attribute that identifies the representational language/format used for encoding the information; rules for combining the symbols of the language to form syntactic structures

The rules and principles for constructing meaning out of syntactic structures. Semantics refers to **the meaning** of information.

Semantic Layer Information Type → The attribute that identifies the kind of information. Different categorisations are possible, e.g., financial vs. non-financial information, internal vs. external origin of the information, forecasted/predicted values vs. observed values, planned values vs. realised values

Semantic Layer Information Currency → The attribute that identifies the time horizon referred to by the information, i.e., information on the past, the present or the future

Semantic Layer Information Level → The attribute that identifies the degree of detail information (e.g., sales per year, quarter, month)

The rules and structures for constructing larger language structures that fulfil specific purposes in human communication. Pragmatics refers to **the use** of information.

Pragmatic Layer Retention Period → The attribute that identifies how long information can be retained before it is destroyed

Pragmatic Layer Information Status → The attribute that identifies whether the information is operational or historical

Pragmatic Layer Novelty → The attribute that identifies whether the information creates new knowledge or confirms existing knowledge (i.e., information vs. confirmation)

Pragmatic Layer Contingency → The attribute that identifies the information that is required to precede this information (for it to be considered as information)

The world that is socially constructed through the use of language structures at the pragmatic level (e.g., contracts, law, culture)

Social World Layer Context → The attribute that identifies the context in which the information makes sense, is used, has value, etc., e.g., cultural context, subject domain context

3.1.4.1 GOOD PRACTICE EXAMPLE

Figure 29 gives the information good practice attributes for customer data, what the attribute identifies and example values for customer data.

Figure 29—Information Good Practice Attributes for Customer Data

Attribute	Identifies…	Example(s)
Physical/ information carrier/media	the physical carrier of the information.	The selected physical data management platform, e.g., a particular relational database management system (RDBMS) on a particular server.
Empirical/ information access channel	the access channel of the information.	Customer data might be accessed over Structured Query Language (SQL) middleware over a TCP/IP connection. This implies using several layers of the communications stack, SQL operating at the application level and the rest at lower levels.
Syntactical/ code/language	the representational language/ format used for encoding the information.	Examples of symbol sets encoding the data are Roman, Cyrillic and Unicode. Examples of formats are string, digit and date. A customer's name might be in Roman characters in the Unicode character set and associated notes about their related transactions might be written in English. Names are textual strings, as are addresses and emails; some postal codes are all digits while others are an alphanumeric mix. Phone numbers typically are all digits. Associated transactions may be dollars tied to dates. Record creation and update dates are time stamps.
Semantic/ information type	the kind of information.	Customer data often includes personal data, e.g., name, birth date, address. Other types of information with regards to customer data might include financial data when looking into customer spending, observed values and forecasted values when analysing customer purchasing, etc.
Semantic/ information currency	the time horizon referred to by the information.	Customer data could be on the past, on the present (if it has been updated very recently) or on the future (if forecasts or predictions are made). Not all data needs to be updated as frequently: addresses might need regular revision whereas the birth date of a person does not change.
Semantic/ information level	the degree of detail of the information level.	Customer data may be segmented and aggregated in various ways. More static approaches might include by city, state and region, or by the primary channel serving that customer. More dynamic approaches might be defined for the customer's purchasing habits, attempting to segment them into general buying populations (e.g., upscale technology enthusiast, suburban mother).
Pragmatic/ retention period	how long information can be retained before it is destroyed.	Customer data is often assigned a defined retention schedule, for example life of the customer's active business relationship with the enterprise plus seven years (after seven years of inactivity, the customer record is purged).
Pragmatic/ information status	whether the information is operational or historical.	Customer data moves through a life cycle and may be flagged as inactive prior to purging. Related customer records might be current or historical, e.g., current open orders vs. closed orders. Historical audit trails on attributes such as customer address and contact information may be kept.
Pragmatic/ novelty	whether the information creates new knowledge or confirms existing knowledge.	A customer record may contain an indicator for confirming accuracy at a point in time. If a company representative speaks to the customer and the customer indicates his/her address is still correct as represented in the company's system, the system may provide the capability to confirm this. Trend analysis on customers' purchasing habits may confirm known patterns or show new trends.
Pragmatic/ contingency	the information that is required to precede this information.	Customer data might be contingent on other information, e.g., product information or sales records, before it can be used as intended or be turned into knowledge. Some companies may distinguish between prospective and actual customers, but, in general, the data is sufficient unto itself.
Social/context	the context in which the information makes sense, is used, has value, etc., e.g., cultural context, subject domain context.	Customer data tracks, at the highest level, the marketing, sales, logistics, financials and support life cycle of product delivery. A customer might originate as a lead from a marketing-sourced commercial data system, be converted via a sales system to a true customer, flow into the receivables and delivery systems, and finally end up in the support system. Other companies may use one common master data system to approach all of these business activities.

3.2 Additional Examples of COBIT 5 Information Model Use

3.2.1 Sample Use Cases for the COBIT 5 Information Model

The COBIT 5 information model is rich in terms of different components. To illustrate and inspire the many possible uses of this model, additional examples are shown in **figures 30** through **34**.

Figure 30—Building Information System Specifications

When developing a new application, the information model can be used to assist with the specifications of the application and the associated information or data models. The information attributes of the information model can be used to define specifications for the application and the business processes that will use the information. The model helps to ensure that all types of requirements are included.

For example, the design and specifications of the new system need to specify:
- Physical layer—Where will information be stored?
- Empirical layer—How can the information be accessed?
- Syntactical layer—How will the information be structured and coded?
- Semantic layer—What type of information is it? What is the information level?
- Pragmatic layer—What are the retention requirements? What other information is required for this information to be useful and usable?
- Social layer—What is the context that is important when using the information? What knowledge prerequisites are needed?

Looking at the stakeholder dimension combined with the information life cycle, one can define who needs what type of access to the data, during which phase of the information life cycle, and the responsibilities for each stakeholder in each phase. When the application is tested, testers can look at the information quality criteria to develop a comprehensive set of test cases.

Figure 31—Definition of Information Protection Requirements

Security groups within the enterprise can benefit from the attributes dimension of the information model. When charged with protection of information, they need to look at:
- Physical layer—How and where is information physically stored?
- Empirical layer—What are the access channels to the information?
- Semantic layer—What type of information is it? Is the information current or relating to the past or to the future?
- Pragmatic layer—What are the availability and retention requirements? Is information historic or operational?

Using these attributes allows security groups to determine the level of protection and the protection mechanisms required. Addressing such questions effectively is essential because enterprises increasingly need to address privacy concerns related to personally identifiable information and protection of other types of valuable information assets, e.g., intellectual property.

Looking at another dimension of the information model, security professionals can consider the stakeholders and information life cycle stages, because information needs to be protected during all phases of the life cycle, as well as accessible by the appropriate stakeholders. Security starts at the information planning phase and implies different protection mechanisms for storing, sharing and disposition of information. The information model ensures that information is protected during the full life cycle of the information.

Figure 32—Determine Ease of Data Use

When performing a review of a business process (or an application), the information model can be used to assist with a general review of the information processed and of the underlying information systems. The quality criteria can be used to assess the extent to which information is available—whether the information is complete, available on a timely basis, factually correct, relevant and available in the appropriate amount. One can also consider the accessibility criteria—whether the information is accessible when required and adequately protected. The review can be even further extended to include representation criteria, e.g., the ease with which the information can be understood, interpreted, used and manipulated.

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

Figure 33—Modelling of Application Control Practices

Risk associated with any business process and complex processing of business information introduces further risk. Application control practices are intended to provide reasonable assurance that business objectives relative to a given application are being achieved. Management objectives are typically articulated through the definition of specific functional requirements for the solution, the definition of business rules for information processing and the definition of supporting manual procedures.

Examples include:
- Completeness—The application processes all transactions and the resulting information is complete.
- Accuracy—All transactions are processed accurately and as intended and the resulting information is accurate.
- Validity—Only valid transactions are processed and the resulting information is valid.
- Authorisation—Only appropriately authorised transactions have been processed.
- Segregation of duties—The application provides for and supports appropriate segregation of duties and responsibilities as defined by management.

When dealing with application control practices, the following risk needs to be identified, assessed and responded to:
- Physical layer—What is the risk related to errors or inefficiencies that may be made during the physical capture of information?
- Empirical layer—What is the risk related to lack of data integrity, erroneous or illegitimate transactions being processed, invalid or unauthorised updates being processed and unauthorised changes?
- Semantic layer—What is the risk when bypass, overrides or manual entries are made to avoid automated application control practices? These functions are inherent in most, if not all, application systems.
- Pragmatic layer—What is the risk of loss of confidentiality or unavailability of information when it is required?

Figure 34—Developing a System of Internal Control

The requirement for effective internal control has been well established for some time. However, as a result of the Sarbanes-Oxley Act in the United States and similar legislation in other jurisdictions around the world, significant attention has been focused recently on a specific subset of management objectives as they relate to financial information: ensuring that internal control over financial reporting has been designed appropriately and is operating effectively to reduce the risk of a material misstatement in financial statements and related disclosures.

The information model information goals help to establish internal control over financial reporting. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control-Integrated Framework is often used as the base reference for internal control guidance. COSO states that information is needed at all levels of an organization to run the business and achieve the entity's business objectives. The determination of which information is required to achieve the required business objectives, and the communication of this information in a form and time frame that allow people to carry out their duties can be done with the help of the information model.

COSO also notes that the quality of information is key to achieving business goals and, for example, includes ascertaining whether the information has:
- Intrinsic quality:
  - Accuracy—Is the data correct?
- Contextual and representational quality:
  - Appropriate—Is it the right information?
  - Timely—Is it available when required and reported in the right period of time?
  - Current—Is it the latest available?
- Security/accessibility quality:
  - Accessible—Can only authorised individuals gain access to it as necessary?

These example requirements and others that may apply to information quality clearly link back to the quality goals of the information model.

3.2.2 Comprehensive Information Item Description—Risk Profile

The information dimension information stakeholders, goals and quality criteria, life cycle phases, and good practices and information attributes were discussed in previous sections. This section contains an example of an information item that has all of its information dimension descriptions completed, i.e., a 'risk profile'. (See **figure 35**.) The risk profile aggregates all the information dimensions described in earlier sections. It can be useful for addressing information–centric questions, such as for:

- **Risk managers:**
  - What does a risk profile look like?
  - What are the quality criteria for a risk profile (and how can they be achieved)?
  - Who are important stakeholders?
  - What are their stakes?
  - What are good practices?
  - What are related enablers, etc.?
- **Auditors:**
  - How can I review the quality of a risk profile?
  - What are the criteria that I need to review?
- **Stakeholders:** What responsibilities do I have in the life cycle of the risk profile?

Additional elaborated examples of information items specific to risk, assurance and information security are detailed in the respective ISACA publications *COBIT 5 for Risk*, *COBIT 5 for Assurance* and *COBIT 5 for Information Security*.

Figure 35—Information Item Risk Profile

A risk profile is a description of the overall (identified) risk to which the enterprise is exposed. A risk profile consists of:

- **Risk register**
  - **Risk scenarios**
  - **Risk analysis**
- **Risk action plan**
- **Loss events (historical and current)**
- **Risk factors**
- **Independent assessment findings**

	Life Cycle Stage	Internal Stakeholder	External Stakeholder	Description/Stake
Life Cycle and Stakeholders	**Information planning**	ERM committee, board	External audit, regulator	• Internal stakeholders: Initiate and drive the implementation and appoint a CRO. Have adequate information on the exposure. • External stakeholders: To have comfort on the risk management capabilities
	Information design	Risk function, compliance, CIO, CISO, business process owners, internal audit		• CRO: To obtain information from the other roles in order to provide the overview for the governance bodies • CIO: To be able to develop an adequate information system • Other roles: To be able to provide relevant information and to ensure completeness/adequacy
	Information build/acquire	Risk function, internal audit		• CRO: Provides functional requirements and consults others. • Internal audit: Provides quality assurance services on the implementation.
	Information use/operate: store, share, use	Board, ERM committee, business executive, CIO, risk function, CISO, business process owners, compliance, internal audit	External audit, regulator	• Business process owners, business executives and CIO: To efficiently provide relevant information • Board and ERM committee: To receive relevant information and to enable decision making • Internal audit, external audit and regulator: Receive relevant information • CRO: Oversees the caption, processing and interpretation of information
	Information monitor	Board, ERM committee, risk function, internal audit	External audit	• CRO: Ongoing monitoring on adequacy, completeness and accuracy of information; semi-annual assessment of performance (MEA01) and controls (MEA02) to maintain the information • Internal audit: Annual validation of format and level of contents
	Information dispose	Risk function		• CRO: According to data retention policy, to ensure confidentiality of information and to reduce the amount of information

Figure 35—Information Item Risk Profile *(cont.)*

	Quality Subdimension and Goals		Description—The extent to which information is…	Relevance *	Goal
Goals	Intrinsic	**Accuracy**	correct and reliable	High	Source information needs to be accurate (confirm through audit) and needs to be aggregated in the risk management application according to fixed rules.
		Objectivity	unbiased, unprejudiced and impartial	High	Information is based on verifiable facts and substantiations, using the common risk view established throughout the enterprise.
		Believability	regarded as true and credible	Medium	Reporting is fully trusted.
		Reputation	regarded as coming from a true and credible source	Medium	Source information is collected from competent and recognised sources.
	Contextual and Representational	**Relevancy**	applicable and helpful for the task at hand	High	The risk profile is structured as defined and the recipient confirms the relevancy of information provided.
		Completeness	not missing and is of sufficient depth and breadth for the task at hand	High	The risk profile covers the full enterprise scope and the full risk register. However, not all information might be available and assumptions need to be made and substantiated.
		Currency	sufficiently up to date for the task at hand	Low	The need for currency of the risk profile is driven by the frequency and impact of alterations and depending on the component.
		Amount of information	is appropriate in volume for the task at hand	High	The volume of information is appropriate to the recipient's needs and shall be defined during the design.
		Concise representation	compactly represented	Medium	The risk profile is concisely represented; this is obtained by aggregating data for the entire enterprise and by retaining only individual cases from a predefined threshold onwards.
		Consistent representation	presented in the same format	Low	The risk profile is always presented according to an agreed-on template. However, single scenarios might be analysed differently when agreed on.
		Interpretability	in appropriate languages, symbols and units, and the definitions are clear	High	To ease decision making, the information 'sweet spot' can be identified and focused on.
		Understandability	easily comprehended	High	In order to make informed decisions, the risk profile should be understood by many stakeholders.
		Manipulation	easy to manipulate and apply to different tasks	Low	Scenarios can be modified and simulated.
	Security	**Availability**	available when required, or easily and quickly retrievable	Medium	The risk profile is at all times available to its stakeholders; a temporary unavailability is acceptable in case of an incident.
		Restricted access	restricted appropriately to authorised parties	High	Access to the risk profile is determined by the risk function, and is restricted as follows: • Write access: Risk function (based on input from contributors) • Read access: All other stakeholders

* The relevance column entries are enterprise contextual. This is an illustration, but the actual importance depends on each enterprise's specific context.

Figure 35—Information Item Risk Profile *(cont.)*

	Attribute	Description	Value
Good Practice	**Physical**	Information carrier/media	The information carrier for the risk profile can be an electronic or printed document or an information system (e.g., dashboard).
	Empiric	Information access channel	The risk profile is accessible through the ERM portal or printed at specific locations.
	Syntactic	Code/language	The risk profile contains the following subparts: • Risk register (results of risk analysis), which consists of a list of risk scenarios and their associated estimates for impact and frequency (risk map); both current and the previous risk map will be included. • Risk action plan, including action item, status, responsible, deadline, etc. • Loss data related to events occurring over the last reporting period(s) • Risk factors, including both contextual risk factors and capability-related risk factors (vulnerabilities) Result of independent assessments (e.g., audit findings, self-assessments)
	Semantic	Information type	Structured document based on a template and/or an online dashboard with drill-down functionality.
		Information currency	The risk profile contains historical, current and forward looking data.
		Information level	The risk profile aggregates data over the entire enterprise, representing only major risk over a defined threshold and with significant changes to previous periods.
	Pragmatic	Retention period	The risk profile is to be retained for as long as the data/information over which it reports risk needs to be retained. Updates to the risk register should be logged and retained as defined in legal requirements, use the information as evidence or the need to obtain independent assurance.
		Information status	The current instance is operational, older ones are historical data.
		Novelty	The risk profile combines several other sources of data that make up a new instance, hence it is novel data. It is updated regularly (e.g., on a monthly basis).
		Contingency	The risk profile relies on the following information being available and understood by the user: • Risk appetite of the enterprise • Risk factors that apply to the enterprise • Risk taxonomy in use in the enterprise
	Social	Context	The risk profile is primarily meaningful and to be used in a context of ERM, but could also be used in other circumstances (e.g., during a merger).

Figure 35—Information Item Risk Profile *(cont.)*

Link to Other Enablers	
Processes	The risk profile is an output from the management practices: • APO12.03 Maintain a risk profile. • APO12.04 Articulate risk. The risk register is an input for the governance and management practices: • EDM03.02 Direct risk management. • EDM05.02 Direct stakeholder communication and reporting. • APO02.02 Assess the current environment, capabilities and performance. • MEA02.08 Execute assurance initiatives. It is used in the following governance and management practices: • EDM03.03 Monitor risk management. • APO12.06 Respond to risk. It is mentioned in the goal of the process APO12 *Manage Risk*: • A current and complete risk profile exists. And measured by the following metrics: • Percent of key business processes included in the risk profile • Completeness of attributes and values in the risk profile
Organisational Structures	Under the accountability of the CRO, the following roles are responsible for providing/producing the information: • Business process owners • CIO (and IT staff members) • CISO
Infrastructure, Applications and Services	The risk profile is produced by a risk management application or manually maintained by the CRO.
People, Skills and Competencies	The generation of the risk profile requires an understanding of risk management principles and skills. The provision of information requires subject-related expertise and the presentation of information should not require risk management skills but enable governance bodies to steer risk management and to take decisions.
Culture, Ethics and Behaviour	The availability of the risk profile supports the transparency of risk as well as trends and a risk-aware culture.
Principles, Policies and Frameworks	Related principles: • Connect to enterprise objectives • Align with ERM • Balance cost/benefit of IT risk • Consistent approach

Chapter 4
Addressing Information Governance and Management Issues Using COBIT 5

The purpose of this chapter is to demonstrate how the COBIT 5 framework can assist in addressing a number of common information governance and management issues.

4.1 Information Governance and Management Issues Reviewed in This Chapter

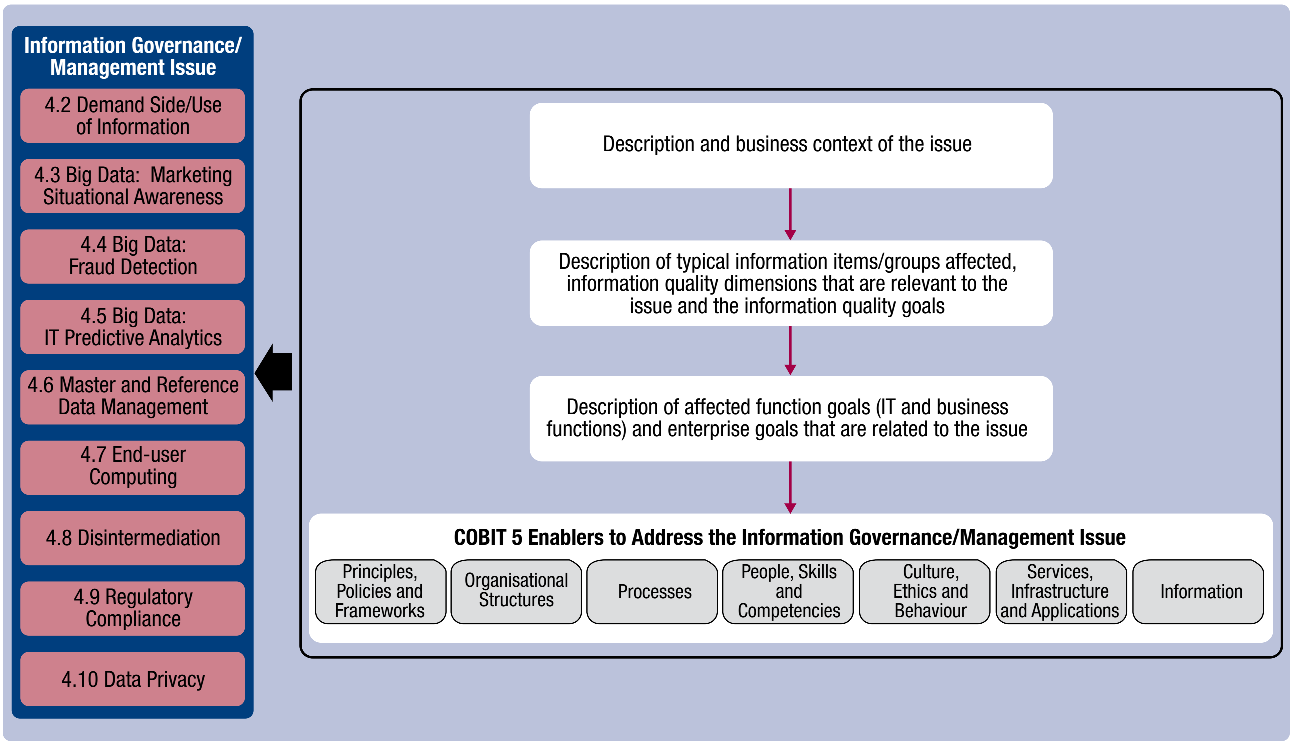
This chapter discusses the following current data and information management issues, as illustrated in **figure 36**:

- Demand side/use of information
- Big data, covering three areas:
  - Marketing situational awareness (variety of information)
  - Fraud detection (volume of information)
  - IT Predictive analytics (velocity of information)
- Master and reference data management
- End-user computing
- Disintermediation
- Regulatory compliance
- Data privacy

For each issue, the following topics are included (see **figure 36.**):

- Description and business context of the issue
- Typical information items/groups affected, information quality dimensions that are relevant to the issue and the information goals
- Affected goals further up the goals cascade, i.e., function goals (IT and business functions) and enterprise goals related to the issue. The related enterprise goals are expressed as a subset of the COBIT 5 enterprise goals, and the IT-related goals are expressed as a subset of the COBIT 5 IT-related goals.
- Enablers to address the issue. COBIT 5 is based on the enabler principle, i.e., any business issue can be resolved by a combination of interdependent enablers. The seven COBIT 5 enabler categories are used to provide high-level guidance on addressing the information governance/management issue.

Figure 36—Discussion Format for Information Governance and Management Issues


Information Governance/ Management Issue
4.2 Demand Side/Use of Information
4.3 Big Data: Marketing Situational Awareness
4.4 Big Data: Fraud Detection
4.5 Big Data: IT Predictive Analytics
4.6 Master and Reference Data Management
4.7 End-user Computing
4.8 Disintermediation
4.9 Regulatory Compliance
4.10 Data Privacy
Description and business context of the issue
Description of typical information items/groups affected, information quality dimensions that are relevant to the issue and the information quality goals
Description of affected function goals (IT and business functions) and enterprise goals that are related to the issue
COBIT 5 Enablers to Address the Information Governance/Management Issue
Principles, Policies and Frameworks
Organisational Structures
Processes
People, Skills and Competencies
Culture, Ethics and Behaviour
Services, Infrastructure and Applications
Information

4.1.1 Big Data

According to the March 2013 ISACA white paper on the impacts and benefits of big data[9], 'big data' is a common term for a set of problems and techniques concerning the management and exploitation of very large sets of data. The notion of a 'very large' set of data can be different for all enterprises. In essence, enterprises face the issue of big data whenever traditional techniques or tools are no longer sufficient to capture, manage and process the data at a reasonable elapsed time.

Enterprises must find a way to govern big data in alignment with business requirements, without obstructing the free flow of information and innovation. The data ranges from structured to unstructured and includes customer and employee data, metadata, trade secrets, email, video and audio. Information can be:

- Spread across multiple, complex silos that are isolated from each other
- Repeated, with redundant copies of data (and the business processes using them) located throughout the enterprise
- Uncoordinated and lacking standardisation of terms

The benefits of big data are plentiful. When correctly managed, big data can provide a more accurate view on product development, the behaviours of consumers in the marketplace, operational efficiency, etc. Consequently, predictions will be more accurate or improvement projects can target exact pain points.

Practically, issues regarding big data can be categorised according to three dimensions:

- Variety of information
- Velocity of information creation
- Volume of information, which is the result of increasing variety and velocity

Furthermore, all of these dimensions are growing and becoming even more complex. Information is coming from an ever wider array of channels, sensors and formats. Enterprises ask to process data more quickly, so they can respond to it as events happen. Information can be altered at a fast pace, which adds to the complexity of the issue.

Consequently, big data presents a number of challenges relating to its complexity including how the enterprise can:

- **Understand** and use big data when it is in an unstructured format, such as text or video
- **Capture** the most important data as it is created or acquired and deliver it to the right people in real time
- **Store, protect and utilise** the data, and how the enterprise can analyse and understand the data, given its size and the enterprise's computational capacity

Related to these basic issues, there are numerous other challenges, from privacy and security to access and deployment. Building the business case to implement the proper practices to handle big data is challenging. The clear value needs to be demonstrated to the outcomes of big data projects.

One issue for each of the dimensions of big data is discussed in sections 4.3 through 4.5 in this chapter.

4.2 Information Governance/Management Issue: Demand Side/Use of Information

4.2.1 Issue Description and Business Context

Often, information users in business functions throughout the enterprise struggle to get their information needs understood (and fulfilled) by the IT organisation. This issue is caused by a gap between business and technical knowledge, and it can be analysed from the following two perspectives:

- Assuming sufficient technical knowledge to configure information systems is in place within the IT organisation, a lack of understanding of the business process by IT can lead to a suboptimal configuration of these systems, because expert knowledge on the data and how the data can be structured or combined is required.
- A lack of insight by the business users about information systems or the information models used, their functionalities and their limitations can lead to expectations that cannot be met.

The demand side/use of information issue applies to many systems in an enterprise. Common examples are data warehouses and their BI solutions and enterprise information management systems/portals. Input on details and nuances regarding data are crucial to set up these solutions in an optimal way. Additionally, this issue is not restricted to occur during a solution under development, which is usually managed through a proper project management framework. New reports for data warehouses, for example, typically originate from change requests, which are generated continuously, independent of whether the system is still under development.

[9] ISACA, *Big Data: Impact and Benefits*, USA, 2013, *www.isaca.org/Knowledge-Center/Research/Pages/White-Papers.aspx*

Example request: How can the marketing officer turn raw customer data into monthly reports that allow him/her to obtain better insights into the potential client segments and needs? The solution requires a thorough knowledge of the marketing process and expertise regarding the customer relationship management (CRM) solution and related data warehouse that are used to extract the relevant information. Both marketing and IT need to combine their expertise to configure the reports that will allow this type of client insight.

From an enterprise point of view, a number of potential risk scenarios can be identified, such as:

- When business decisions are based on information included in incorrectly configured reports, these decisions can affect the competitive advantage and be hazardous for the enterprise.
- Even though business cases are made to evaluate the benefits of information systems and these systems are implemented properly, the misuse of these systems or the information produced by these systems after they are in production results in the information systems not meeting the required value because users' needs are not addressed or accommodated correctly. The analysis of the benefits and cost of these information systems will become incorrect if this risk is not managed properly.
- When information is handled and configured without adequate knowledge or with imprudent use of technology, disclosure of sensitive information may accidentally occur.
- Poor training leads to documented and substantial productivity loss.
- Business users may have a tendency to abandon solutions that make them feel uncomfortable, which may lead to several other potential issues, such as:
  - General feeling of frustration from the business towards IT, or vice versa
  - Development efforts (costs) do not deliver any added value for the enterprise.
  - Issues regarding the optimal use of licences and the associated cost
  - Users turn to end-user computing or disintermediation with the related risk as described in the following sections.

4.2.2 Affected Information

Figure 37 lists typical information items or types that are affected by a lack of capacity to grasp user needs. Information quality goals of the information that is processed to support business users might not be achieved, depending on the scale of mismatch.

Figure 37—Illustrative Information Quality Goals for Information Demand Side

Information Item	Most Relevant Quality Dimension	Information Quality Goal
Typically, this mismatch occurs for management information that is used for decision making and is based on feeds of operational information.	The management information is combined data. The following quality goals should be applied to the final combined information. • Accuracy • Believability • Relevancy • Completeness • Interpretability	• Output of information systems is accurately configured, believable and relevant. • Users can use complete and correct interpretable information to manage business functions.

4.2.3 Affected Enterprise Goals and IT Goals

Failing to understand and deliver user needs can affect the following goals throughout the goals cascade:

- The information quality goals listed in **figure 37** support the achievement of the goals that are associated with an IT function, i.e., IT-related goals, which are listed in **figure 38**.
- The IT-related goals support the enterprise goals, which are also listed in **figure 38**. The ultimate purpose of the business user is to better achieve overall enterprise goals.

Figure 38—Illustrative Goals Cascade for Information Demand Side

IT-related Goals and Business Function Goals	Many IT-related goals can be derived. Following are several of the most important goals: • ITG03 Commitment of executive management to making IT-related decisions • ITG05 Realised benefits from IT-enabled investments and services portfolio • ITG06 Transparency of IT costs, benefits and risk • ITG07 Delivery of IT services in line with business requirements • ITG08 Adequate use of applications, information and technology solutions • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG14 Availability of reliable and useful information for decision making • ITG16 Competent and motivated IT personnel
Enterprise Goals	• EG01 Stakeholder value of business investments • EG02 Portfolio of competitive products and services • EG05 Financial transparency • EG06 Customer-oriented service culture • EG09 Information-based strategic decision making • EG17 Product and business innovation culture

4.2.4 Enablers to Address the Issue

COBIT 5 is a comprehensive framework for governance and management of enterprise IT; hence, it is possible to address the demand side/use of information issue using COBIT 5. **Figure 39** gives a set of enablers that can assist in achieving the desired benefits while optimising risk and resource use.

Figure 39—Illustrative Set of Enablers for Information Demand Side

Enabler	How Can This Enabler Help to Address the Issue?
Principles, Policies and Frameworks	Providing rules/guidance in capturing, implementing and reviewing business user needs, and ensuring effective and efficient use of information and related technology, including: • The use of a well-defined and managed software development life cycle • Proper guidance regarding demand management, change and requirements management, use management, user support and relationship management • The defined implementation of a business governance and management framework that includes responsibilities for IT, relationship management, requirements management, etc. • A useful reference framework to consult for more detailed management of demand and use of information is Business Information Services Library (BiSL®) (*www.aslbislfoundation.org*)
Processes	A number of governance and management processes (from *COBIT 5: Enabling Processes*) are relevant in the context of lacking capacity to grasp user needs, and can be used to define a set of management practices capable of dealing with this issue: • EDM02 Ensure benefits delivery. • APO01 Manage the IT management framework. • APO07 Manage human resources. • APO08 Manage relationships. • APO09 Manage service agreements. • APO11 Manage quality. • BAI02 Manage requirements definition. • BAI06 Manage changes. These processes allow an organisation to diminish the mismatch between the user and IT by clarifying each party's responsibility in the relationship.
Organisational Structures	Key responsibility to overcome this issue lies with: • CIO: Accountable to manage the relationship between IT and the business • Business executives • Business process owners Other related functions can include: • Head development • Head IT operations • Service manager • Business relationship manager • Information manager • Key user
Culture, Ethics and Behaviour	The following behaviours are important for improving the relationship between IT and the business: • Openness and interest in both business and IT activities • 'Continuous improvement' is promoted and executed. • Transparent and participative culture is an important focus point.
Information	A number of information items are essential for improving the relation between IT and the business: • Documented requirements • Documented change requests • Business expectations • Satisfaction analysis • Requirements development template • Business process architecture documentation • Information strategy (related to business strategy) • Impact of business needs in terms of understandable benefits, costs and risk • Business expectations and agreements (e.g., service level agreement [SLA])
Services, Infrastructure and Applications	A number of services and tools (usually to be provided by the IT function) are relevant to overcome the mismatch between IT and the business: • Business process modelling and simulation tools • Systems dynamics modelling tools • Repository-based structured enterprise architecture tools • Free form and templated diagramming tools (e.g., Microsoft® Visio®) • Computer assisted software engineering (CASE) tools, including Unified Modeling Language (UML™) and older approaches • Requirements management tools • System mockup tools • Enterprise architecture (modelling tools)
People, Skills and Competencies	Skills and competencies requirements for improving the relationship between IT and the business include some affinity of IT staff with the business. In addition, training must be foreseen for both IT and the business: • IT: to improve their knowledge of business processes • Business process owners and related staff members: several user-friendly solutions exist that empower the business user to structure the information required. • Training for end users

4.3 Information Governance/Management Issue: Marketing Situational Awareness (Big Data Dimension 1: Variety of Information)

4.3.1 Issue Description and Business Context

An enterprise marketing team wishes to increase its awareness of and capacity to respond to public perceptions of its company's offerings. Data sources include social media postings, such as micro and traditional blogs, social sites, and audio conversations between customers and service representatives. The enterprise wishes to correlate the sentiment detected in both online and call centre channels with sales trends in various segments and regions around the world. Speech-to-text conversion, web indexing and natural language text processing are required. In big data terms, this is a **variety** issue.

4.3.2 Affected Information

Figure 40 lists typical information items or types affected by the suboptimal use of a large variety of information sources. It also contains the most relevant quality criteria and goals for these information items in the given context of big data.

Figure 40—Illustrative Information Quality Goals for Marketing Situational Awareness

Information Item	Most Relevant Quality Dimension	Information Quality Goal
Marketing reports	• Relevancy • Accuracy • Availability • Currency • Completeness • Believability	• The enterprise bases important decisions on correct market analysis. • Client insight is analysed and used in the most optimal way possible.
Product strategies	• Relevancy • Accuracy • Availability • Currency • Completeness	The go-to-market of future products is carefully planned to obtain the maximal exposure and return.

4.3.3 Affected Goals

Suboptimal use of a large variety of information sources can affect the following goals throughout the goals cascade:

- The information quality goals listed in **figure 40** support the achievement of the goals that are associated with an IT function, i.e., IT-related goals, which are listed in **figure 41**.
- The IT-related goals support the enterprise goals, which are also listed in **figure 41**. The ultimate purpose of the business user is to better achieve overall enterprise goals.

Figure 41—Illustrative Goals Cascade for Marketing Situational Awareness

IT-related Goals and Business Function Goals	Many IT-related goals can be derived. Following are several of the most important goals: • ITG09 IT agility • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG14 Availability of reliable and useful information for decision making • ITG17 Knowledge, expertise and initiatives for business innovation
Enterprise Goals	• EG08 Agile responses to a changing business environment • EG09 Information-based strategic decision making • EG17 Product and business innovation culture

4.3.4 Enablers to Address the Issue

COBIT 5 is a comprehensive framework for governance and management of enterprise IT; hence, it is possible to address the issue using COBIT 5. **Figure 42** gives a set of enablers that can assist in achieving the desired benefits while optimising risk and resource use.

Figure 42—Illustrative Set of Enablers for Marketing Situational Awareness

Enabler	How Can This Enabler Help to Address the Issue?
Principles, Policies and Frameworks	Providing rules/guidance in capturing, implementing and reviewing business user needs, including: • Policies specifying the use of social media by staff and by the enterprise, both as input and output of information • Privacy policy • Data protection policy • Managing knowledge throughout the enterprise • Policies for big data governance
Processes	A number of governance and management processes (from *COBIT 5: Enabling Processes*) are relevant in the context of the suboptimal use of a large variety of information sources, and can be used to define a set of management practices capable of dealing with this issue: • EDM04 Ensure resource optimisation. • APO04 Manage innovation. • APO13 Manage security. • BAI08 Manage knowledge. • MEA01 Monitor, evaluate and assess performance and conformance.
Organisational Structures	Key responsibility to overcome this issue lies with: • Marketing department, which should identify the many sources of information • Group responsible for managing the BI systems to assist in understanding, capturing and storing the information • CIO Other related functions can include: • Head development • Head IT operations
Culture, Ethics and Behaviour	The following behaviours are important for optimally using a large variety of information: • A critical mindset towards the: – Current way of working – Investment required to analyse information compared to the added value of this effort • A no-blame culture is required when mistakes are made regarding tendencies and evolutions • A strong lessons learned culture
Information	A number of information items are essential for optimally using a large variety of information to obtain customer insight: • Customer communication: – Enterprise has a complete stream of customer and market reactions/interactions, including old and new media and customer service communications. For example, audio is converted to text; unstructured text is analysed with natural language processing; semantic and sentiment models are developed. • Customer sentiment (satisfaction/dissatisfaction): – Customer sentiment is structured and quantified along appropriate dimensions. – Trends are tracked and reported. • Sentiment/sales correlation: – Correlation between sentiment and sales is understood. – Marketing can usefully leverage sentiment/sales analytics to generate new, testable strategies. • Identified public relations issues and adequate advice to react: – Important negative trends are identified and escalated on an urgent basis to corporate communications and executive leadership. – False negatives and positives are avoided.
Services, Infrastructure and Applications	A number of services and tools (usually to be provided by the IT function) are relevant to effectively understand, capture and store information: • BI solutions • Automated data analysis tools • Forensic research tools • The proper infrastructure to support the storing of large amounts of raw and analysed information • Automated speech-to-text transcription • Semantic analysis tools (e.g., IBM Watson) • Workstation-based statistical tools (IBM SPSS, SAS)
People, Skills and Competencies	In addition to marketing skills that are required to identify and understand the sources of information, a strong analytic IT capability is needed as well. A strong product knowledge of the IT analytical systems (BI, forensic research, etc.) are completed with a business mindset and an openness to change.

4.4 Information Governance/Management Issue: Fraud Detection (Big Data Dimension 2: Velocity of Information)

4.4.1 Issue Description and Business Context

The value of this case can be demonstrated in the prevention of fraud based on the impact of such an event. A merchant is concerned about detecting fraudulent online transactions. Fraudulent activity can be very sophisticated, involving multiple transactions over a period of time. This activity can involve payment mechanisms (e.g., fraudulent credit cards) or manipulation of company policies regarding deliveries and returns. Understanding current fraud trends in a given region or market sector is important.

The challenge in obtaining the needed information is the massive, high-speed flow of the transactions; patterns must be detected in near real time across hundreds of transactions per minute. In big data terms, this is a velocity issue.

4.4.2 Affected Information

Figure 43 lists typical information items or types affected by frauds. It also contains the most relevant quality criteria and quality goals for these information items.

Figure 43—Illustrative Quality Goals Cascade for Fraud Detection

Information Item	Most Relevant Quality Dimension	Information Quality Goal
Fraud signature	• Relevancy • Accuracy • Availability/currency • Completeness	• Relevant fraud patterns are distilled from e-commerce transactions. • Fraud patterns are accurately recognised from the transactions data set. • New fraud patterns are validated and moved to operational status.
Suspected fraud reports	• Availability • Currency • Concise representation/understandable	• Fraudulent transactions are recognised in a timely manner and reported to the security operations centre. • Existing and known fraud patterns are part of the signatures being matched.
Fraud trends reports	• Availability • Currency • Concise representation/understandable	• Fraud trend reports from internal and market sources are made available in a timely fashion. • Fraud trend reports are current. • Fraud trend reports are understandable.

4.4.3 Affected Goals

Inadequate use of rapidly changing information can affect the following goals throughout the goals cascade:

- The information quality goals listed in **figure 43** support the achievement of the goals that are associated with an IT function, i.e., IT-related goals, which are listed in **figure 44**.
- The IT-related goals support the enterprise goals, which are also listed in **figure 44**. The ultimate purpose of the business user is to better achieve overall enterprise goals.

Figure 44—Illustrative Goals Cascade for Fraud Detection

IT-related Goals and Business Function Goals	Many IT-related goals can be derived. Following are several of the most important goals: • ITG04 Managed IT-related business risk • ITG10 Security of information, processing infrastructure and applications • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG14 Availability of reliable and useful information for decision making • ITG16 Competent and motivated business and IT personnel
Enterprise Goals	• EG03 Managed business risk (safeguarding of assets)

4.4.4 Enablers to Address the Issue

COBIT 5 is a comprehensive framework for governance and management of enterprise IT; hence, it is possible to address the issue using COBIT 5. **Figure 45** gives a set of enablers that can assist in achieving the desired benefits while optimising risk and resource use.

Figure 45—Illustrative Set of Enablers for Fraud Detection

Enabler	How Can This Enabler Help to Address the Issue?
Principles, Policies and Frameworks	Providing rules/guidance in fraud prevention and detection includes: • Regulatory compliance policy • Data protection policy • Internal control framework • Information security principles and policy • Business continuity and disaster recovery policy • Fraud risk policy
Processes	A number of governance and management processes (from *COBIT 5: Enabling Processes*) are relevant in the context of fraud prevention and detection and can be used to define a set of management practices capable of dealing with this issue: • EDM03 Ensure risk optimisation. • APO12 Manage risk. • APO13 Manage security. • BAI03 Manage solutions identification and build. • BAI08 Manage knowledge. • BAI09 Manage assets. • DSS05 Manage security services. • MEA01 Monitor, evaluate and assess performance and conformance.
Organisational Structures	Key responsibility to overcome this issue lies with: • CFO • Legal representation • Chief information security officer (CISO) • Information security steering committee • Information security manager • Risk function • CIO • Business process owner Other related functions can include: • Head development • Head IT operations
Culture, Ethics and Behaviour	The following behaviours are important for detecting fraud efficiently: • People respect the importance of information security policies and principles. • 'Continuous Improvement' is promoted and executed. • Positive behaviour towards raising issues or negative outcomes
Information	A number of information items are essential for detecting fraud given the velocity of modifying information: • Transaction data • Client information • Insights in fraud patterns using camera images • Information released by regulators and local authorities • Insights in trends from specialist interest groups or analysts • Information security and system configuration documentation
Services, Infrastructure and Applications	A number of services and tools (usually to be provided by the IT function) are relevant to efficiently prevent and detect fraud: • Fraud detection systems • Other security measures • Continuous stream query processing
People, Skills and Competencies	Technical skills are required to set up the required security and perform the required fraud detection. Analytical skills are required to perceive fraud trends.

4.5 Information Governance/Management Issue: IT Predictive Analytics (Big Data Dimension 3: Volume of Information)

4.5.1 Issue Description and Business Context

Modern IT infrastructures generate great volumes of information (e.g., logs). Data mining and predictive analytics can provide insights into system failures by analysing these logs. Root cause analysis is facilitated, and emerging incidents and problems can even be predicted from this data at times. Ideally, the logs are analysed and combined with systems management data (incidents, changes, configuration items and dependencies) to provide a full picture of what happened, why and whether any emerging risk is present. In big data terms, this is a volume issue.

4.5.2 Affected Information

Figure 46 lists the information items, quality dimensions, and quality goals.

Figure 46—Illustrative Quality Goals Cascade for IT Predictive Analytics

Information Item	Most Relevant Quality Dimension	Information Quality Goal
Systems management telemetry	• Completeness • Currency	Complete access to stream/archive of system management logs and related information
Service management data (incidents, changes, releases, configuration items, dependencies, SLAs)	• Relevancy • Accuracy • Availability/currency • Completeness	Complete representation of service support and delivery processes, especially operational
Root cause analyses (analysis logic/methods)	• Currency • Relevancy • Completeness	Derived analyses of combined data showing the likely root causes of incidents and recurring problems, suitable for input into problem management for mitigation
Proactively identified problems	• Currency • Concise representation/understandable	Derived analyses of combined data using machine learning or other appropriate techniques to identify signatures of past failures and potential indications of their recurrence, for input into incident, problem or continual service improvement processes. Also, data can be used for continuous diagnostics and monitoring so that patterns and anomalies can be detected before something bad happens to the system.

4.5.3 Affected Goals

The lack of efficiently processed large volumes of system information can affect the following goals throughout the goals cascade:

- The information quality goals listed in **figure 46** support the achievement of the goals that are associated with an IT function, i.e., IT-related goals, which are listed in **figure 47**. In particular, historical data can be used for continuous diagnostics and monitoring so that patterns and anomalies can be detected before something bad happens to the system—optimising enterprise IT asset value.
- The IT-related goals support the enterprise goals, which are also listed in **figure 47**. The ultimate purpose of the business user is to better achieve overall enterprise goals.

Figure 47—Illustrative Goals Cascade for IT Predictive Analytics

IT-related Goals and Business Function Goals	Note that these goals reflect the circular nature of 'IT for IT', which is still valuable from a business perspective due to the fact that IT investments are highly leveraged. Following are several of the most important goals: • ITG11 Optimisation of IT assets, resources and capabilities • ITG14 Availability of reliable and useful information for decision making
Enterprise Goals	• EG07 Business service continuity and availability

4.5.4 Enablers to Address the Issue

COBIT 5 is a comprehensive framework for governance and management of enterprise IT; hence, it is possible to address the issue using COBIT 5. **Figure 48** gives a set of enablers that can assist in achieving the desired benefits while optimising risk and resource use.

Figure 48—Illustrative Set of Enablers for IT Predictive Analytics

Enabler	How Can This Enabler Help to Address the Issue?
Principles, Policies and Frameworks	Providing rules/guidance for efficiently processing large volumes of system information includes: • Policies for big data governance, including privacy policy if appropriate • Internal control framework, operational control practices • Governance, risk, and compliance (GRC) framework for monitoring adherence to these operational control practices • CRM policy that requires the deletion of this data on a periodic basis to maintain customer privacy policy requirements Useful reference frameworks to consult are: • DMBOK • ISO/IEC 11179 Metadata Registry
Processes	A number of governance and management processes (taken from *COBIT 5: Enabling Processes*) are relevant in the context of efficiently processing large volumes of system information and can be used to define a set of governance and management practices capable of dealing with this issue: • EDM04 Ensure resource optimisation. • APO02 Manage strategy. • APO03 Manage enterprise architecture. • APO11 Manage quality. • APO13 Manage security. • BAI03 Manage solutions identification and build. • BAI04 Manage availability and capacity. • BAI08 Manage knowledge. • BAI09 Manage assets. • BAI10 Manage configuration. • DSS04 Manage continuity. • DSS05 Manage security services. • MEA01 Monitor, evaluate and assess performance and conformance.
Organisational Structures	Key responsibility to overcome this issue lies with: • Head IT operations • Information security manager • CIO Other related functions can include: • Head architect • Head development • Head IT operations
Culture, Ethics and Behaviour	The following behaviours are important for efficiently processing large volumes of system information: • Learning culture • Sense of ownership
Information	A number of information items are essential for efficiently processing large volumes of system information: • Architecture principles • Data classification guidelines • Defined scope of architecture • Guiding principles for enterprise architecture • Information architecture model • Process architecture model • Transition architectures
Services, Infrastructure and Applications	A number of services and tools (usually to be provided by the IT function) are relevant to efficiently process large volumes of system information: • Analytical tools • Mechanism for storage and retrieval of data, e.g., NoSQL repositories • Enterprise architecture may be a key means to reduce the creation of data silos.
People, Skills and Competencies	Skills required to efficiently process large volumes of system information: • Technical expertise • Curiosity: a desire to go beneath the surface and discover and distill a problem down into a very clear set of hypotheses that can be tested • Storytelling: the ability to use data to tell a story and to be able to communicate it effectively • Cleverness: the ability to look at a problem in different, creative ways • The far-reaching nature of big data analytics projects can have uncomfortable aspects: data must be broken out of silos to be mined, and the organisation must learn how to communicate and interpret the results of analysis. The skills of storytelling and cleverness are the gateway factors that ultimately dictate whether the benefits of analytical labours are absorbed by an organisation.

4.6 Information Governance/Management Issue: Master and Reference Data Management

4.6.1 Issue Description and Business Context

Master data management comprises a set of processes, policies, standards and tools that consistently defines and manages the reference and master data of an organisation.

Some organisations distinguish between reference and master data, others often only use the term master data to cover both:

- Reference data is data used to classify or categorise other data[10]. Reference data usually is restrained to certain allowed values also called the value domain. Reference data value domains can be defined internally (e.g., request status, sales order status) or externally (e.g., official country codes, currency codes, medical procedure codes for insurance billing). Typically, reference data changes slowly. Metadata about reference data may include:
  - Meaning and purpose of reference value domains
  - Reference tables and databases where reference data is used
  - Source of the data
  - Version and last update date
  - Roles (RACI) with regard to the data
- Master data is data that provides context for business transactions. Common types of master data include data about:
  - Parties—individuals or organisations—and their roles (customer, vendor, supplier, employee, regulator, citizen, etc.)
  - Products
  - Financial structures (general ledger, cost centres, etc.)
  - Locations

  Master data is about identifying, or developing, and maintaining a single source of truth (sometimes called a 'golden record') for each relevant information item, e.g., product, place, party. Challenges for master data management include finding answers to the following questions:
  - What is the shared data—which parties, products, places are used across business process silos?
  - Which data is describing the same things?
  - What is the source of this data and where is it stored?
  - Which version is more accurate, more reliable, current?
  - Which data from different sources can be integrated to the benefit of the enterprise?
  - How do 'golden records' find their way into other systems across the enterprise?

Reference and master data provide the context for transaction data. Current issues around master data management, i.e., consequences of inadequate master data management, include:

- Low(er) data and information quality
- Business process integrity issues
- Business process outcomes not as per expectation
- Customer service problems due to inconsistent definitions (attributes, etc.) across customer interaction channels

As a consequence, the business drivers that are related to the covered enterprise goals for master data management initiatives include:

- Improving data quality and integration across data sources
- Providing consolidated 360-degree view of information about important business partners, products and roles, especially for reporting, analytics and subsequent decision making

These master data management initiatives are very often triggered by a new vision (related to personnel change), some disruptive events with root cause in data quality problems or a major project where master data management can be integrated.

[10] Source: Data Management Association International (DAMA), *The DAMA Guide to the Data Management Body of Knowledge* (DMBOK), USA, 2009

4.6.2 Affected Information

Figure 49 lists the information items, quality dimensions, and goals.

Figure 49—Illustrative Quality Goals Cascade for Master and Reference Data Management

Information Item	Most Relevant Quality Dimension	Information Quality Goal
• Operational data—party data (clients, customers, etc.) • Product data • Financial master data location data	• Accuracy • Objectivity • Completeness • Consistent representation • Reputation	Clear, complete enterprise data items that support achievement of business goals
Reference data	• Availability • Currency • Completeness • Accuracy • Relevancy	Availability of complete, up-to-date reference data items
Metadata on reference data and master data	• Availability • Currency • Accuracy	Availability of complete, up-to-date metadata items

4.6.3 Affected Goals

Master and reference data management can affect the following goals throughout the goals cascade, in either direction:

- The information quality goals listed in **figure 49** support the achievement of the goals that are associated with an IT function, i.e., IT-related goals, which are listed in **figure 50**.
- The IT-related goals support the enterprise goals, which are also listed in **figure 50**. Frequently mentioned business benefits of master and reference data management include operational effectiveness, customer intimacy and product and service leadership. In COBIT 5 terms, these business benefits are transformed into the goals cascade enterprise goals in **figure 50**.

Figure 50—Illustrative Goals Cascade for Master and Reference Data Management

IT-related Goals and Business Function Goals	Many IT-related goals can be derived. Following are several of the most important goals: • ITG04 Managed IT-related business risk • ITG08 Adequate use of applications, information and technology solutions • ITG11 Optimisation of IT assets, resources and capabilities • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG14 Availability of reliable and useful information for decision making
Enterprise Goals	• EC01 Stakeholder value of business investments • EG02 Portfolio of competitive products and services • EG03 Managed business risk (safeguarding of assets) • EG07 Business service continuity and availability • EG09 Information-based strategic decision making • EG10 Optimisation of service delivery costs • EG11 Optimisation of business process functionality • EG12 Optimisation of business process costs • EG14 Operational and staff productivity

4.6.4 Enablers to Address the Issue

COBIT 5 is a comprehensive framework for governance and management of enterprise IT; hence, it is possible to address the issue of master data management using COBIT 5. **Figure 51** gives a set of enablers that can assist in achieving the desired benefits while optimising risk and resource use of master data management.

Figure 51—Illustrative Set of Enablers for Master and Reference Data Management

Enabler	How Can This Enabler Help to Address the Issue?
Principles, Policies and Frameworks	Providing rules/guidance for reference and master data management includes: • Establishing principles for reference and master data management, such as:[11] – Shared reference and master data belongs to the enterprise, not to a particular application or department – Reference and master data management is an ongoing data quality improvement programme; its goals cannot be achieved by one project alone. – Accountability for managing reference data values lies with 'data stewards' who, in larger enterprises, are information architects or other similar information-centric roles and, in smaller enterprises, generally belong to an IT-function data management role. – Golden data records represent the enterprise's best efforts at determining the most accurate, current and relevant data. – Replicate master data values only from the database of record. • There must be a set of data classification guidelines, information model guidelines, data integrity policies, data security, and governance and management practice guidelines. • Establishing accountability for data-related decisions, across the enterprise and not only within IT
Processes	A number of governance and management processes (from *COBIT 5: Enabling Processes*) are relevant in the context of master and reference data management and can be used to define a set of governance and management practices that are capable of dealing with this issue: • EDM02 Ensure benefits delivery. • EDM03 Ensure risk optimisation. • EDM04 Ensure resource optimisation. • APO01 Manage the IT management framework. • APO03 Manage enterprise architecture. (e.g., manage the data integration architecture) • APO05 Manage portfolio. • APO11 Manage quality. • APO12 Manage risk. • BAI02 Manage requirements definition. (e.g., understand integration needs for reference data[12]) • BAI03 Manage solutions identification and build. For example: – Identify reference data sources and contributors. – Implement reference and master data management solutions. – Maintain match rules. – Establish golden records. • BAI05 Manage organisational change enablement. • BAI06 Manage changes. • BAI08 Manage knowledge. • DSS06 Manage business process controls. • MEA01 Monitor, evaluate and assess performance and conformance. The processes identified here are not the exclusive responsibility of the IT function; rather, if a business decides to use a master data management approach, it should address the processes (and related practices) identified here to do so efficiently and effectively.
Organisational Structures	The following information-centric organisational structures/roles are key in supporting master and reference data management activities (Note: These are not current COBIT 5 RACI roles.): • Enterprise architecture committee • Business data stewards • Data/information architects • Application architects • Data providers • Data integration architects and developers • Data consumers, for example: – Application users – BI and reporting users – Application developers
Culture, Ethics and Behaviour	The following behaviours are important for maintaining control over master data management: • People focus—Stakeholders have different data needs. • Negotiating skills—Data architects/stewards need to be able to negotiate amongst different stakeholders to gradually progress. • Ability to think outside of silos and consider enterprise perspective

[11] Source: Data Management Association International (DAMA), *The DAMA Guide to the Data Management Body of Knowledge* (DMBOK), USA, 2009, Section 8.3.1

[12] Source for all example activities in this table: Data Management Association International (DAMA), *The DAMA Guide to the Data Management Body of Knowledge* (DMBOK), USA, 2009, Section 8.3.2

Figure 51—Illustrative Set of Enablers for Master and Reference Data Management *(cont.)*

Enabler	How Can This Enabler Help to Address the Issue?
Information	A number of information items are essential for governing and managing master data management initiatives: • Information architecture diagram • Data models • Data quality metrics • Data classification scheme • Data security and control • Data integrity procedures • Record matching rules • Data quality reports • Change request procedures, reference and master data requirements, description of sources of data and data contributors
Services, Infrastructure and Applications	A number of services (usually to be provided by the IT function) are relevant in a master data management context, for example: • Database master data management tools (Microsoft®, Oracle®, etc.) • Reference data management applications • Master data management applications • Process modelling tools • Metadata repositories • Data cleansing tools • Data integration tools • Change management tools • Business process and rule engines
People, Skills and Competencies	Some skills and competencies requirements for master data management use include: • Information architects • Enterprise architecture

4.7 Information Governance/Management Issue: End-user Computing

4.7.1 Issue Description and Business Context

The ISACA online glossary (*www.isaca.org/glossary*) defines end-user computing as the ability of end users to design and implement their own information system utilising computer software products.

End-user computing in an enterprise/business context is not strictly defined; it can include a broad range of technologies and techniques that allow end users to build their own applications for their personal or departmental purposes. Very often, they are built to replace or to complement corporate applications that do not address adequately personal or departmental information requirements, or do not address them fast enough. Usually, the end-user computing applications do not run on enterprise servers, but on user workstations or the like, using, in most cases, spreadsheet and database-based applications.

End users perceive a number of benefits to end-user computing, such as they feel that they:
- Are empowered and more valued to process information to meet their own needs
- Can obtain the information that they require for achieving their business objectives much faster and in the format that they require
- Have much more flexibility in obtaining and working with the required information

From an enterprise point of view, a number of potential business issues and risk are often raised, such as:
- The business case for end-user computing is often very informal and based on departmental needs and benefits. The enterprise may lose oversight over the applications that are being developed and subsequently put in operation, with the potential of many duplications and inefficiencies. Although efficiency gains might be realised at the departmental level, this is not necessarily the case at the enterprise level.
- Quality control is not to the same level over end-user computing application development; hence, processing results might be more subject to errors, etc. At the same time, getting end-user computing applications to a stable state might require more time and effort than originally planned (if planned at all).
- The technologies used are usually inherently more prone to errors. The level of requirements specification and documentation is often much more informal.
- In many cases, data feeds into end-user computing applications are not automated and introduce manual interventions; data feeds may also be misinterpreted or the structure of data feeds may change, etc., all leading to potential 'garbage in, garbage out' applications.
- Expertise on end-user computing applications is usually concentrated with very few people or one person.
- Skill levels of end users for application development vary widely and are usually not part of the enterprise skills management system (unlike the skills of the IT department). In other words, there is no adequate view and management of required skill levels and, consequently, training might be lacking.
- Compliance with the enterprise information architecture, data definitions and classification schemes has less assurance, e.g., end-user computing applications might generate information/reports that define certain information items differently compared to other enterprise applications.
- Usually, access to sensitive enterprise information systems is secured, but once data exits enterprise systems and enters end-user computing applications, assurance of adequately secured data no longer exists, resulting in a higher risk of data leakage.
- Pertaining to the previous risk, information is pushed to or shared with all types of new devices, mostly mobile, with the related security problems.
- Pertaining to the previous risk, the distribution (and life cycle in general) of the information resulting from end-user computing applications is more difficult to manage and control.
- Supporting a wide variety of end users with varying skill levels, from highly governed (controlled) users to information and knowledge workers with great degrees of autonomy, is a challenge.
- There is potential for further disintermediation for IT, e.g., by using cloud services, software as a service (SaaS) solutions, etc.
- Managing and controlling (semi-)structured information in spreadsheets and related types of applications is a challenge. Outdated or intermediate versions should not be distributed to external parties.
- There is risk for legal exposure due to regulatory violations and failure to implement retention practices. Intellectual property ownership issues can arise if an employee claims to be the author of a certain end-user computing application.
- When 'bring your own device' (BYOD) is allowed, control over the dissemination of the information becomes even more important.

It is the responsibility of each enterprise to weigh the potential advantages against the risk and to decide how to deal with end-user computing and how to achieve maximum benefits from end-user computing, within optimal risk and resourcing levels.

4.7.2 Affected Information

4.7.2.1 GOALS DIMENSION—QUALITY GOALS

Figure 52 lists typical information items or types affected by end-user computing. Information quality goals of the information processed and delivered by the end-user computing may or may not be achieved, depending on the quality of the end-user computing design, implementation and use.

Figure 52—Illustrative Information Quality Goals for End-user Computing

Information Item	Most Relevant Quality Dimension	Information Quality Goal
• Any type of information in any business function can be subject to end-user computing. • Usually, end-user computing is used in a context of obtaining management information for decision making that is based on feeds of operational information.	• Accuracy • Objectivity • Relevancy • Completeness • Currency • Interpretability • Ease of manipulation • Availability • Security and accessibility	• Output of end-user computing applications is accurate, timely, available and suitable for basing management decisions. • End-user computing applications and the resulting information do not increase the information risk of the enterprise.

4.7.3 Affected Goals

End-user computing can affect the following goals throughout the goals cascade, in either direction:[13]

- The information quality goals listed in **figure 52** support the achievement of the goals that are associated with an IT function, i.e., IT-related goals, which are listed in **figure 53**.
- The IT-related goals support the enterprise goals, which are also listed in **figure 53**. The ultimate purpose of the business user is to better achieve overall enterprise goals. The enterprise goals that are possibly affected by end-user computing are listed in **figure 53**.

Figure 53—Illustrative Goals Cascade for End-user Computing

IT-related Goals and Business Function Goals	Many IT-related goals can be derived. Following are several of the most important goals: • ITG02 IT compliance and support for business compliance with external laws and regulations • ITG04 Managed IT-related business risk • ITG05 Realised benefits from IT-enabled investments and services portfolio • ITG07 Delivery of IT services in line with business requirements • ITG08 Adequate use of applications, information and technology solutions • ITG09 IT agility • ITG10 Security of information, processing infrastructure and applications • ITG11 Optimisation of IT assets, resources and capabilities • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards • ITG14 Availability of reliable and useful information for decision making In more general terms, the business functions that use end-user computing have equivalent goals, for example: • Availability of reliable and useful information for decision making • Flexible and expedient access to required information for business function management
Enterprise Goals	The following enterprise goals can be considered most relevant: • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with external laws and regulations • EG08 Agile responses to a changing business environment • EG09 Information-based strategic decision making • EG11 Optimisation of business process functionality • EG12 Optimisation of business process costs

[13] 'Either direction' means that a number of goals can be positively influenced by a good end-user computing implementation and that others may be negatively influenced by a lower quality end-user computing implementation.

4.7.4 Enablers to Address the Issue

COBIT 5 is a comprehensive framework for governance and management of enterprise IT that allows enterprises to address the issue arising from end-user computing. **Figure 54** gives a set of enablers that can assist in achieving the desired benefits while optimising risk and resource use of end-user computing.

Figure 54—Illustrative Set of Enablers for End-user Computing

Enabler	How Can This Enabler Help to Address the Issue?
Principles, Policies and Frameworks	Provides rules/guidance of adoption, use, sharing and disposal of information in the context of end-user computing, including: • Defining what is expected from end users in terms appropriate use and custodianship of allocated assets and privileges • Communicating what the enterprise is going to govern and manage regarding end-user computing concerns and how it will accomplish this • Treatment of information on edge devices • Continuous education of accountable end-user professionals Useful reference frameworks to consult are: • The Institute for End User Computing, Inc. (*www.ieuc.org*) • ITIL® (*www.itil-officialsite.com*) • COBIT 5 (*www.isaca.org/COBIT*) • The Help Desk Institute (HDI®) (*www.thinkhdi.com*)
Processes	A number of governance and management processes (from *COBIT 5: Enabling Processes*) are relevant in the context of end-user computing, and can be used to define a set of governance and management practices capable of dealing with end-user computing issues. The processes identified here are not the exclusive responsibility of the IT function; rather, if a business function decides to use end-user computing, it should at least participate in the following processes or put in place its own processes: • EDM02 Ensure benefits delivery. • EDM03 Ensure risk optimisation. • EDM04 Ensure resource optimisation. • APO03 Manage enterprise architecture. • APO08 Manage relationships. • APO09 Manage service agreements. • APO10 Manage suppliers (when end-user applications and infrastructure is outsourced). • APO11 Manage quality. • APO13 Manage security. • BAI03 Manage solutions identification and build. • BAI08 Manage knowledge. • BAI09 Manage assets. • BAI10 Manage configuration. • DSS02 Manage service request and incidents. • DSS05 Manage security services. • DSS06 Manage business process controls. • MEA01 Monitor, evaluate and assess performance and conformance. • MEA02 Monitor, evaluate and assess the system of internal control. End-user computing applications should also be subject to management assessment and to internal audits.
Organisational Structures	Key responsibility in end-user computing: • Business process owners End-user services support function: • Help desk function • Training Other related functions can include: • Architecture • Security • Business continuity management • Quality assurance
Culture, Ethics and Behaviour	The following behaviours are important for maintaining control over end-user computing: • Guard against unauthorised use of privileged information by companies and individuals. • Guard against misuse of corporate assets. • Guard against security breaches. • Ensure due diligence and accountability in knowledge work and corporate reporting, for example, supported by spreadsheets (i.e., testing and quality assurance is not required only in the classical 'IT development' process).

Figure 54—Illustrative Set of Enablers for End-user Computing *(cont.)*

Enabler	How Can This Enabler Help to Address the Issue?
Information	A number of information items are essential for managing end-user computing initiatives: • Employee data • IT assets data • Configuration data • End-user computing (process and systems) performance data • Vendor scorecards • Security and incident related data • Legal and regulatory requirements
Services, Infrastructure and Applications	A number of services (usually to be provided by the IT function) are relevant in an end-user computing context: • Mobile device management (MDM) • Encryption • Remote wiping • Remote operation • Service desk workflow and knowledge management • Virtualisation • Cloud services
People, Skills and Competencies	Some skills and competencies requirements for end-user computing include: • Adequate skills in technologies used for end-user computing need to be developed or acquired • Basic quality management and software development skills • Knowledge management (documentation to reduce overdependence on single individuals • Soft skills and communication skills

4.8 Information Governance/Management Issue: Disintermediation

4.8.1 Issue Description and Business Context

Disintermediation describes a situation whereby end users or departments are building their own information solutions, avoiding all or most involvement of the enterprise IT department. Disintermediation is somewhat related to end-user computing, although, with disintermediation, usually more robust solutions and services are acquired (e.g., cloud, SaaS solutions) compared to end-user computing applications. As with end-user computing applications, disintermediation is often used to replace or complement corporate applications that are not addressing adequately personal or departmental information requirements or not addressing them fast enough, and doing so at a lower cost and providing more autonomy.

End users perceive a number of benefits to disintermediation, they feel:

- Empowered and more valued to process information to their own needs and/or they feel less restrained by the enterprise IT department
- That they can obtain the information they require to achieve their business objectives much faster and in the format that they require
- Much more flexibility in obtaining and working with the required information

From an enterprise point of view, potential risk is often raised, for example:

- The business case of disintermediation is often less formal and based on departmental needs and benefits, not taking into account any dependencies. The enterprise might lose oversight over the applications that are being developed and subsequently put into operation, with the potential of many duplications and inefficiencies. Although efficiency gains might be realised at the departmental level, this is not necessarily the case at the enterprise level.
- Additional overhead is created, e.g., a number of supporting activities usually assumed by the enterprise department (help desk, support, problem management, training, application maintenance, relationship management with vendor, etc.) have to be established, and these might or might not be accounted for in the business case.
- Compliance with enterprise information architecture and data definitions has less assurance, e.g., disintermediated applications might generate information/reports that define certain information items differently, compared to other enterprise applications. These information items might not be easy to integrate with other enterprise applications.
- Usually, access to sensitive enterprise information systems is secured, but once data exits an enterprise system and enters disintermediated applications, assurance of adequately secured data no longer exists. Access control and security are partially out of control.
- Pertaining to the previous risk, information is pushed to or shared with all types of new devices, mostly mobile, with the related security problems.
- Pertaining to the previous risk, the distribution (and life cycle in general) of the information resulting from disintermediated applications is more difficult to manage and control.
- There is less assurance that all legal requirements have been duly taken into account, i.e., there is risk for legal exposure due to regulatory violations, failure to implement retention practices.

It is the responsibility of each enterprise to weigh the potential advantages against the risk and to decide how to deal with disintermediation and how to achieve maximum benefits from disintermediation, within optimal risk and resourcing levels.

4.8.2 Affected Information

Figure 55 lists typical information items or types affected by information disintermediation. Information quality goals of the information processed and delivered by the disintermediated solutions may or may not be achieved, depending on disintermediated services, their design, implementation, use and level of support.

Figure 55—Illustrative Information Quality Goals for Disintermediation

Information Item	Most Relevant Quality Dimension	Information Quality Goal
Any type of information in any business function can be subject to disintermediation, depending on what is available from (external) suppliers. Disintermediation can be applied to operational information and management information.	Quality dimension requirements vary depending on the data type. For example, for a disintermediated CRM-type application that works with customer (sales) data to support the sales function, the following dimensions are most relevant: • Accuracy • Completeness • Currency • Appropriate amount • Concise representation • Consistent representation • Understandability • Availability	• All department or end-user information processing needs are achieved, in support of the business function. • The department or end-user needs have a sufficient level of support and maintenance at an optimal cost level. • Disintermediation does not increase the information risk of the enterprise.

4.8.3 Affected Goals

Disintermediation can affect the following goals throughout the goals cascade, in either direction:

- The information quality goals listed in **figure 55** support the achievement of the goals that are associated with an IT function, i.e., IT-related goals, which are listed in **figure 56**.
- The IT-related goals support the enterprise goals, which are also listed in **figure 56**. The ultimate purpose of disintermediation is to better achieve overall enterprise goals. The enterprise goals that are possibly affected by disintermediation are those listed in **figure 56**.

Figure 56—Illustrative Goals Cascade for Disintermediation

IT-related Goals and Business Function Goals	Many IT-related goals can be derived. Following are several of the most important goals: • ITG05 Realised benefits from IT-enabled investments and services portfolio • ITG06 Transparency of IT costs, benefits and risk • ITG07 Delivery of IT services in line with business requirements • ITG08 Adequate use of applications, information and technology solutions • ITG09 IT agility • ITG10 Security of information, processing infrastructure and applications • ITG11 Optimisation of IT assets, resources and capabilities • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG14 Availability of reliable and useful information for decision making • ITG17 Knowledge, expertise and initiatives for business innovation
Enterprise Goals	The following enterprise goals can be considered most relevant: • EG03 Managed business risk (safeguarding of assets) • EG08 Agile responses to a changing business environment • EG09 Information-based strategic decision making • EG10 Optimisation of service delivery costs • EG11 Optimisation of business process functionality • EG12 Optimisation of business process costs

4.8.4 Enablers to Address the Issue

COBIT 5 is a comprehensive framework for governance and management of enterprise IT that allows enterprises to address the issue of disintermediation. **Figure 57** gives a set of enablers that can assist in achieving the desired benefits while optimising risk and resource use of disintermediation initiatives.

Figure 57—Illustrative Set of Enablers for Disintermediation

Enabler	How Can This Enabler Help to Address the Issue?
Principles, Policies and Frameworks	Provides rules/guidance of adoption, use, sharing, disposal of information in the context of disintermediation, including: • Setting expectation to what is expected from departmental users in terms of appropriate use and custodianship of allocated assets and privileges • Communicating what and how the organisation is going to manage and govern disintermediated solution concerns • Treatment of information on edge devices • Continuous education of accountable end-user professionals Useful reference frameworks to consult are: • COBIT 5 • ITIL
Processes	A number of governance and management processes (from *COBIT 5: Enabling Processes*) are relevant in the context of disintermediation and can be used to define a set of governance and management practices for disintermediation: • EDM02 Ensure benefits delivery. • EDM03 Ensure risk optimisation. • EDM04 Ensure resource optimisation. • APO03 Manage enterprise architecture. • APO08 Manage relationships. • APO09 Manage service agreements. • APO10 Manage suppliers (when end-user applications and infrastructure is outsourced). • APO13 Manage security. • BAI03 Manage solutions identification and build. • BAI10 Manage configuration. • DSS02 Manage service request and incidents. • DSS05 Manage security services. • DSS06 Manage business process controls. • MEA01 Monitor, evaluate and assess performance and conformance. • MEA02 Monitor, evaluate and assess the system of internal control. Disintermediated applications should be subject to management assessment and to internal audits. The processes identified here are not the exclusive responsibility of the IT function; rather, if a business function decides to disintermediate, it should at least participate in the processes identified above or put in place its own processes, based on those listed here.

Figure 57—Illustrative Set of Enablers for Disintermediation ***(cont.)***

Enabler	How Can This Enabler Help to Address the Issue?
Organisational Structures	Key responsibility in disintermediation belongs to: • Business process owners End-user services support functions: • Help desk function • Training Other related functions can include: • Architecture • Security • Business continuity management • Vendor management
Culture, Ethics and Behaviour	The following behaviours are important for maintaining control over disintermediated solutions: • Objectivity and fairness in decisions on business cases for disintermediation • Balanced view on value, considering benefits but also risk and resource use; take into account the entire enterprise, i.e., the benefits and the burden for the entire enterprise • Sense of responsibility for protecting the enterprise information assets • Compensation practices aligned with the above described behaviours
Information	Information items are essential for managing disintermediation initiatives: • SLAs • Vendor performance (process and systems) data/dashboard • Security and incident related data • Legal and regulatory requirements
Services, Infrastructure and Applications	A number of services (usually to be provided by the IT function) are relevant in a disintermediation context: • Mobile device management (MDM) • Encryption • Service desk workflow and knowledge management • Cloud services
People, Skills and Competencies	Some skills and competencies requirements for disintermediation include: • Adequate skills in technologies used by service providers • Relationship management and negotiation skills • Basic quality management and software development skills • Knowledge management (documentation) to reduce overdependence on single individuals • Soft skills and communication skills

4.9 Information Governance/Management Issue: Regulatory Compliance

4.9.1 Issue Description and Business Context

According to the Organisation for Economic Co-operation and Development (OECD), the objectives of compliance are to 'influence positively the behaviour of the regulated community to make its members comply with environmental requirements. Voluntary compliance and reversal of an offence can be considered to be the main goal of inspection and enforcement. Punishment of the offender should be a secondary purpose'.[14]

Regulatory compliance is the term generally used to describe the policies and processes that enterprises have in place to ensure that they follow the many laws, rules and regulations established by the regulating bodies that control activity in a given jurisdiction.

Regulatory requirements exist at various levels, for example:

- **Cross-industry**—All enterprises that are publicly traded are subject to Sarbanes Oxley (for the United States), all enterprises are subject to personal data protection regulations (for the European Union).
- **Industry-specific**—Several industry sectors have very specific requirements, e.g., health care (the US Health Insurance Portability and Accountability Act [HIPAA]), pharmaceuticals (Good Manufacturing Practices), financial industry (Anti-Money Laundering [AML]).
- **Foreign nation regulatory issues**—Requirements of foreign countries that affect the enterprise and laws of the enterprise home country that affect trade with and use of products from foreign countries, e.g., Unfair competition laws (in the United States).

Issues to address when dealing with regulatory compliance include:

- **Identifying all applicable compliance requirements and managing these requirements adequately**—Multiple requirements may partially overlap and different requirements may apply to different parts of the enterprise (based on location, type of activities, etc.). Conflicting requirements need to be managed.
- **Mapping requirements to existing systems and information**—This mapping may result in new system and information quality requirements that need to be implemented, based on a business case that weighs added value against risk of non-compliance.

The following example (**figure 58**) illustrates the types of information items that are important with regard to regulatory compliance.

Figure 58—Example Regulatory Requirements

A governance, risk, and compliance (GRC) team is challenged by Sarbanes-Oxley (SOX) regulations and is concerned especially with IT systems that process and produce information employed in material statements of the enterprise financial position. The direction is that SOX-related systems need to demonstrate the highest levels of compliance with IT best practices that are related to security, software quality, release management and change management. However, development and operations staff cannot easily determine whether a system is SOX-related.

The GRC team works with its IT partners in corporate systems development and support (functional areas) to understand the information that they need and build the necessary capability. Fortunately, a comprehensive list of the application services has been compiled and is under active maintenance. At first, the development team proposes that a simple 'SOX attribute' be added to this list. This is done, and the presence or absence of this flag signals to the IT staff and auditors whether the system needs to meet the highest standards for security, testing, release and change management.

This solution works well for a time, and, due to its success, additional regulatory flags are sought (HIPAA/HITECH and others). At this point, IT development proposes that, rather than adding a distinct flag for each regulation (which requires development effort), a more generalised structure be developed that can be administratively maintained by the GRC team. Also, process discussions concerning the maintenance of the data are ongoing, and data quality checks are established.

This case illustrates a nuance of data management that is critical for both business and IT staff to understand. Although the major information items may be 'application portfolio' and 'relevant regulations', the value is found in their combination: **the regulations applicable to each application**. Each information item may live in very distinct data sets, perhaps on very different IT infrastructures, but cross-referencing them requires that both items reside in a common system. Trained staff must define a process to establish the cross references, and this, in turn, may drive training requirements, since no one may understand both information items and their environments. Such requirements to join or cross-reference data may drive IT architecture and should be understood early in an information-centric project. These requirements also demonstrate the importance of data modellers and their involvement from the outset of a project.

Regulatory compliance and compliance reporting need to be viewed as a natural extension of the governance duties of enterprise boards and executive management. Moreover, only good governance can ensure that compliance is aligned with the enterprise business objectives and risk management strategies—and is thereby adding real value (and not just cost) to the enterprise.

[14] Organisation for Economic Co-operation and Development (OECD), "Assuring Environmental Compliance," France, 2004

4.9.2 Affected Information

Figure 59 lists typical information items or types affected by regulatory compliance issues. It also contains the most relevant information quality goals of the information processed and delivered by the solutions that need to comply with applicable regulations.

Figure 59—Illustrative Information Quality Goals for Regulatory Compliance

Information Item	Quality Dimension	Information Quality Goal
Application service portfolio	• Completeness • Currency • Accuracy	Comprehensive listing of all IT services that directly support business operations.
Relevant regulations	• Relevancy • Accuracy • Availability • Currency • Completeness	Comprehensive listing of all regulations that are relevant to a given enterprise; includes the allocation of those regulations to the IT systems that are particularly concerned with or affected by the regulatory burden.
Regulated information can be any type of information, depending on industry, territory, etc. For example, transaction data, client data and product data.	• Completeness • Accuracy • Available • Security/accessibility • Appropriate amount	Regulated information of any type that needs to comply with applicable regulations; this translates to the quality dimensions listed in this figure.

4.9.3 Affected Goals

Regulatory compliance can affect the following goals throughout the goals cascade:

- The information quality goals listed in **figure 59** are related to overall goals that are associated with an IT function, i.e., IT-related goals, which are listed in **figure 60**.
- The IT-related goals support the enterprise goals, which are also listed in **figure 60**. The ultimate purpose of regulatory compliance is to better achieve overall enterprise goals. The enterprise goals that are possibly affected by regulatory compliance are those listed in **figure 60**.

Figure 60—Illustrative Goals Cascade for Regulatory Compliance

IT-related Goals and Business Function Goals	Many IT-related goals can be derived. Following are several of the most important goals: • ITG02 IT compliance and support for business compliance with external laws and regulations • ITG04 Managed IT-related business risk • ITG10 Security of information, processing infrastructure and applications • ITG15 IT compliance with internal policies
Enterprise Goals	The following enterprise goals can be considered most relevant: • EG04 Compliance with external laws and regulations • EG15 Compliance with internal policies

4.9.4 Enablers to Address the Issue

COBIT 5 is a comprehensive framework for governance and management of enterprise IT that allows enterprises to address the issue of regulatory compliance. **Figure 61** gives a set of enablers that can assist in achieving the desired benefits while optimising risk and resource use of regulatory compliance. Regulatory compliance efforts must be properly governed and managed to ensure their effectiveness.

Figure 61—Illustrative Set of Enablers for Regulatory Compliance

Enabler	How Can This Enabler Help to Address the Issue?
Principles, Policies and Frameworks	• Policies—Policy documents that broadly define an enterprise's values with respect to regulatory compliance • Planning and design documents—Help to organise the regulatory compliance tasks • Internal control documentation • Procedures—The use of standard operating procedures (SOPs) increases reproducibility of execution and allows for further brevity in both internal control documentation and reports. • Approvals—Each of the internal control documents described in regulatory compliance is subject to formal control and approval.

Figure 61—Illustrative Set of Enablers for Regulatory Compliance *(cont.)*

Enabler	How Can This Enabler Help to Address the Issue?
Processes	A number of governance and management processes (from *COBIT 5: Enabling Processes*) are relevant in the context of regulatory compliance: • EDM03 Ensure risk optimisation. • EDM05 Ensure stakeholder transparency. • APO03 Manage enterprise architecture. • APO12 Manage risk. • APO13 Manage security. • BAI01 Manage programmes and projects. • BAI06 Manage changes. • BAI08 Manage knowledge. • BAI10 Manage configuration. • DSS04 Manage continuity. • DSS05 Manage security services. • DSS06 Manage business process controls. • MEA02 Monitor, evaluate and assess the system of internal control. • MEA03 Monitor, evaluate and assess compliance with external requirements.
Organisational Structures	The following organisational structures are key for regulatory compliance: • Compliance group • Business process owners • Business executives • Audit • Architecture board
Culture, Ethics and Behaviour	The following behaviours are important for maintaining regulatory compliance: • Ethical behaviour • Learning culture • Risk awareness • Sense of ownership
Information	The following information items are essential for managing regulatory compliance: • Rules for validating and approving mandatory reports • Assessment of reporting effectiveness • Communications of changed compliance requirements • Compliance assurance reports • Compliance audit results • Compliance confirmations • Compliance requirements register • Identified compliance gaps • Insurance policy reports • Legal and regulatory compliance requirements • Licence deviations • Log of required compliance actions • Reports of non-compliance issues and root causes • Results of installed licence audits • Updated policies, principles, procedures and standards
Services, Infrastructure and Applications	A number of services (usually to be provided by the IT function) are relevant for regulatory compliance: • Configuration management database • Metadata repository/data dictionary • Security management systems • Enterprise/data architecture system • Testing and validation The following applications are also relevant: • GRC applications • Reporting tools • Logs • Identity management • Business process management • Audit trail
People, Skills and Competencies	The core regulatory compliance skills may cover a substantial range of skills, including: • Risk assessment • Internal control • Regulations contents • Information architecture • Security • Business process analysis

4.10 Information Governance/Management Issue: Privacy

4.10.1 Issue Description and Business Context

The ISACA glossary defines privacy as the freedom from unauthorised intrusion or disclosure of information about an individual. This information can include:

- Personal information of the individual
- Indications of behaviour including sensitive social issues, such as sexual preference, political activities and religious practices
- Communication carried out by the individual, which involves all forms of communication, including voice, data, speech and writing

This freedom from unauthorised intrusion or disclosure is globally acknowledged. However, differences can be found when nations translate privacy into the different legislations, because 'privacy' (sometimes referred to as 'data protection') also deals with the protection of rights of individuals with respect to their data or information (right to be informed, right to modify personal information, right to destroy personal information, etc.). This difference in legislation translation creates an additional challenge for multinational enterprises when implementing the required enablers to cope with privacy regulatory compliance. In this regard, privacy is a holistic subject that requires the enterprise to take a holistic approach, as follows:

- **Regulatory compliance on privacy requirements**—Regulatory requirements are important; however, the actual initiator of the need for privacy is the implied individual. This means that enterprises should assess whether the regulatory requirements with which they are compliant are sufficient to satisfy privacy requirements of other clients.
- **Information security**—The implementation of privacy is often directly linked to the implementation of technical information security measures. The protection of information within the enterprise in terms of confidentiality is imperative to avoid unauthorised intrusion or disclosure. However, other enablers are at least as important to protect the privacy of information. Culture, for example, can induce the necessary awareness with staff members who handle sensitive information that cannot always be protected with only technical measures.
- **The IT department**—To efficiently protect the privacy of individuals, cooperation is required throughout the entire enterprise, including the legal, human resources (HR), marketing and finance departments.

It is clear that a balance needs to be found between the use of information and the privacy related to it. The profitability and competitive position of an enterprise is often dependent on analysing existing information. From an enterprise point of view, the lack of regulatory compliance can lead to fines or convictions. Moreover, the reputational damage related to privacy incidents can lead to the loss of clients and strongly undermine the competitive position of the enterprise.

4.10.2 Affected Information

Figure 62 lists typical information items or types affected by privacy compliance issues. It also contains the most relevant information quality goals of the information processed and delivered by the solutions that need to comply with privacy regulations.

Figure 62—Illustrative Information Quality Goals for Privacy Compliance

Information Item	Most Relevant Quality Dimension	Information Quality Goal
All information items related to individuals, including customers and staff	• Accuracy • Completeness • Currency • Security/accessibility	Personal information of any type needs to comply with the relevant regulations.

4.10.3 Affected Goals

Privacy issues can affect following goals throughout the goals cascade:

- The information quality goal listed in **figure 62** supports the achievement of the goals that are associated with an IT function, i.e., IT-related goals, which are listed in **figure 63**.
- The IT-related goals support the enterprise goals, which are also listed in **figure 63**. The ultimate purpose of privacy compliance is to better achieve overall enterprise goals. The enterprise goals that are possibly affected by privacy compliance are those listed in **figure 63**.

Figure 63—Illustrative Goals Cascade for Privacy Compliance

IT-related Goals and Business Function Goals	Many IT-related goals can be derived. Following are several of the most important goals: • ITG02 IT compliance and support for business compliance with external laws and regulations • ITG04 Managed IT-related business risk • ITG08 Adequate use of applications, information and technology solutions • ITG10 Security of information, processing infrastructure and applications • ITG15 IT compliance with internal policies • ITG16 Competent and motivated business and IT personnel
Enterprise Goals	The following enterprise goals can be considered most relevant: • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with external laws and regulations • EG15 Compliance with internal policies

4.10.4 Enablers to Address the Issue

COBIT 5 is a comprehensive framework for governance and management of enterprise IT that allows enterprises to address the business issues raised by privacy-focused legislation and regulations. **Figure 64** gives a set of enablers that can assist in achieving the desired benefits while optimising risk and resource use in privacy-related initiatives.

Figure 64—Illustrative Set of Enablers for Privacy Compliance

Enabler	How Can This Enabler Help to Address the Issue?
Principles, Policies and Frameworks	Various countries have very specific laws and regulations relating to the data that may and may not be stored and transmitted across jurisdictions. This may include absolute prohibitions and contextual prohibitions. For example, storing an individual's race may be absolutely prohibited in all cases. A company may be further prohibited from storing data about customers that have no apparent relationship to its business. For example, an apparel vendor may store the individual's height, but a computer company would be prohibited from doing so. Therefore, enterprises should adopt a privacy-by-design principle in every part of the information life cycle. In addition to the regulatory requirements, customer rights, such as 'opt-in' and 'opt-out', are critical privacy enablers and must be respected. In terms of policies, a number of policies can be relevant: • Relevant board-level policies may include records management and information security management policies. • Specific data governance or data management policies may also exist or be in consideration. • A dedicated privacy policy can be developed outlining the rights of the individuals involved and how privacy will/needs to be protected.
Processes	A number of governance and management processes (from *COBIT 5: Enabling Processes*) are relevant in the context of privacy and can be used to define a set of governance and management practices capable of dealing with privacy issues: • EDM03 Ensure risk optimisation. • EDM05 Ensure stakeholder transparency. • APO1 Manage the IT management framework (specifically APO1.06 for data classification guidelines). • APO03 Manage enterprise architecture. • APO12 Manage risk. • APO13 Manage security. • BAI02 Manage requirements definition. • DSS05 Manage security services. • MEA02 Monitor, evaluate and assess the system of internal control. • MEA03 Monitor, evaluate and assess compliance with external requirements.
Organisational Structures	Key responsibility to overcome this issue belongs to: • Privacy officer—An individual who is responsible for monitoring the risk and business impacts of privacy laws and for guiding and coordinating the implementation of policies and activities that will ensure that the privacy directives are met • Information security manager Other related functions can include: • Records management • Document management • Enterprise architecture • Data/information architecture • Business process owners • Business executives • Audit
Culture, Ethics and Behaviour	The following behaviours are important for maintaining control over privacy issues: • Ethical behaviour • Learning culture • Risk awareness • Sense of ownership

Figure 64—Illustrative set of Enablers for Privacy Compliance *(cont.)*

Enabler	How Can This Enabler Help to Address the Issue?
Information	A number of information items are essential for managing privacy issues: • Data security and control guidelines • Data classification guidelines • Approved user access rights • Classification of information sources
Services, Infrastructure and Applications	A number of services (usually to be provided by the IT function) are relevant in a privacy context: • Metadata repository/data dictionary • Security management systems • Enterprise/data architecture system • Data profiling tools • Database management systems • Document management systems
People, Skills and Competencies	Some skills and competencies requirements for privacy include: • Business process analysts • Data analysts • Security analysts • Records managers

Page intentionally left blank

Appendix A
Reference to Other Guidance

This appendix provides reference information about the following related framework and standard and a mapping between the guidance and COBIT 5:
- DAMA-DMBOK functional framework
- ISO 15489-1:2001

The mapping consists of a list of clauses from the reference guidance (at a reasonable level of granularity) and the corresponding/relevant sections in *COBIT 5: Enabling Information*, *COBIT 5: Enabling Processes* or the COBIT 5 framework.

DAMA-DMBOK Framework

The DAMA-DMBOK framework is based on the following concepts:
- Data life cycle
- Data management functions
- Data management environmental elements

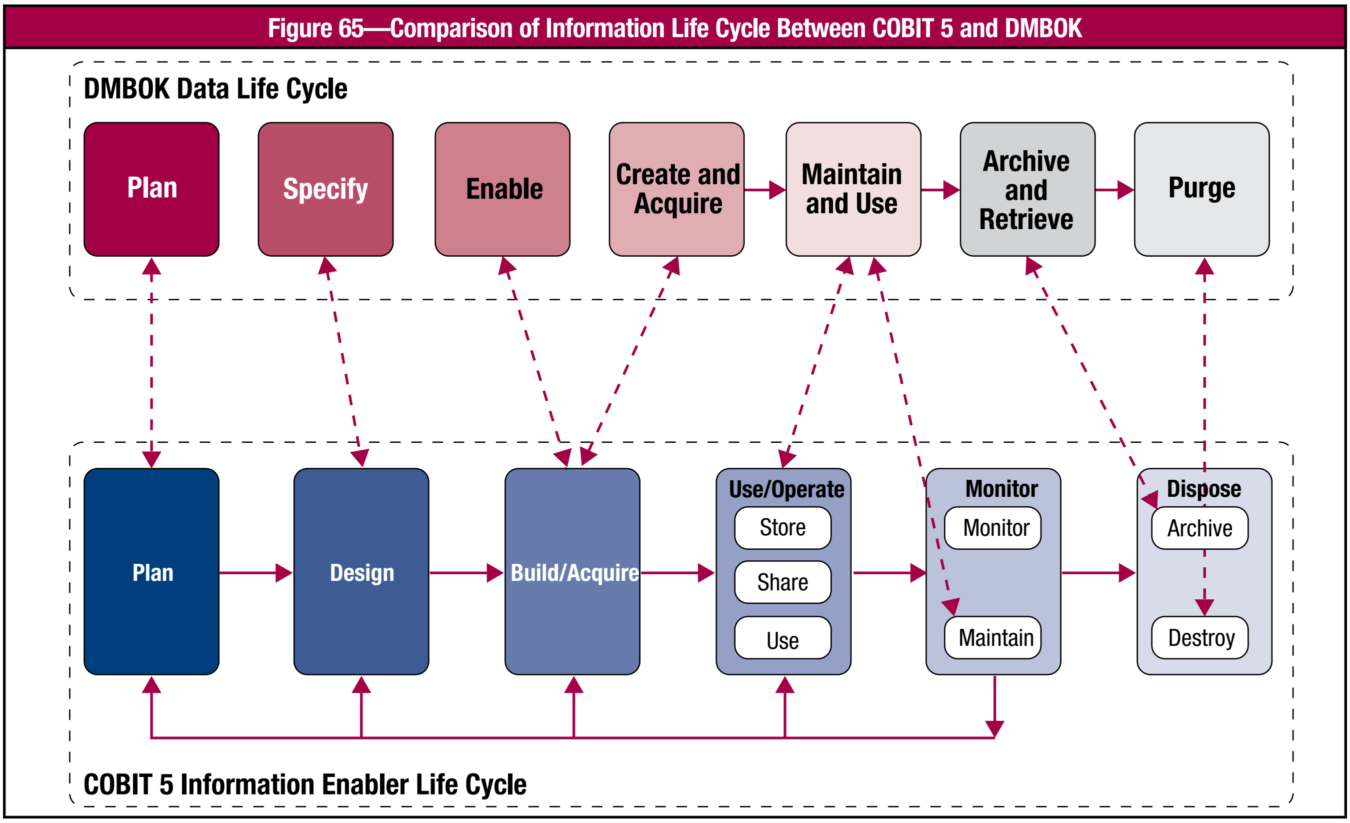
Overall, DAMA-DMBOK contains a great amount of detailed practical guidance that is not found in COBIT 5. COBIT 5 and DAMA-DMBOK are quite complementary to each other, for example:
- COBIT 5 users can benefit from this more detailed guidance by reading the DMBOK topics related to the COBIT 5 area in which they are interested.
- DAMA-DMBOK users can find a more rigorously structured, overall, governance and management framework and thus better position their own practices. In addition, they may find that the enabler concept can add some more value to their established practices.

The remainder of this appendix discusses briefly each of the DAMA-DMBOK framework concepts and how each of them compares to COBIT 5 and/or their COBIT 5 equivalent construct.

The Data Life Cycle

Both DMBOK and COBIT 5 (through the COBIT 5 information model) contain an information life cycle as one of the enabler dimensions. Both are depicted in **figure 65**.

Figure 65—Comparison of Information Life Cycle Between COBIT 5 and DMBOK



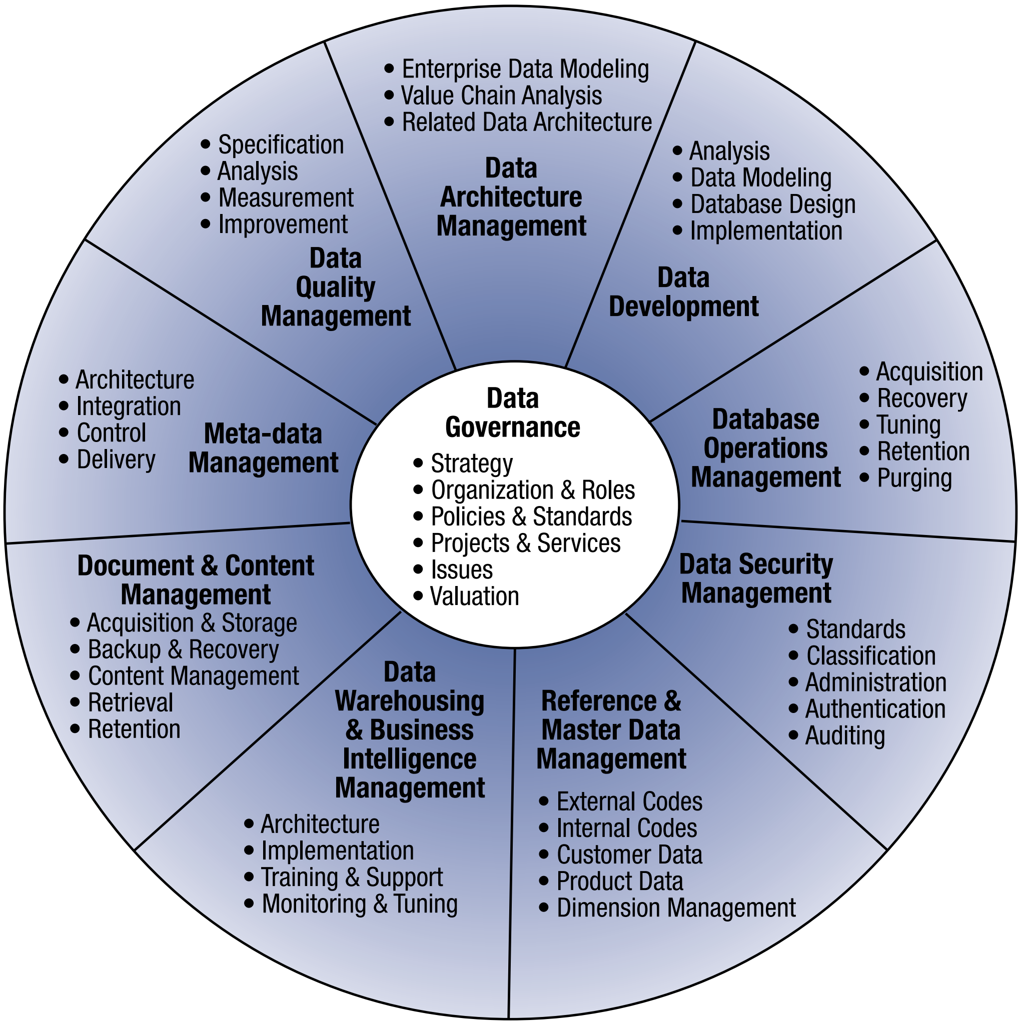
The life cycles are not identical, although they resemble each other reasonably well and most stages in each life cycle can be mapped against each other. It is therefore fair to conclude that both frameworks deal with the full life cycle of information, providing comprehensive and end-to-end guidance.

Data Management Functions

DMBOK identifies 10 data management functions, including data governance, shown in **figure 66**. The 10 functions are process based (activities are defined, etc.), so they are compared mainly to the COBIT 5 process reference model (*COBIT 5: Enabling Processes*).

In general, the COBIT 5 processes covering the functions defined in DMBOK remain at a higher level of abstraction compared to the data management function descriptions in DMBOK, which are (substantially) more detailed. **Figure 67** illustrates how the DMBOK data management functions are covered by COBIT 5 processes. The reader should keep in mind that COBIT 5 processes are often more abstract and generic and, therefore, less specific towards information management.

Figure 66—DMBOK Data Management Functions

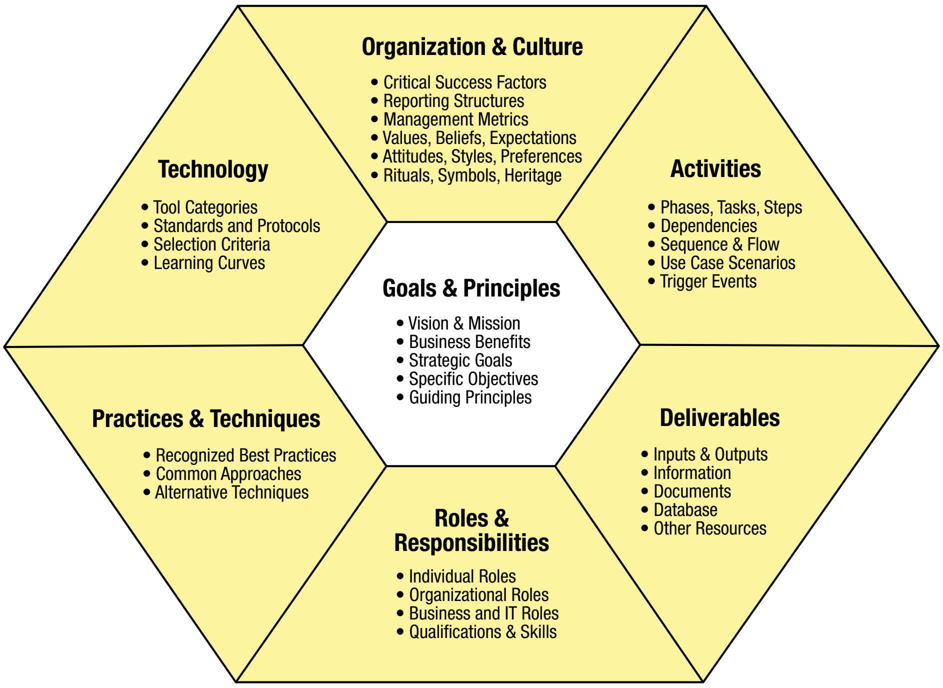


Source: *The DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK Guide), 1st Edition*, 2009, figure 1.4

Figure 67—DMBOK Data Management Functions Compared to COBIT 5

DAMA-DMBOK Component	COBIT 5 Equivalent Constructs/Components
Data Governance	The governance domain is a separate domain (Evaluate, Direct and Monitor [EDM]), containing separate governance processes. These processes are generic, i.e., are not specifically about information governance. However, since COBIT 5 is about information and related technology, inherently these processes cover all governance aspects. COBIT 5 also identifies a number of organisational structures and information items related to governance.
Data Architecture Management	Covered by the following process: • APO03 Manage enterprise architecture.
Data Development	Covered by the following processes: • BAI02 Manage requirements definition. • BAI03 Manage solutions identification and build. • BAI10 Manage configuration.
Database Operations Management	Covered by the following processes: • DSS01 Manage operations. • DSS02 Manage service requests and incidents.
Data Security Management	Covered by the following processes: • APO13 Manage security. • DSS05 Manage security services. • MEA01 Monitor, evaluate and assess performance and conformance. • MEA02 Monitor, evaluate and assess the system of internal control. • MEA03 Monitor, evaluate and assess compliance with external requirements.
Reference a Master Data Management	Covered by the following processes: • APO03 Manage enterprise architecture. • DSS06 Manage business process controls.
Data Warehousing and BI Management	Rather implicitly, BI is considered as one type of application that needs to be planned, developed, built and operated like many others, using a rather comprehensive set of COBIT 5 processes. The most relevant processes in this context are: • APO03 Manage enterprise architecture. • BAI02 Manage requirements definition. • BAI03 Manage solutions identification and build. • BAI10 Manage configuration.
Document and Content Management	Covered by the following processes: • BAI08 Manage knowledge.
Meta-data Management	Covered by the following process (implicitly): • APO03 Manage enterprise architecture.
Data Quality Management	Covered by the following processes: • APO11 Manage quality.

Figure 68—DMBOK Environmental Elements



Source: *The DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK Guide), 1st Edition*, 2009, figure 1.6

Data Management—Environmental Elements

DMBOK defines a number of environmental elements that apply to each of the 10 functional domains. These environmental elements are shown in **figure 68**, with their scope.

COBIT 5 does not have this specific construct, but through the 'enabler' dimension in COBIT 5 many of these elements are covered. **Figure 69** provides a high-level comparison.

Figure 69—DMBOK Environmental Elements Compared to COBIT 5 Enablers

DAMA-DMBOK Component	COBIT 5 Equivalent Constructs/Components
Goals and Principles	COBIT 5 states that governance and management of an area are achieved through continuous interaction between a number of properly working enablers. Each enabler has the same four dimensions, of which 'goals' is one.
Organization and Culture	COBIT 5 states that governance and management of an area are achieved through continuous interaction between a number of effective and efficient enablers. Both Organisational Structures and Culture, Ethics and Behaviour are enablers explicitly identified in COBIT 5 and, hence, always considered.
Activities	Processes are one of the enablers defined in COBIT 5. Within processes, more detailed guidance is provided through 'practices' and, at one deeper level of detail, 'activities'.
Deliverables	Processes are one of the enablers defined in COBIT 5. Within each process, generic inputs and outputs are defined for each process practice.
Roles and Responsibilities	Processes are one of the enablers defined in COBIT 5. Within processes, more detailed guidance is provided through 'practices'. For each process a RACI chart is included, which describes typical responsibilities for each practice. Responsibilities are assigned to one or several generic roles that typically exist in an organisation. Note: COBIT 5 stays at a relatively high level of abstraction when defining roles. More specific roles, e.g., in the area of information management, are not included but implied. DMBOK provides more detailed guidance.
Practices and Techniques	COBIT 5 states that governance and management of an area are achieved through continuous interaction between a number of effective and efficient enablers. This DMBOK component is covered by the COBIT 5 process enabler, where three levels of detail are included: Process, Practices, Activities. Note, however, that COBIT 5 process descriptions are example processes, without any intention to present the unique best practice.
Technology	COBIT 5 states that governance and management of an area are achieved through continuous interaction between a number of effective and efficient enablers. The Services, Infrastructure and Applications enabler deals with supporting technology for whatever topic at hand—information management in this case.

In conclusion, COBIT 5, with its integrated enabler model and the seven enabler categories, deals with all environmental elements as described in DMBOK, and both frameworks are equivalent from that point of view, i.e., they both have attention for more than only processes.

The relatively high level of abstraction of COBIT 5 and the fact that it is an overall governance and management framework for enterprise IT (as opposed to only dealing with data and information management issues) makes both frameworks complementary: COBIT 5 provides the overall framework, and DMBOK provides the specific details when required. Note: DAMA first published an update to the DMBOK framework, DMBOK2, as a comment draft in April 2012. Following a subsequent review period, DMBOK2 is scheduled to be available in the fourth quarter of 2013.

ISO 15489-1:2001

ISO 15489-1:2001 Introduction

International standard ISO 15489, Information and Documentation—Records Management (Geneva, 2001) was designed to meet records management requirements in businesses and governments alike by ensuring that 'appropriate attention and protection is given to all records, and that the evidence and information they contain can be retrieved more efficiently, using standard practices and procedures'.

High-level Comparison Between ISO 15489-1:2001 and COBIT 5

Chapter 4 of this guide discusses a number of information management issues and how COBIT 5 enablers can assist in addressing these issues. ISO 15489-1 can be described as very similar guidance: it describes how to deal with one specific information management issue, records management.

Records are a subset of all information items that an enterprise will generate during its operation, serving a very specific purpose. As such, *COBIT 5: Enabling Information* and the embedded information model applies to 'records' as well.

When comparing the COBIT 5 framework and the ISO 15489-1 standard (**figure 70**), the following should be kept in mind:

- COBIT 5 processes deal mainly with information and IT.
- Records management systems as described in ISO 15489-1 also contain manual/physical processes that are not necessarily excluded by COBIT 5, but are less explicitly described.

Figure 70—Comparing ISO 15489-1:2001 Clauses and COBIT 5

ISO 15489-1:2001 Section	COBIT 5 Equivalent Constructs/Components
6 Policy and responsibilities	Principles, Policies and Frameworks is one of the COBIT 5 enabler categories and, hence, covered by COBIT 5.
6.1 General	N/A
6.2 Policy	In practice, policies are set out by two key processes in COBIT 5: • EDM01 Ensure governance framework setting and maintenance. • APO01 Manage the IT management framework. The principles for records management and the related policies have to be set and maintained by these processes.
6.3 Responsibilities	The COBIT 5 process descriptions contain RACI charts, where responsibilities for process practices are assigned. COBIT 5 RACI charts contain a comprehensive set of roles and functions, most outside of the IT department. This aligns with the suggested records management responsibilities in ISO 15489, which assign most roles to non-IT department functions. ISO 15489 contains a suggested assignment of records management responsibilities, which can easily be translated into a RACI chart.
7 Records management requirements	
7.1 Principles of records management programmes	Principles, Policies and Frameworks is one of the COBIT 5 enabler categories, and the 'principles' aspect is therefore covered by COBIT 5. As in clause 6.2, the same COBIT 5 processes implement this in practice.
7.2 Characteristics of a record	The COBIT 5 framework builds on enablers; the framework describes a generic model for all enablers. In chapter 3 of this guide, this model is applied to the 'Information' enabler, further elaborated and illustrated. One of the dimensions of the Information enabler model is the quality/goals dimension, where a range of up to 15 information quality requirements can be defined. The 'record characteristics' of clause 7.2 correspond to the COBIT 5 information quality criteria, e.g.: • 'Authenticity' corresponds to reputation, restricted access and accuracy. • 'Reliability' corresponds to accuracy. • 'Integrity' corresponds to the COBIT 5 criteria completeness and accuracy. • 'Usability' is a combination of availability, ease of manipulation, understandability and interpretability.
8 Design and implementation of a records system	Services, Infrastructure and Applications is one of the COBIT 5 enabler categories, and hence covered by COBIT 5. A records management system can be considered as a combination of application(s), infrastructure and services, and is hence covered by this enabler category. This clause describes the requirements of such a records management system. COBIT 5 does not go into the detail of the design of any system, but it includes a comprehensive set of example processes to support the life cycle of information systems, i.e.: • APO03 Manage enterprise architecture. • BAI01 Manage programmes and projects. • BAI02 Manage requirements definition. • BAI03 Manage solutions identification and build. • BAI04 Manage availability and capacity. • BAI05 Manage organisational change enablement. • BAI08 Manage knowledge. • BAI09 Manage assets. • BAI10 Manage configuration.
9 Records management processes and controls	This clause deals with the business requirements, processes and associated control activities for records management. COBIT 5 does not describe nor does it enter into any detail of business processes, but there is one important process linking business process controls to the IT environment, i.e., DSS06 *Manage business process controls.* This process assumes that requirements for records management have been correctly identified and translated into supporting applications and processes (see clause 8).

Figure 70—Comparing ISO 15489-1:2001 Clauses and COBIT 5 *(cont.)*

ISO 15489-1:2001 Section	COBIT 5 Equivalent Constructs/Components
10 Monitoring and auditing	The Monitor, Evaluate and Assess (MEA) domain describes three processes designed to monitor and audit the records management systems.
11 Training	The following COBIT 5 process deals with training, BAI05 *Manage organisational change enablement.* In addition, People, Skills and Competencies is one of the COBIT 5 enabler categories.

Appendix B
Example Information Items Supporting Functional Area Goals

Figure 71 shows examples of the business information items that support the goals achievement of the enterprise value-chain functions (shown in **figure 6**) and that are communicated through information flows between the enterprise levels. The figure identifies whether the information items concern the governing body, management, or operations and execution enterprise levels.

Figure 71—Examples of Information Items in Information Flows That Support the Enterprise Value Chain Goals

Functional Area	Key (Business) Information Items Required to Support Achievement of Functional Area Goals		
	Governing Body	Management	Operations and Execution
Enterprise infrastructure (goals)	• Compliance assurance reports • Risk appetite • External financial auditors reports • Internal auditors reports • Compliance reports • Annual financial reports • Policies, processes and procedures • Information architecture and strategy • Business strategies • Project, programme, portfolio management data including results & benefits realization components • Strategic road map • Investment return expectations • Investment portfolio performance reports	• Risk profile • Risk management policies • Business impact analysis (BIA) reports • Financial statements • Financial management internal report (Budgets, revised estimates, benchmarks, periodic burn rates) • Enterprise architecture • Enterprise activity based cost accounting data • Real estate information • (IT) network/communication infrastructure information • Infrastructure capacity and use information • Information on location and reachability of the infrastructure	• Compliance requirements register • Log of required compliance actions • Real estate information • (IT) network/communication infrastructure information • Infrastructure capacity and use information • Information on location and reachability of the infrastructure
Human resources (goals)	• Reporting on allocation and effectiveness of resources and capabilities • Budget communications • Request fulfilment status and trends report • Guiding principles for allocation of resources and capabilities • Success measures and results • Salary information (human cost allocation status of each department or business unit)	• Remedial actions to address resource management deviations • Operation and use plan • Root causes of quality delivery failures • Budget allocations • Resource budget and plan • IT budget and plan • Communication of resourcing strategies • Skills and competencies matrix • Turnover ratios • Salary information (salary tables, human cost analysis) • 360-degree review feedback results	• Approved resources plan • Skills and competencies matrix • Incident status and trends report • Salary information • Performance reports • 360-degree review feedback results
Procurement (goals)	• Business cases • Legal and regulatory requirements • Information on required production goods and services • Information on required maintenance, repairs and operations supplies • Sourcing strategy	• Legal and regulatory requirements • Contractual requirements • Supplier information • Requests for information • Requests for proposals • Tenders • Warranties • Contract terms • Sourcing strategy	• Supplier information • Requests for information • Requests for proposals • Proposals • Warranties • Contract terms
Inbound logistics (goals)	• Business cases • Information on required production good and services • Customer demand • Customer demand forecast • Information on required maintenance, repairs and operations supplies • Information on required capital goods and services	• Legal and regulatory requirements • Contractual requirements • Information on required maintenance, repairs and operations supplies • Information on required capital goods and services • Warehouse information • Distribution centre information • Inventory information • Supplier information • Transportation information • Customer demand • Customer demand forecast	• Information on required maintenance, repairs and operations supplies • Information on required capital goods and services • Warehouse information • Distribution centre information • Inventory information • Supplier information • Transportation information • Customer demand • Customer demand forecast

Figure 71—Examples of Information Items in Information Flows That Support the Enterprise Value Chain Goals *(cont.)*

Functional Area	Key (Business) Information Items Required to Support Achievement of Functional Area Goals		
	Governing Body	Management	Operations and Execution
Operations (goals)	• Business cases • Quality requirements • Customer demand • Innovation ideas	• Legal and regulatory requirements • Contractual requirements • SLAs • Inventory information • Quality management system information • Business/production process models • Customer demand	• Downtime reports • Continuous improvement data—trending, Plan/Do/ Check/Act records/results • Transaction data • Inventory information • Quality management system information • Business/production process models
Outbound logistics (goals)	• Business cases • Customer demand • Customer demand forecast	• Legal and regulatory requirements • Contractual requirements • Warehouse information • Distribution centre information • Inventory information • Transportation information • Customer demand • Customer demand forecast	• Client data • Warehouse information • Distribution centre information • Inventory information • Transportation information • Customer demand • Customer demand forecast
Marketing and sales (goals)	• Stakeholder satisfaction data • BI (benchmarks reports, competitor responses, new laws and regulations) • Information on product • Information on price • Information on place • Information on promotion • Market segmentation information • Income/pricing models	• Competitors information • Customer analytics • Review results of quality of service, including customer feedback • Information on product • Information on price • Information on place • Information on promotion • Market segmentation information • Churn rates • Conversion rates • Income/pricing models • Sales information • Marketing cost • Marketing channel information	• Customer information • Product and services information • Churn rates • Conversion rates • Sales information • Marketing cost • Marketing channel information
Service (goals)	• Claims and dissatisfaction reports, number of claims resolved, metrics • SSAE 16 reports • Market research (input to service identification and delivery) • Benchmark information	• Enterprise service desk and customer satisfaction surveys • Evaluation criteria (for service providers) • Customer surveys (business needs driven, results driven, satisfaction driven) • Business SLAs • Customer analytics • Enterprise service level catalogue and agreements • Reverse logistics information	• Business continuity plan (BCP) • BCP testing results • Enterprise operations centre data, availability management • Customer analytics • Enterprise service level catalogue and agreements • Reverse logistics information
IT goals	Appendix C contains a comprehensive sample mapping table that shows how the IT-related goals are supported by a number of information items.		

Appendix C
Example Information Items Supporting IT-related Goals

Figure 72 contains typical information items that support the achievement of all 17 IT-related goals from the COBIT 5 goals cascade in the main COBIT 5 framework publication. The table is comprehensive, but not complete—each enterprise has unique information item needs and definitions.

Figure 72—Information Items Supporting IT-related Goals (Comprehensive)

Generic IT-related Goals		Key Information Items to Support Achievement of the IT-related Goal	Illustrative Quality Criteria	Related Metrics
ITG01	Alignment of IT and business strategy	IT strategy plan	• Currency	Time since last update of the IT strategic plan
		Enterprise strategy	• Completeness	Percentage of IT-related goals that are translated into potential IT-enabled investment programmes (road map)
		Investment types and criteria	• Reputation • Believability • Relevancy	Benchmark investment portfolio composition against industry (industry analyst reports)
		Performance reports	• Accuracy • Currency • Concise representation	Ease of reading and understanding by stakeholders
			• Relevance • Completeness	Stakeholder satisfaction with scope of the planned portfolio of programmes and services
ITG02	IT compliance and support for business compliance with external laws and regulations	• IT-related compliance requirements register • Compliance assurance reports	• Accuracy • Completeness • Currency	Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss
			• Accuracy • Completeness • Currency • Concise representation • Interpretability	Number of IT-related non-compliance issues reported to the board of directors or causing public comment or embarrassment
			• Accuracy • Completeness • Currency • Concise representation • Interpretability	Number of non-compliance issues relating to contractual agreements with IT service providers
			• Accuracy • Completeness • Currency	Coverage of compliance assessments
ITG03	Commitment of executive management for making IT-related decisions	Reward systems approach	• Relevancy	Number of reward approaches referencing IT-related decision making
		IT-related decision making model	• Availability • Currency • Believability	Percentage of executive management roles with clearly defined accountabilities for IT decisions
			• Accuracy • Availability • Currency • Believability	Frequency of IT strategy (executive) committee meetings
			• Accuracy • Currency • Believability	Rate of execution of executive IT-related decisions
		Enterprise governance guiding principles	• Accuracy	Number of times IT-related items are on the board of directors agenda in a proactive manner
			• Relevancy • Completeness • Understandability	Approval of governance principles by executive committee

Figure 72—Information Items Supporting IT-related Goals (Comprehensive) *(cont.)*

Generic IT-related Goals		Key Information Items to Support Achievement of the IT-related Goal	Illustrative Quality Criteria	Related Metrics
ITG04	Managed IT-related business risk	Risk appetite	• Objectivity • Accuracy	Diversity and accountability level (board of directors, executive, management, operational) of people determining the risk appetite
		Risk profile, including risk assessment results	• Currency	Frequency of update of risk profile
			• Accuracy • Objectivity	Percentage of critical business processes, IT services and IT-enabled business programmes covered by risk assessment
			• Accuracy • Objectivity • Currency	Number of significant IT-related incidents that were not identified in risk assessment
		Risk management policies	• Accuracy • Availability • Currency	Percentage of enterprise risk assessments including IT-related risk
ITG05	Realised benefits from IT-enabled investments and services portfolio	Strategic road map	• Accuracy • Relevancy • Completeness • Understandability	Percentage of IT-enabled investments included in the strategic road map
		Identified gaps in IT services to the business	• Accuracy • Objectivity • Reputation • Completeness • Currency	Percentage of gaps in IT services to the business previously identified covered by new IT services
		Performance reports	• Objectivity • Completeness	Percentage of IT-enabled investments where benefit realisation is monitored through full economic life cycle
			• Accuracy • Relevance • Currency	Percentage of IT services where expected benefits are realised
			• Accuracy • Relevance • Completeness • Currency	Percentage of IT-enabled investments where business case benefits are met or exceeded
		Actions to improve value delivery	• Objectivity • Believability • Relevance • Understandability	Percentage of contribution to improved value delivery per action
			• Accuracy • Objectivity • Believability • Understandability	Percentage of actions realising expected improvement in value delivery

Figure 72—Information Items Supporting IT-related Goals (Comprehensive) *(cont.)*

Generic IT-related Goals		Key Information Items to Support Achievement of the IT-related Goal	Illustrative Quality Criteria	Related Metrics
ITG06	Transparency of IT costs, benefits and risk	Requirements for stage-gate reviews	• Accuracy • Relevancy • Currency	Percentage of stage-gate reviews including budget versus actual check and related go/no-go limits
		Budget communications	• Completeness • Consistent representation • Understandability	Percentage of investment business cases with clearly defined and approved expected IT-related costs and benefits
			• Objectivity • Relevancy • Currency • Interpretability • Ease of manipulation	Satisfaction of key stakeholders regarding the transparency, understanding and accuracy of IT financial information
		Cost allocation communications	• Accuracy • Believability • Completeness • Consistent representation	Percentage of IT services with clearly defined and approved operational costs and expected benefits
			• Objectivity • Relevancy • Currency • Interpretability • Ease of manipulation	Satisfaction of key stakeholders regarding the transparency, understanding and accuracy of IT financial information
		Aggregated risk profile, including status of risk management actions	• Accuracy • Completeness	Percentage of risk profiles including IT financial impact information
		Results of cost optimisation reviews	• Accuracy • Reputation • Relevancy • Currency	Percentage of IT cost savings realised versus target realisation
		Benefits realisation reports	• Accuracy • Reputation • Relevancy • Currency	Percentage of IT benefits realised versus target benefit realisation
			• Objectivity • Believability • Relevancy • Completeness	Percentage of satisfaction amongst business users on new IT services

Figure 72—Information Items Supporting IT-related Goals (Comprehensive) *(cont.)*

Generic IT-related Goals		Key Information Items to Support Achievement of the IT-related Goal	Illustrative Quality Criteria	Related Metrics
ITG07	Delivery of IT services in line with business requirements	Clarified and agreed-on business expectation	• Accuracy • Completeness • Consistent representation • Understandability	Percentage of business cases for IT-enabled investments having clear and agreed-on business expectations/requirements
		Service level performance reports	• Accuracy • Objectivity • Reputation • Relevancy • Interpretability	Percentage of business process owners satisfied with IT service delivery meeting agreed-on service levels
		Quality review results including customer feedback, exceptions and corrections	• Objectivity • Believability • Relevancy • Completeness	Number of business disruptions due to IT service incidents
			• Accuracy • Objectivity • Relevancy • Currency	Percentage of users satisfied with quality and timeliness of IT service delivery
		Identified gaps in IT services to the business	• Accuracy • Objectivity • Relevancy • Currency	Percentage of users satisfied with the number of services IT delivers
			• Accuracy • Objectivity • Reputation • Completeness • Currency	Percentage of gaps in IT services to the business previously identified covered by new IT services
		Results of processing effectiveness reviews	• Accuracy • Objectivity • Relevancy • Completeness • Currency	Percentage of business users convinced recently updated IT services have considerably improved processing effectiveness

Figure 72—Information Items Supporting IT-related Goals (Comprehensive) ***(cont.)***

Generic IT-related Goals		Key Information Items to Support Achievement of the IT-related Goal	Illustrative Quality Criteria	Related Metrics
ITG08	Adequate use of applications, information and technology solutions	Recognition and reward programme	• Objectivity • Believability • Completeness	Percentage of business users considering the IT services provided as enhancing and facilitating their work
			• Objectivity • Believability • Completeness	Percentage of business process owners satisfied of the collaboration with the IT department
		Assessments of the use of innovative approaches	• Accuracy • Objectivity • Reputation • Understandability	Level of business user understanding of how technology solutions support their processes
		Success measures and results	• Objectivity • Believability • Completeness	Percentage of business process owners satisfied with supporting IT products and services
			• Accuracy • Relevancy • Completeness	Net present value (NPV) showing business satisfaction on the quality and usefulness of the technology solutions
		Compliance audit results	• Accuracy • Relevancy • Currency • Appropriate amount	Percentage of technology solutions compliant with policies and other applicable regulations
		Reviews of operational use	• Accuracy • Objectivity • Relevancy • Completeness	Percentage of unused features that were explicitly specified in the functional requirements
		Postimplementation review report	• Objectivity • Believability • Reputation • Currency	Satisfaction level of business users with training and user manuals
ITG09	IT agility	Data architecture (information architecture model), especially master data management and process architecture model	• Accuracy • Completeness • Relevance • Currency • Consistent representation • Ease of manipulation • Availability	Number of critical business processes supported by up-to-date infrastructure and applications
		Service portfolio	• Currency • Relevance • Availability	Average time to turn strategic IT objectives into an agreed-on and approved initiative
		Service portfolio operational metrics	• Objectivity • Relevance • Concise representation	Satisfaction level of business executives with IT's responsiveness to new requirements

Figure 72—Information Items Supporting IT-related Goals (Comprehensive) *(cont.)*

Generic IT-related Goals		Key Information Items to Support Achievement of the IT-related Goal	Illustrative Quality Criteria	Related Metrics
ITG10	Security of information, processing infrastructure and applications	Data classification guidelines	• Accuracy • Completeness • Interpretability • Understandability	Percentage of business users having a thorough understanding of the data classification guidelines
		Approved user access rights (in terms of roles and data sensitivities)	• Accuracy • Completeness	Time to grant, change and remove access privileges, compared to agreed-on service levels
		Classification of information sources (security taxonomy)	• Accuracy • Currency	Percentage of information classifications according to the security taxonomy
		Data security and control guidelines	• Accuracy • Objectivity • Completeness • Currency	Number of IT services with outstanding security requirements
		Security issues/incident counts	• Accuracy • Objectivity • Reliability • Relevancy • Completeness	Number of security incidents causing financial loss, business disruption or public embarrassment
		Summary metrics for information security	• Accuracy • Completeness • Currency • Interpretability	Percentage of accordance with current standards and guidelines during latest information security assessment
ITG11	Optimisation of IT assets, resources and capabilities	Enterprise architecture (data/information architecture model)	• Accuracy • Completeness • Currency	Frequency of capability maturity and asset optimisation assessments
			• Objectivity • Believability • Relevancy • Completeness • Currency • Interpretability • Understandability	Satisfaction levels of business and IT executives with IT-related assets, resources and capabilities
		Data integrity procedures	• Accuracy • Objectivity • Relevancy • Completeness • Currency	Percentage of business users satisfied with the integrity of business data
			• Accuracy • Completeness • Currency • Availability	Number of audit findings on timely follow-up and resolution of data integrity issues
		Portfolio alignment with information strategy (data redundancy, architecture gap analysis)	• Objectivity • Believability • Relevancy • Completeness • Currency • Interpretability • Understandability	Satisfaction level of business and IT executives with the alignment of IT-enabled initiatives with the information strategy
			• Accuracy • Objectivity • Believability • Relevancy • Completeness • Currency	Contribution of the portfolio initiatives to the (long term) information strategy realisation
			• Accuracy • Relevancy • Currency	Percentage of identified gaps solved by new portfolio initiatives

Figure 72—Information Items Supporting IT-related Goals (Comprehensive) ***(cont.)***

Generic IT-related Goals		Key Information Items to Support Achievement of the IT-related Goal	Illustrative Quality Criteria	Related Metrics
ITG12	Enablement and support of business processes by integrating applications and technology into business processes	Data architecture with mappings to business process (life cycle)	• Accuracy • Completeness • Currency	Percentage of business processes covered in the data architecture mapping
		Process architecture model	• Accuracy • Objectivity • Believability • Relevancy • Completeness • Currency	Level of accordance between process model and real life process execution
			• Accuracy • Completeness • Currency	Number of critical business processes fully supported by the process architecture model
		Information architecture model	• Accuracy • Objectivity • Completeness	Number of duplications found for each information entity
			• Accuracy • Completeness • Currency • Consistent representation • Interpretability	Evolution of the number of relationships between information items
			• Accuracy • Completeness • Currency	Number of unused information item attributes
		Architecture gap analysis	• Accuracy • Objectivity • Completeness • Currency	Number of applications or critical infrastructures operating in silos and not integrated
		Architecture quality assessments	• Accuracy • Relevancy • Completeness • Appropriate amount • Understandability	Number of business process changes that need to be delayed or reworked because of technology integration issues
			• Accuracy • Objectivity • Relevancy • Completeness	Number of business processing incidents caused by technology integration errors
			• Accuracy • Relevancy • Completeness • Appropriate amount • Understandability	Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues

Figure 72—Information Items Supporting IT-related Goals (Comprehensive) *(cont.)*

Generic IT-related Goals		Key Information Items to Support Achievement of the IT-related Goal	Illustrative Quality Criteria	Related Metrics
ITG13	Delivery of programmes delivering benefits on time, on budget, and meeting requirements and quality standards	Investment portfolio performance reports	• Accuracy • Completeness • Currency	Number of running programmes/projects on time and within budget
			• Objectivity • Believability • Relevancy • Completeness	Percentage of stakeholders satisfied with programme/project quality of deliverables
			• Accuracy • Objectivity • Relevancy • Currency	Number of programmes needing significant rework due to quality defects
		Skills and competencies matrix	• Objectivity • Relevancy • Completeness • Currency	Level of required skills and competencies versus actual skills and competencies present in the project organisation
		IT budget allocations	• Accuracy • Completeness • Currency • Appropriate amount	Cost of programmes and new developments versus overall IT cost
			• Accuracy • Completeness • Appropriate amount	Percentage of projects overrunning budget at completion
		Investment return expectations	• Accuracy • Completeness • Currency	Percentage of projects/programmes realising the benefits as defined in the business case
		Risk analysis results	• Accuracy • Objectivity • Relevancy • Completeness • Understandability	Percentage of projects or programmes at high/medium/low risk of failing to meet time, quality, scope and/or budget requirements
ITG14	Availability of reliable and useful information for decision making	SLAs/OLAs	• Objectivity • Reputation • Relevancy • Completeness • Currency • Understandability	Level of business user satisfaction with quality and timeliness (or availability) of management information
			• Accuracy • Objectivity • Relevancy • Completeness • Currency	Percentage of management information not produced according to defined levels in the SLAs/OLAs
		Root causes of quality delivery failures and recommendations	• Accuracy • Objectivity • Relevancy • Completeness	Number of business process incidents caused by non-availability of information
		Risk analysis and risk profile reports for stakeholders	• Accuracy • Objectivity • Relevancy • Completeness • Currency	Ratio and extent of erroneous business decisions where erroneous or unavailable risk information was a key factor
		Incident status and trends report	• Objectivity • Reputation • Completeness • Currency	Satisfaction of business and IT executives with the quality and content of produced trend reports, as support for decision making

Figure 72—Information Items Supporting IT-related Goals (Comprehensive) ***(cont.)***

Generic IT-related Goals		Key Information Items to Support Achievement of the IT-related Goal	Illustrative Quality Criteria	Related Metrics
ITG15	IT compliance with internal policies	Internal policies and frameworks	• Objectivity • Believability • Relevancy • Completeness	Level of stakeholder understanding of internal policies
			• Accuracy • Currency	Frequency of policies review and update
		Emerging risk issues and factors	• Accuracy • Relevancy • Completeness • Currency • Ease of manipulation	Percentage of emerging risk issues and factors addressed in the internal policies
		Results of (third-party) quality/risk assessments	• Accuracy • Relevancy • Completeness	Number of incidents related to non-compliance to policy
			• Accuracy • Objectivity • Completeness • Currency	Percentage of policies supported by effective standards and working practices
ITG16	Competent and motivated IT personnel	Reward systems approach	• Accuracy • Relevancy • Completeness • Currency	Percentage of IT personnel satisfied with their rewards and possible career path
		Skills and competencies matrix	• Objectivity • Completeness	Satisfaction of business and IT executives with the competencies of IT personnel
			• Accuracy • Objectivity • Relevancy • Currency	Percentage of staff whose IT-related skills are sufficient for the competency required for their role
			• Accuracy • Completeness	Number of learning/training hours per staff
		Strategic road map	• Objectivity • Relevancy • Currency	Degree of alignment between recruiting strategy and strategic road map of the organisation
		Quality management system (QMS) roles, responsibilities and decision rights	• Accuracy • Objectivity • Currency	Percentage of IT personnel performing QMS roles and assuming QMS responsibilities

Figure 72—Information Items Supporting IT-related Goals (Comprehensive) ***(cont.)***

Generic IT-related Goals		Key Information Items to Support Achievement of the IT-related Goal	Illustrative Quality Criteria	Related Metrics
ITG17	Knowledge, expertise and initiatives for business innovation	Strategic road map	• Believability • Completeness • Currency • Interpretability • Understandability	Level of business executive awareness and understanding of IT innovation possibilities
		Innovation plan	• Availability • Completeness • Currency • Believability • Relevance	Number of approved initiatives resulting from innovative IT ideas
		Innovation performance reports	• Currency • Objectivity • Reputation	Executive stakeholder satisfaction with levels of IT innovation expertise and ideas present in the organisation