COBIT® 2019
FRAMEWORK

Introduction and Methodology

COBIT® 2019 FRAMEWORK: INTRODUCTION & METHODOLOG

About ISACA

Nearing its 50th year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Technology powers today's world and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISA leverages the expertise of its half-million engaged professionals in information and cyber security, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 217 chapt and offices in both the United States and China.

Disclaimer

ISACA has designed and created *COBIT® 2019 Framework: Introduction and Methodology* (the "Work") primaril as an educational resource for enterprise governance of information and technology (EGIT), 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, enterprise governance of information and technology (EGIT), assurance, risk and security professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

ISACA
1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Phone: +1.847.660.5505
Fax: +1.847.253.1755

In Memoriam: John Lainhart (1946-2018)

Dedicated to John Lainhart, ISACA Board chair 1984-1985. John was instrumental in the creation of the COB framework and most recently served as chair of the working group for COBIT® 2019, which culminated in the creation of this work. Over his four decades with ISACA, John was involved in numerous aspects of the assoc as well as holding ISACA's CISA, CRISC, CISM and CGEIT certifications. John leaves behind a remarkable personal and professional legacy, and his efforts significantly impacted ISACA.

Page intentionally left blank

Acknowledgments

ISACA wishes to recognize:

COBIT Working Group (2017-2018)
John Lainhart, Chair, CISA, CRISC, CISM, CGEIT, CIPP/G, CIPP/US, Grant Thornton, USA
Matt Conboy, Cigna, USA
Ron Saull, CGEIT, CSP, Great-West Lifeco & IGM Financial (retired), Canada

Development Team
Steven De Haes, Ph.D., Antwerp Management School, University of Antwerp, Belgium
Matthias Goorden, PwC, Belgium
Stefanie Grijp, PwC, Belgium
Bart Peeters, PwC, Belgium
Geert Poels, Ph.D., Ghent University, Belgium
Dirk Steuperaert, CISA, CRISC, CGEIT, IT In Balance, Belgium

Expert Reviewers
Sarah Ahmad Abedin, CISA, CRISC, CGEIT, Grant Thornton LLP, USA
Floris Ampe, CISA, CRISC, CGEIT, CIA, ISO27000, PRINCE2, TOGAF, PwC, Belgium
Elisabeth Antonssen, Nordea Bank, Sweden
Krzystof Baczkiewicz, CHAMP, CITAM, CSAM, Transpectit, Poland
Christopher M. Ballister, CRISC, CISM, CGEIT, Grant Thornton, USA
Gary Bannister, CGEIT, CGMA, FCMA, Austria
Graciela Braga, CGEIT, Auditor and Advisor, Argentina
Ricardo Bria, CISA, CRISC, CGEIT, COTO CICSA, Argentina
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore

Acknowledgments *(cont.)*

TABLE OF CONTENTS

LIST OF FIGURES

Page intentionally left blank

Chapter 1
Introduction

1.1 Enterprise Governance of Information and Technology

In the light of digital transformation, information and technology (I&T) have become crucial in the support, sustainability and growth of enterprises. Previously, governing boards (boards of directors) and senior manage could delegate, ignore or avoid I&T-related decisions. In most sectors and industries, such attitudes are now il advised. Stakeholder value creation (i.e., realizing benefits at an optimal resource cost while optimizing risk) i driven by a high degree of digitization in new business models, efficient processes, successful innovation, etc. Digitized enterprises are increasingly dependent on I&T for survival and growth.

Given the centrality of I&T for enterprise risk management and value generation, a specific focus on enterpris governance of information and technology (EGIT) has arisen over the last three decades. EGIT is an integral p corporate governance. It is exercised by the board that oversees the definition and implementation of processe structures and relational mechanisms in the organization that enable both business and IT people to execute th responsibilities in support of business/IT alignment and the creation of business value from I&T-enabled busi investments (**figure 1.1**).

Figure 1.1—The Context of Enterprise Governance of Information and Technology

and within budget, that generate the intended financial and nonfinancial benefits. The value that I&T delivers should be aligned directly with the values on which the business is focused. IT value should also be measured i way that shows the impact and contributions of IT-enabled investments in the value creation process of the enterprise.

- **Risk optimization**—This entails addressing the business risk associated with the use, ownership, operation, involvement, influence and adoption of I&T within an enterprise. I&T-related business risk consists of I&T-rela events that could potentially impact the business. While value delivery focuses on the *creation* of value, risk management focuses on the *preservation* of value. The management of I&T-related risk should be integrated wi the enterprise risk management approach to ensure a focus on IT by the enterprise. It should also be measured i way that shows the impact and contributions of optimizing I&T-related business risk on preserving value.
- **Resource optimization**—This ensures that the appropriate capabilities are in place to execute the strategic plan and sufficient, appropriate and effective resources are provided. Resource optimization ensures that an integrate economical IT infrastructure is provided, new technology is introduced as required by the business, and obsolet systems are updated or replaced. Because it recognizes the importance of people, in addition to hardware and software, it focuses on providing training, promoting retention and ensuring competence of key IT personnel. A important resource is data and information, and exploiting data and information to gain optimal value is another key element of resource optimization.

Strategic alignment and performance measurement are of paramount importance and apply overall to all activities ensure that I&T-related objectives are aligned with the enterprise goals.

In a large case study of an international airline company, EGIT's benefits were demonstrated to include: lower IT-related continuity costs, increased IT-enabled innovation capacity, increased alignment between digital investmen and business goals and strategy, increased trust between business and IT, and a shift toward a "value mindset" aro digital assets.[2]

Research has shown that enterprises with poorly designed or adopted approaches to EGIT perform worse in align business and I&T strategies and processes. As a result, such enterprises are much less likely to achieve their intended business strategies and realize the business value they expect from digital transformation.[3]

1.3.1 What Is COBIT and What Is It Not?

Before describing the updated COBIT framework, it is important to explain what COBIT is and is not:

COBIT is a framework for the governance and management of enterprise information and technology,[4] aimed whole enterprise. Enterprise I&T means all the technology and information processing the enterprise puts in p achieve its goals, regardless of where this happens in the enterprise. In other words, enterprise I&T is not limi the IT department of an organization, but certainly includes it.

The COBIT framework makes a clear distinction between governance and management. These two disciplines encompass different activities, require different organizational structures and serve different purposes.

- **Governance** ensures that:
  - Stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objec
  - Direction is set through prioritization and decision making.
  - Performance and compliance are monitored against agreed-on direction and objectives.

In most enterprises, overall governance is the responsibility of the board of directors, under the leadership of t chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

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

In most enterprises, management is the responsibility of the executive management, under the leadership of th executive officer (CEO).

COBIT defines the components to build and sustain a governance system: processes, organizational structures policies and procedures, information flows, culture and behaviors, skills, and infrastructure.[5]

1.4 Structure of This Publication

The remainder of this publication contains the following chapters:

- Chapter 2 discusses the target audience for COBIT.
- Chapter 3 explains the principles for governance systems for I&T, and the principles for good governance frameworks.
- Chapter 4 explains the basic concepts and terminology of COBIT® 2019, including the updated core COBIT mo with its 40 governance and management objectives.
- Chapter 5 elaborates on the 40 governance and management objectives.
- Chapter 6 explains how performance monitoring in COBIT® 2019 is conceived and, in particular, how Capabili Maturity Model Integration (CMMI®)-inspired capability levels are introduced.
- Chapter 7 contains a brief introduction and overview of the workflow of the *COBIT® 2019 Design Guide*.
- Chapter 8 contains a brief introduction and overview of the *COBIT® 2019 Implementation Guide*.
- Chapter 9 contains a detailed example to illustrate making the case for the adoption and implementation of COI in an enterprise.
- Chapter 10 lists the standards, frameworks and regulations that have been used during the development of COE 2019.

Chapter 2
Intended Audience

2.1 Governance Stakeholders

The target audience for COBIT is the stakeholders for EGIT and, by extension, stakeholders for corporate governance. These stakeholders and the benefits they can gain from COBIT are shown in **figure 2.1**.

Figure 2.1—COBIT Stakeholders

Stakeholder	Benefit of COBIT
Internal Stakeholders	
Boards	Provides insights on how to get value from the use of I&T and expl relevant board responsibilities
Executive Management	Provides guidance on how to organize and monitor performance c across the enterprise
Business Managers	Helps to understand how to obtain the I&T solutions enterprises re and how best to exploit new technology for new strategic opportu
IT Managers	Provides guidance on how best to build and structure the IT depar manage performance of IT, run an efficient and effective IT operati control IT costs, align IT strategy to business priorities, etc.
Assurance Providers	Helps to manage dependency on external service providers, get assurance over IT, and ensure the existence of an effective and eff system of internal controls
Risk Management	Helps to ensure the identification and management of all IT-relatec
External Stakeholders	
Regulators	Helps to ensure the enterprise is compliant with applicable rules a regulations and has the right governance system in place to mana

Page intentionally left blank

Chapter 3
COBIT Principles

3.1 Introduction

COBIT® 2019 was developed based on two sets of principles:

- Principles that describe the core requirements of a **governance system** for enterprise information and techn
- Principles for a **governance framework** that can be used to build a governance system for the enterprise

3.2 Six Principles for a Governance System

The six principles for a governance system are (**figure 3.1**):

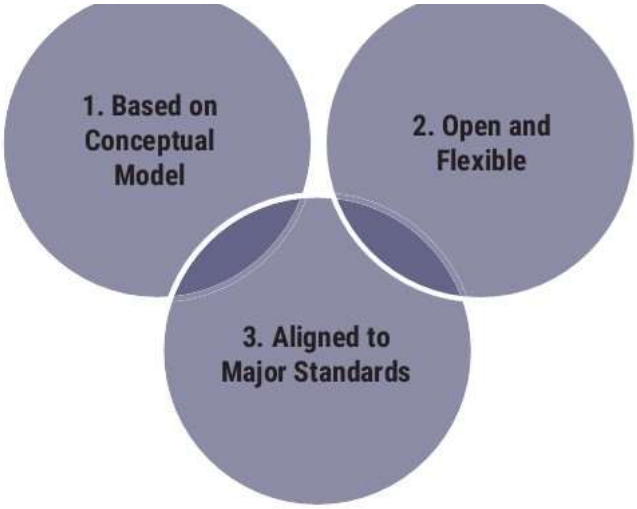
1. Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the us I&T. Value reflects a balance among benefits, risk and resources, and enterprises need an actionable strate governance system to realize this value.
2. A governance system for enterprise I&T is built from a number of components that can be of different typ that work together in a holistic way.
3. A governance system should be dynamic. This means that each time one or more of the design factors are changed (e.g., a change in strategy or technology), the impact of these changes on the EGIT system must considered. A dynamic view of EGIT will lead toward a viable and future-proof EGIT system.
4. A governance system should clearly distinguish between governance and management activities and struc
5. A governance system should be tailored to the enterprise's needs, using a set of design factors as paramet customize and prioritize the governance system components.
6. A governance system should cover the enterprise end to end, focusing not only on the IT function but on a

3.3 Three Principles for a Governance Framework

The three principles for a governance framework are (**figure 3.2**):

1. A governance framework should be based on a conceptual model, identifying the key components and relationships among components, to maximize consistency and allow automation.
2. A governance framework should be open and flexible. It should allow the addition of new content and the ab to address new issues in the most flexible way, while maintaining integrity and consistency.
3. A governance framework should align to relevant major related standards, frameworks and regulations.

Figure 3.2—Governance Framework Principles



Chapter 4
Basic Concepts: Governance System and Components

4.1 COBIT Overview

The COBIT® 2019 product family is open-ended and designed for customization. The following publications a currently available:[7]

- ***COBIT® 2019 Framework: Introduction and Methodology*** introduces the key concepts of COBIT® 2019.
- ***COBIT® 2019 Framework: Governance and Management Objectives*** comprehensively describes the 40 cc governance and management objectives, the processes contained therein, and other related components. Thi also references other standards and frameworks.
- ***COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*** explores d factors that can influence governance and includes a workflow for planning a tailored governance system fo enterprise.
- ***COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*** represents an evolution of the *COBIT® 5 Implementation* guide and develops a road m continuous governance improvement. It may be used in combination with the *COBIT® 2019 Design Guide.*

Figure 4.1 shows the high-level overview of COBIT® 2019 and illustrates how different publications within th cover different aspects.

Figure 4.1—COBIT Overview

The content identified as focus areas in **figure 4.1** will contain more detailed guidance on specific themes.[8]

COBIT® 2019 is based on COBIT® 5 and other authoritative sources. COBIT is aligned to a number of related standards and frameworks. The list of these standards is included in Chapter 10. The analysis of related standards and COBIT's alignment to them underly COBIT's established position of being the umbrella I&T governance framework.

In the future, COBIT will call upon its user community to propose content updates, to be applied as controlled contributions on a continuous basis, to keep COBIT up to date with the latest insights and evolutions.

The following sections explain the key concepts and terms used in COBIT® 2019.

4.2 Governance and Management Objectives

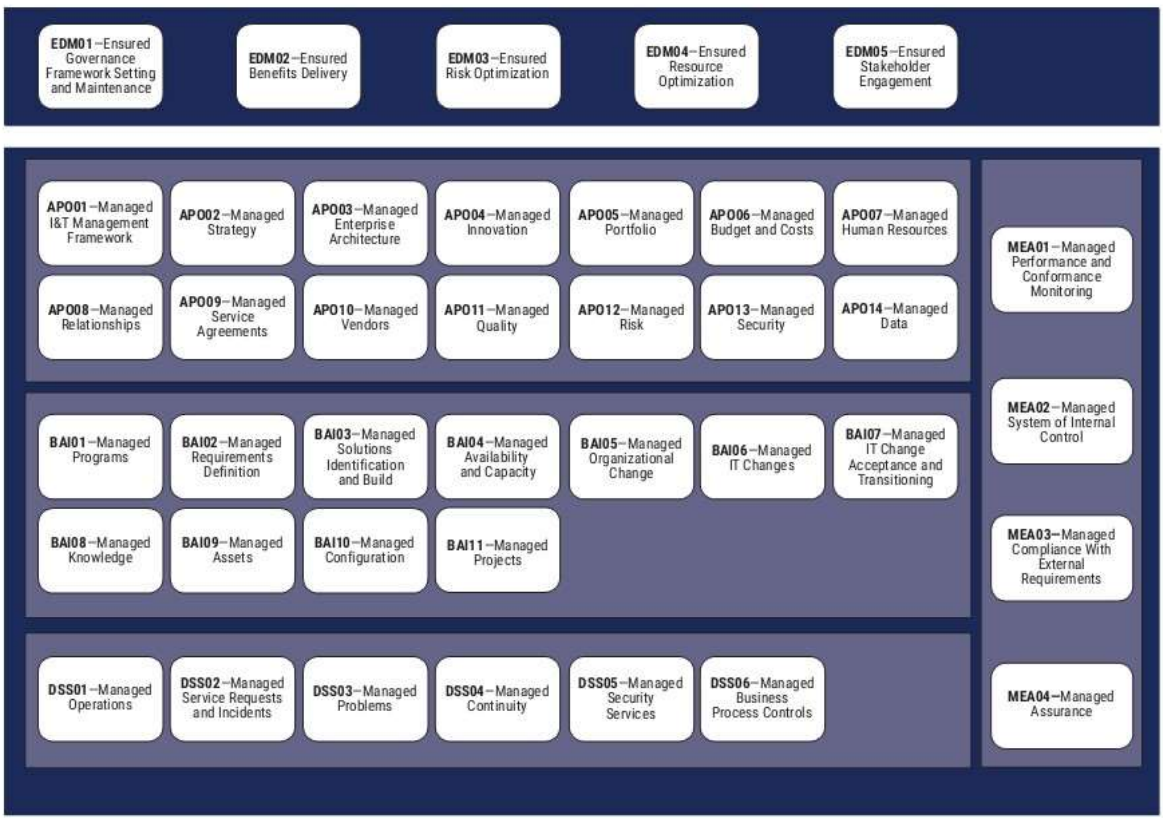
For information and technology to contribute to enterprise goals, a number of governance and management objectives should be achieved. Basic concepts relating to governance and management objectives are:

- A governance or management objective **always relates to one process** (with an identical or similar name) and a series of related components of other types to help achieve the objective.
- A governance objective relates to a governance process (depicted in the dark blue background in **figure 4.2**), wh a management objective relates to a management process (depicted on the lighter blue background in **figure 4.2** Boards and executive management are typically accountable for governance processes, while management processes are the domain of senior and middle management.

The governance and management objectives in COBIT are grouped into five domains. The domains have names w verbs that express the key purpose and areas of activity of the objective contained in them:

- Governance objectives are grouped in the **Evaluate, Direct and Monitor** (EDM) domain. In this domain, the governing body evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy.

Figure 4.2—COBIT Core Model



- **Culture, ethics and behavior** of individuals and of the enterprise are often underestimated as factors in the success of governance and management activities.
- **People, skills and competencies** are required for good decisions, execution of corrective action and successf completion of all activities.
- **Services, infrastructure and applications** include the infrastructure, technology and applications that provic the enterprise with the governance system for I&T processing.

Figure 4.3—COBIT Components of a Governance System

The number of focus areas is virtually unlimited. That is what makes COBIT open-ended. New focus areas ca added as required or as subject matter experts and practitioners contribute to the open-ended COBIT model.

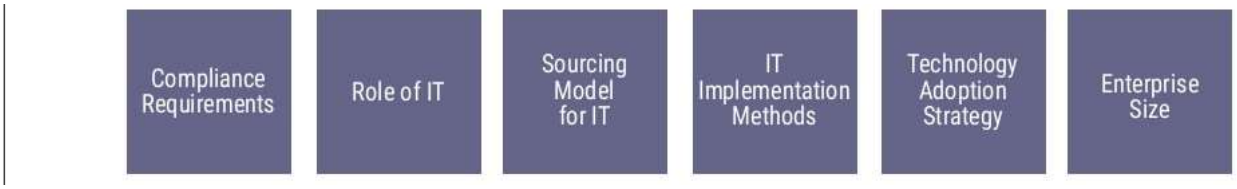
4.5 Design Factors

Design factors are factors that can influence the design of an enterprise's governance system and position it fo success in the use of I&T.

The potential impacts design factors can have on the governance system are noted in section 7.1. More information and detailed guidance on how to use the design factors for designing a governance system can b found in the *COBIT® 2019 Design Guide*.

Design factors include any combination of the following (**figure 4.4**):

Figure 4.4—COBIT Design Factors



2. **Enterprise goals** supporting the enterprise strategy—Enterprise strategy is realized by the achievement of (a s of) enterprise goals. These goals are defined in the COBIT framework, structured along the balanced scorecard (BSC) dimensions, and include the elements shown in **figure 4.6.**

Figure 4.6—Enterprise Goals Design Factor

Reference	Balanced Scorecard (BSC) Dimension	Enterprise Goal
EG01	Financial	Portfolio of competitive products and services
EG02	Financial	Managed business risk
EG03	Financial	Compliance with external laws and regulations
EG04	Financial	Quality of financial information
EG05	Customer	Customer-oriented service culture
EG06	Customer	Business-service continuity and availability
EG07	Customer	Quality of management information
EG08	Internal	Optimization of internal business process functionalit
EG09	Internal	Optimization of business process costs
EG10	Internal	Staff skills, motivation and productivity
EG11	Internal	Compliance with internal policies
EG12	Growth	Managed digital transformation programs
EG13	Growth	Product and business innovation

Section 4.6 includes more information on the COBIT goals cascade, which is the detailed elaboration of this design factor.

3. **Risk profile** of the enterprise and current issues in relation to I&T—The risk profile identifies the sort of I&T-related risk to which the enterprise is currently exposed and indicates which areas of risk are exceeding the risk appetite. The risk categories[14] listed in **figure 4.7** merit consideration.

Figure 4.7—Risk Profile Design Factor (IT Risk Categories)

4. **I&T-related issues**—A related method for an I&T risk assessment for the enterprise is to consider which I& related issues it currently faces, or, in other words, what I&T-related risk has materialized. The most common issues[15] include those in **figure 4.8**.

Figure 4.8—I&T-Related Issues Design Factor

Reference	Description
A	Frustration between different IT entities across the organization because of a perception of low contribution to business value
B	Frustration between business departments (i.e., the IT customer) and the IT department becaus failed initiatives or a perception of low contribution to business value
C	Significant IT-related incidents, such as data loss, security breaches, project failure and applicati errors, linked to IT
D	Service delivery problems by the IT outsourcer(s)
E	Failures to meet IT-related regulatory or contractual requirements
F	Regular audit findings or other assessment reports about poor IT performance or reported IT qu

F	Regular audit findings or other assessment reports about poor IT performance or reported IT qu service problems
G	Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the c of the normal IT investment decision mechanisms and approved budgets
H	Duplications or overlaps between various initiatives, or other forms of wasted resources
I	Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction
J	IT-enabled changes or projects frequently failing to meet business needs and delivered late or ov budget
K	Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT
L	Complex IT operating model and/or unclear decision mechanisms for IT-related decisions
M	Excessively high cost of IT
N	Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems
O	Gap between business and technical knowledge, which leads to business users and information

6. **Compliance requirements**—The compliance requirements to which the enterprise is subject can be classified according to the categories listed in **figure 4.10**.

Figure 4.10—Compliance Requirements Design Factor

Regulatory Environment	Explanation
Low compliance requirements	The enterprise is subject to a minimal set of regular compliance requirements that are lower than average.
Normal compliance requirements	The enterprise is subject to a set of regular compliance requirements t are common across different industries.
High compliance requirements	The enterprise is subject to higher-than-average compliance requirements, most often related to industry sector or geopolitical conditions.

7. **Role of IT**—The role of IT for the enterprise can be classified as indicated in **figure 4.11**.

Figure 4.11—Role of IT Design Factor

Role of IT[17]	Explanation
Support	IT is not crucial for the running and continuity of the business process and services, nor for their innovation.
Factory	When IT fails, there is an immediate impact on the running and contin of the business processes and services. However, IT is not seen as a driver for innovating business processes and services.
Turnaround	IT is seen as a driver for innovating business processes and services. this moment, however, there is not a critical dependency on IT for the current running and continuity of the business processes and service
Strategic	IT is critical for both running and innovating the organization's busine processes and services.

9. **IT implementation methods**—The methods the enterprise adopts can be classified as noted in **figure 4.13**.

Figure 4.13—IT Implementation Methods Design Factor

IT Implementation Method	Explanation
Agile	The enterprise uses Agile development working methods for its software development.

DevOps	The enterprise uses DevOps working methods for software build deployment and operations.
Traditional	The enterprise uses a more classic approach to software develo (waterfall) and separates software development from operations
Hybrid	The enterprise uses a mix of traditional and modern IT implemer often referred to as "bimodal IT."

10. **Technology adoption strategy**—The technology adoption strategy can be classified as listed in **figure 4.1**

Figure 4.14—Technology Adoption Strategy Design Factor

Technology Adoption Strategy	Explanation
First mover	The enterprise generally adopts new technologies as early as po and tries to gain first-mover advantage.
Follower	The enterprise typically waits for new technologies to become mainstream and proven before adopting them.
Slow adopter	The enterprise is very late with adoption of new technologies.

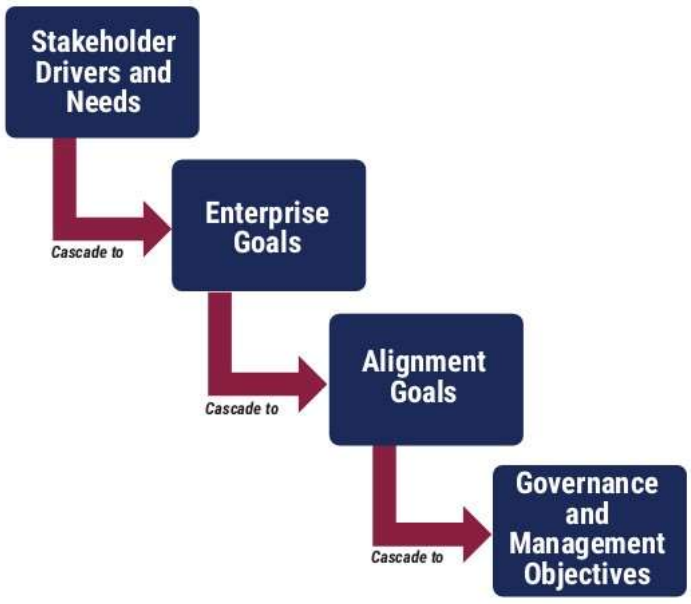
11. **Enterprise size**—Two categories, as shown in **figure 4.15**, are identified for the design of an enterprise's governance system.[18]

Figure 4.15—Enterprise Size Design Factor

4.6 Goals Cascade

Stakeholder needs have to be transformed into an enterprise's actionable strategy. The goals cascade (**figure 4.16**) supports enterprise goals, which is one of the key design factors for a governance system. It supports prioritizatio management objectives based on prioritization of enterprise goals.

Figure 4.16—COBIT Goals Cascade



4.6.1 Enterprise Goals

Stakeholder needs cascade to enterprise goals. **Figure 4.17** shows the set of 13 enterprise goals along with a n of accompanying example metrics.

Figure 4.17—Goals Cascade: Enterprise Goals and Metrics

Reference	BSC Dimension	Enterprise Goal	Example Metrics
EG01	Financial	Portfolio of competitive products and services	• Percent of products and services that meet or exce targets in revenues and/or market share • Percent of products and services that meet or exce customer satisfaction targets • Percent of products and services that provide comp advantage • Time-to-market for new products and services
EG02	Financial	Managed business risk	• Percent of critical business objectives and services covered by risk assessment • Ratio of significant incidents that were not identifie risk assessments vs. total incidents • Appropriate frequency of update of risk profile
EG03	Financial	Compliance with external laws and regulations	• Cost of regulatory noncompliance, including settlen and fines • Number of regulatory noncompliance issues causin public comment or negative publicity • Number of noncompliance matters noted by regula supervisory authorities • Number of regulatory noncompliance issues relatin contractual agreements with business partners
EG04	Financial	Quality of financial information	• Satisfaction survey of key stakeholders regarding th transparency, understanding and accuracy of enterp financial information

Figure 4.17—Goals Cascade: Enterprise Goals and Metrics *(cont.)*

Reference	BSC Dimension	Enterprise Goal	Example Metrics
EG08	Internal	Optimization of internal business process functionality	• Satisfaction levels of board and executive managemen with business process capabilities • Satisfaction levels of customers with service delivery capabilities • Satisfaction levels of suppliers with supply chain capabilities
EG09	Internal	Optimization of business process costs	• Ratio of cost vs. achieved service levels • Satisfaction levels of board and executive managemen with business processing costs
EG10	Internal	Staff skills, motivation and productivity	• Staff productivity compared to benchmarks • Level of stakeholder satisfaction with staff expertise ar skills • Percent of staff whose skills are insufficient relative to competencies required for their roles • Percent of satisfied staff
EG11	Internal	Compliance with internal policies	• Number of incidents related to noncompliance with pol • Percent of stakeholders who understand policies • Percent of policies supported by effective standards ar working practices
EG12	Growth	Managed digital transformation programs	• Number of programs on time and within budget • Percent of stakeholders satisfied with program delivery • Percent of business transformation programs stopped • Percent of business transformation programs with regu reported status updates
EG13	Growth	Product and business	• Level of awareness and understanding of business

		innovation	• Level of awareness and understanding of business innovation opportunities • Stakeholder satisfaction with levels of product and innovation expertise and ideas • Number of approved product and service initiatives resulting from innovative ideas

Figure 4.18—Goals Cascade: Alignment Goals and Metrics *(cont.)*

Reference	IT BSC Dimension	Alignment Goal	Metrics
AG03	Financial	Realized benefits from I&T-enabled investments and services portfolio	• Percent of I&T-enabled investments for which claim benefits in the business case are met or exceeded • Percent of I&T services for which expected benefits stated in the service level agreements) are realized
AG04	Financial	Quality of technology-related financial information	• Satisfaction of key stakeholders regarding the level transparency, understanding and accuracy of IT fina information • Percent of I&T services with defined and approved operational costs and expected benefits
AG05	Customer	Delivery of I&T services in line with business requirements	• Percent of business stakeholders satisfied that IT s delivery meets agreed service levels • Number of business disruptions due to IT service incidents • Percent of users satisfied with the quality of IT serv delivery
AG06	Customer	Agility to turn business requirements into operational solutions	• Level of satisfaction of business executives with IT' responsiveness to new requirements • Average time-to-market for new I&T-related services applications • Average time to turn strategic I&T objectives into ar agreed and approved initiative • Number of critical business processes supported b date infrastructure and applications
AG07	Internal	Security of information, processing infrastructure and applications, and privacy	• Number of confidentiality incidents causing financia business disruption or public embarrassment • Number of availability incidents causing financial lo business disruption or public embarrassment • Number of integrity incidents causing financial loss business disruption or public embarrassment

Figure 4.18—Goals Cascade: Alignment Goals and Metrics *(cont.)*

Reference	IT BSC Dimension	Alignment Goal	Metrics
AG11	Internal	I&T compliance with internal policies	• Number of incidents related to noncompliance with related policies • Number of exceptions to internal policies • Frequency of policy review and update
AG12	Learning and Growth	Competent and motivated staff with mutual understanding of technology and business	• Percent of I&T-savvy business people (i.e., those ha the required knowledge and understanding of I&T to direct, innovate and see opportunities of I&T for the domain of expertise) • Percent of business-savvy IT people (i.e., those havi required knowledge and understanding of relevant business domains to guide, direct, innovate and see opportunities of I&T for the business domain) • Number or percentage of business people with tech management experience
AG13	Learning and	Knowledge, expertise and	• Level of business executive awareness and underst

	Growth	initiatives for business innovation	of I&T innovation possibilities • Number of approved initiatives resulting from innov I&T ideas • Number of innovation champions recognized/awar

Chapter 5
COBIT Governance and Management Objectives

5.1 Purpose

In section 4.2, **figure 4.2**, the COBIT core model was presented, including the 40 governance and managemen objectives. **Figure 5.1** lists all the governance and management objectives, each with its purpose statement. Th purpose statement is a further elaboration—a next level of detail—of each governance and management objec

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose

Reference	Name	Purpose
EDM01	Ensured governance framework setting and maintenance	Provide a consistent approach, integrated and aligned with t enterprise governance approach. I&T-related decisions must made in line with the enterprise's strategies and objectives a desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compl with legal, contractual and regulatory requirements is confir and the governance requirements for board members are m
EDM02	Ensured benefits delivery	Secure optimal value from I&T-enabled initiatives, services a assets; cost-effective delivery of solutions and services; and reliable and accurate picture of costs and likely benefits so t business needs are supported effectively and efficiently.
EDM03	Ensured risk optimization	Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I& to enterprise value is identified and managed, and the poten compliance failures is minimized.
EDM04	Ensured resource optimization	Ensure that the resource needs of the enterprise are met in t optimal manner, I&T costs are optimized, and there is an inc

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose *(cont.)*

Reference	Name	Purpose
APO05	Managed portfolio	Optimize the performance of the overall portfolio of programs in response to individual program, product and service performanc and changing enterprise priorities and demand.
APO06	Managed budget and costs	Foster a partnership between IT and enterprise stakeholders to enable the effective and efficient use of I&T-related resources an provide transparency and accountability of the cost and busines

		value of solutions and services. Enable the enterprise to make informed decisions regarding the use of I&T solutions and services.
APO07	Managed human resources	Optimize human-resources capabilities to meet enterprise objectives.
APO08	Managed relationships	Enable the right knowledge, skills and behaviors to create improved outcomes, increased confidence, mutual trust and effective use of resources that stimulate a productive relationsh with business stakeholders.
APO09	Managed service agreements	Ensure that I&T products, services and service levels meet curre and future enterprise needs.
APO10	Managed vendors	Optimize available I&T capabilities to support the I&T strategy a road map, minimize the risk associated with nonperforming or noncompliant vendors, and ensure competitive pricing.
APO11	Managed quality	Ensure consistent delivery of technology solutions and services meet the quality requirements of the enterprise and satisfy stakeholder needs.
APO12	Managed risk	Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the cost and benefits of managing I&T-related enterprise risk.
APO13	Managed security	Keep the impact and occurrence of information security inciden within the enterprise's risk appetite levels.
APO14	Managed data	Ensure effective utilization of the critical data assets to achieve

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose *(con*

Reference	Name	Purpose
BAI08	Managed knowledge	Provide the knowledge and management information requir support all staff in the governance and management of ente I&T and allow for informed decision making.
BAI09	Managed assets	Account for all I&T assets and optimize the value provided b use.
BAI10	Managed configuration	Provide sufficient information about service assets to enabl service to be effectively managed. Assess the impact of cha and deal with service incidents.
BAI11	Managed projects	Realize defined project outcomes and reduce the risk of unexpected delays, costs and value erosion by improving communications to and involvement of business and end us Ensure the value and quality of project deliverables and max their contribution to the defined programs and investment portfolio.
DSS01	Managed operations	Deliver I&T operational product and service outcomes as pla
DSS02	Managed service requests and incidents	Achieve increased productivity and minimize disruptions thr quick resolution of user queries and incidents. Assess the ir of changes and deal with service incidents. Resolve user rec and restore service in response to incidents.
DSS03	Managed problems	Increase availability, improve service levels, reduce costs, im customer convenience and satisfaction by reducing the num operational problems, and identify root causes as part of pro resolution.
DSS04	Managed continuity	Adapt rapidly, continue business operations, and maintain availability of resources and information at a level acceptab the enterprise in the event of a significant disruption (e.g., th opportunities, demands).
DSS05	Managed security services	Minimize the business impact of operational information se vulnerabilities and incidents.

Page intentionally left blank

CHAPTI
PERFORMANCE MANAGEMENT IN CO

Chapter 6
Performance Management in COBIT

6.1 Definition

Performance management is an essential part of a governance and management system. "Performance manage represents a general term for all activities and methods. It expresses how well the governance and managemen system and all the components of an enterprise work, and how they can be improved to achieve the required le includes concepts and methods such as capability levels and maturity levels. COBIT uses the term COBIT performance management (CPM) to describe these activities, and the concept is an integral part of the COBIT framework.

6.2 COBIT Performance Management Principles

COBIT® 2019 is based on the following principles:

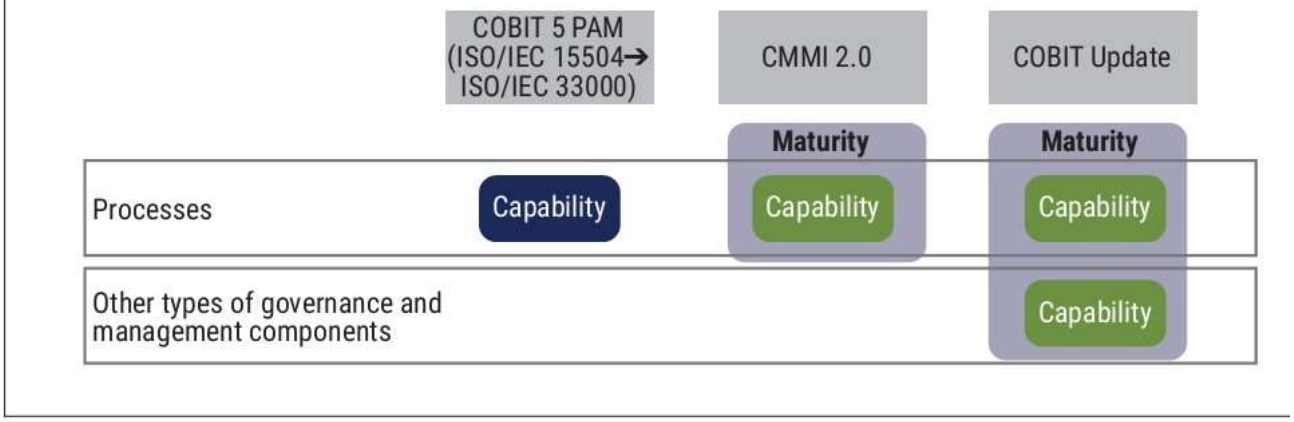
1. The CPM should be simple to understand and use.
2. The CPM should be consistent with, and support, the COBIT conceptual model. It should enable manager the performance of all types of components of the governance system; it must be possible to manage the performance of processes as well as the performance of other types of components (e.g., organizational structures or information), if users wish to do so.
3. The CPM should provide reliable, repeatable and relevant results.
4. The CPM must be flexible, so it can support the requirements of different organizations with different pric and needs.

and needs.

5. The CPM should support different types of assessment, from self-assessments to formal appraisals or aud

COBIT® 2019 FRAMEWORK: INTRODUCTION & METHODOLOG

Figure 6.1—Capability Levels



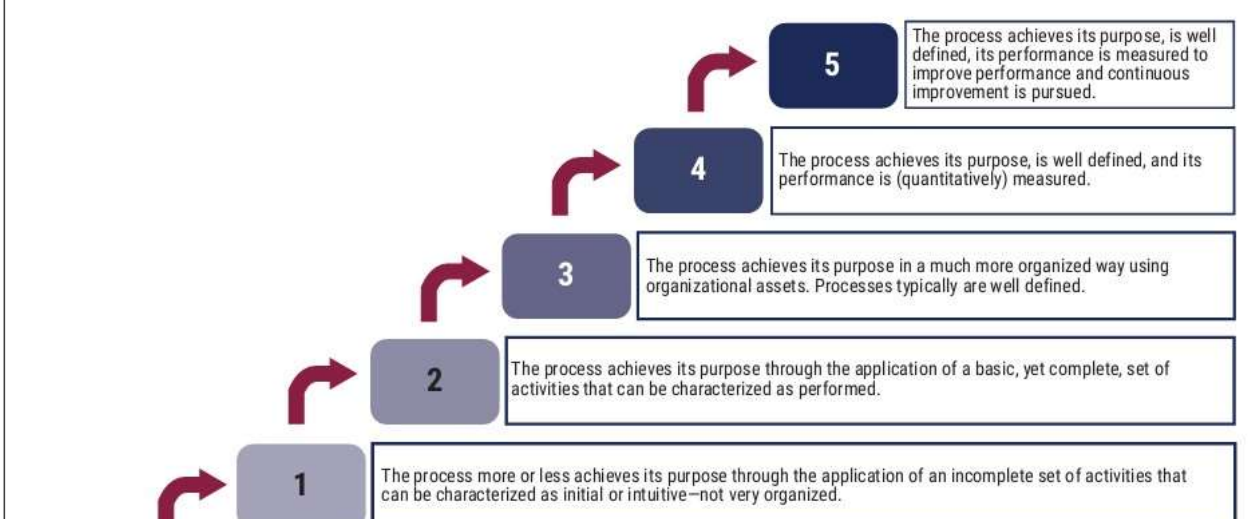
If enterprises desire to continue using the COBIT 5 process capability model based on International Organization Standardization (ISO)/International Electrotechnical Commission (IEC) 15504 (now ISO/IEC 33000, in which capability levels have very different meanings), they have all required information to do so in *COBIT® 2019 Framework: Governance and Management Objectives*. No separate process assessment model (PAM) publication are necessary, nor will they be provided with COBIT® 2019.

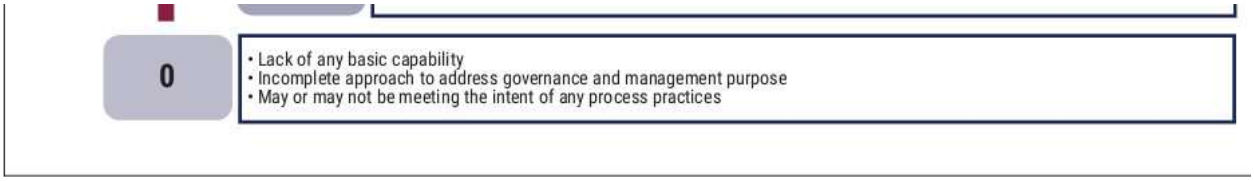
In COBIT® 2019, the explicit process outcomes or process goals are replaced by the process practices themselves This results in the following situation for an ISO/IEC33000 evaluation:

1. Process outcomes are now linked to the process practices on a one-to-one basis (i.e., the process outcomes ar the successful completion of the process practices). Note: the process practices are formulated as practices, a the outcomes can be derived from there. Example: APO01.01 *Design the management system for enterprise* has as process outcome APO01.01: *A management system for enterprise I&T is designed.*

CHAPTI PERFORMANCE MANAGEMENT IN CO

Figure 6.2—Capability Levels for Processes



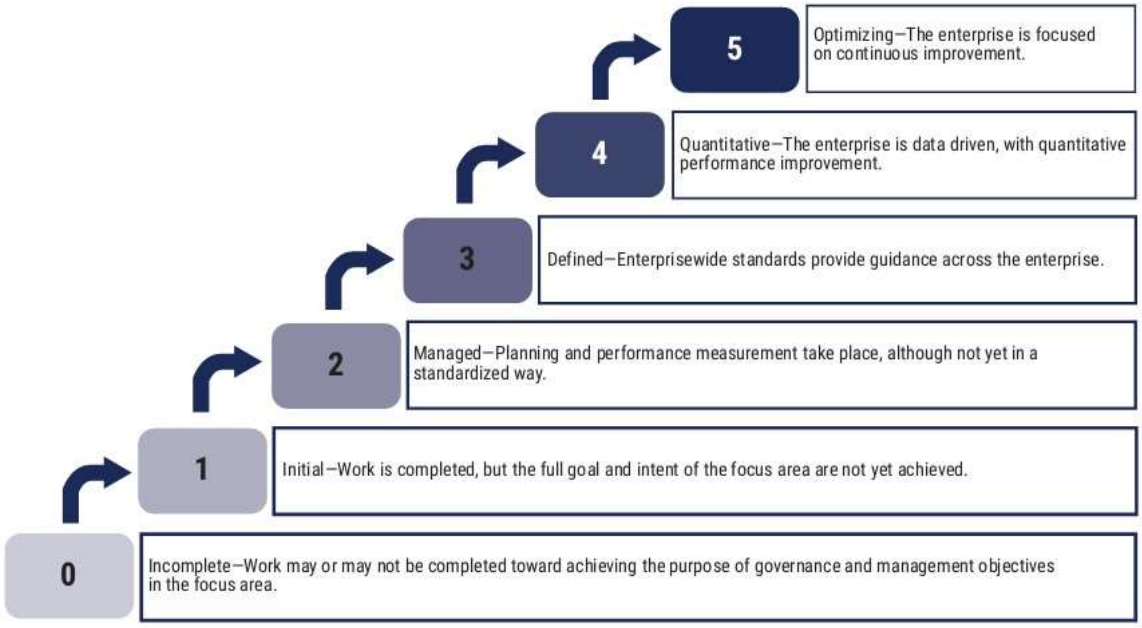


The COBIT core model assigns capability levels to all process activities, enabling clear definition of the proce and required activities for achieving the different capability levels. See *COBIT® 2019 Framework: Governanc Management Objectives* for more detail.

6.4.2 Rating Process Activities

COBIT® 2019 FRAMEWORK: INTRODUCTION & METHODOLOG

Figure 6.3—Maturity Levels for Focus Areas



Maturity levels are associated with focus areas (i.e., a collection of governance and management objectives and underlying components) and a certain maturity level is achieved if all the processes contained in the focus area achieve that particular capability level.

6.5 Managing Performance of Other Governance System Components

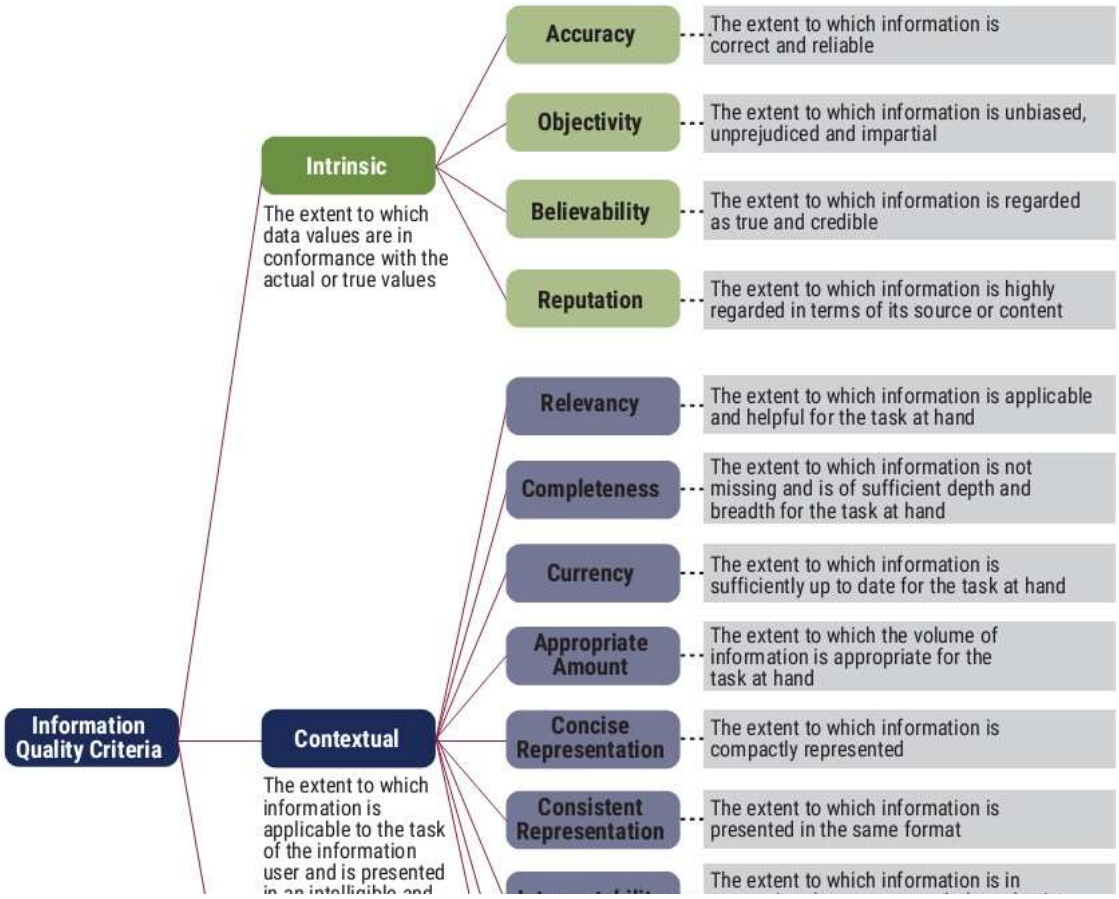
CHAPTI
PERFORMANCE MANAGEMENT IN CO

- Span of control
  - The organizational structure has a clear, documented and well-understood mandate.
  - Operating principles are documented.
  - Regular meetings take place as defined in the operating principles.
  - Meeting reports/minutes are available and are meaningful.
- Level of authority and decision rights
  - Decision rights of the organizational structure are defined and documented.

- Decision rights of the organizational structure are respected and complied with (also a culture/behavior
- Delegation of authority
  - Delegation of authority is implemented in a meaningful way.
- Escalation procedures
  - Escalation procedures are defined and applied.

- Successful application of a number of organizational structure management practices (nonfunctional practic arising from an organizational structure point of view):
  - Objectives for the performance of the organizational structures are identified.
  - Performance of the organizational structure is planned and monitored.
  - Performance of the organizational structure is adjusted to meet plans.
  - Resources and information necessary for the organizational structure are identified, made available, alloca and used.
  - Interfaces between the organizational structure and other stakeholders are managed to ensure both effectiv communication and clear assignment of responsibility.
  - Regular evaluations result in the required continuous improvement of the organizational structure—in its composition, mandate or any other parameter.

Figure 6.4—Information Reference Model: Quality Criteria for Information



6.5.3 Performance Management of Culture and Behavior

For the culture and behavior governance component, it should be possible to define a set of desirable (and/or undesirable) behaviors for good governance and management of IT, and to assign different levels of capability each.

COBIT® 2019 Framework: Governance and Management Objectives defines aspects of the culture and behavi component for most objectives. From there, it is possible to assess the extent to which these conditions or beh are met.

Focus area content, which will contain a more detailed set of desired behaviors, will be developed going forw The user is advised to consult *isaca.org/cobit* for the latest status and available focus area guidance.

Page intentionally left blank

Chapter 7
Designing a Tailored Governance System

7.1 Impact of Design Factors

This section provides a high-level overview of the potential impact of design factors on a governance system for ent I&T. It also describes, at a high level, a workflow for designing a tailored governance system for the enterprise. Mo information on these subjects can be found in the *COBIT® 2019 Design Guide*.

Design factors influence in different ways the tailoring of the governance system of an enterprise. This publication distinguishes three different types of impact, illustrated in **figure 7.1**.

Figure 7.1—Impact of Design Factors on a Governance and Management System

Example: When an enterprise identifies the most relevant enterprise goal(s) from the enterprise goal list and applies t goals cascade, this will lead to a selection of priority management objectives. For example, when EG01 *Portfolio of competitive products and services* is ranked as very high by an enterprise, this will make management objective APO *Managed portfolio* an important part of this enterprise's governance system.

Example: An enterprise that is very risk averse will give more priority to management objectives that aspire to gover and manage risk and security. Governance and management objectives EDM03 *Ensured risk optimization*, APO12 *Managed risk,* APO13 *Managed security* and DSS05 *Managed security services* will become important parts of that enterprise's governance system and will have higher target capability levels defined for them.

Example: An enterprise operating within a high threat landscape will require highly capable security-related processe APO13 *Managed security* and DSS05 *Managed security services.*

Example: An enterprise in which the role of IT is strategic and crucial to the success of the business will require high involvement of IT-related roles in organizational structures, a thorough understanding of business by IT professionals (and vice versa), and a focus on strategic processes such as APO02 *Managed strategy* and APO08 *Managed relationships.*

2. **Components variation**—Components are required to achieve governance and management objectives. Some desi factors can influence the importance of one or more components or can require specific variations.

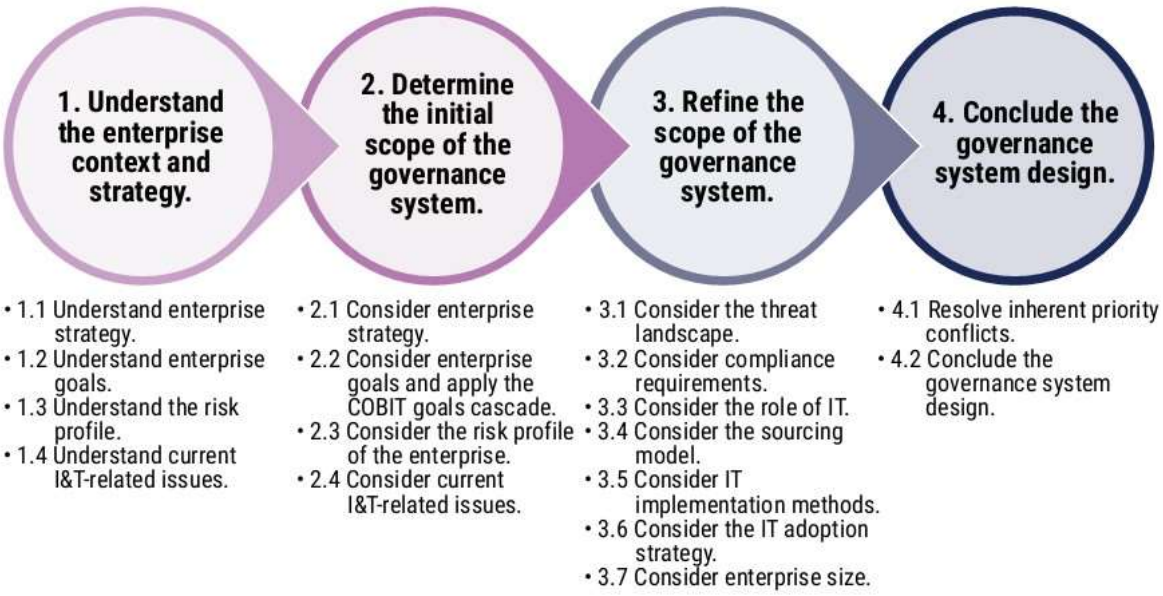
Example: Small and medium-sized enterprises might not need the full set of roles and organizational structures as laid out in the COBIT core model, but may use a reduced set instead. This reduced set of governance and management objectives and the included components is defined in the Small and Medium Enterprise focus area.[22]

Example: An enterprise which operates in a highly regulated environment will attribute more importance to *documented work products and policies and procedures* and to some roles, e.g. the compliance officer function.

7.2 Stages and Steps in the Design Process

Figure 7.2 illustrates the proposed flow for designing a tailored governance system.

Figure 7.2—Governance System Design Workflow



The different stages and steps in the design process, as illustrated in **figure 7.2**, will result in recommendations for

Page intentionally left blank

Chapter 8
Implementing Enterprise Governance of IT

8.1 COBIT Implementation Guide Purpose

The *COBIT® 2019 Implementation Guide* emphasizes an enterprisewide view of governance of I&T. This guic recognizes that I&T are pervasive in enterprises and that it is neither possible nor good practice to separate bu and IT-related activities. The governance and management of enterprise I&T should, therefore, be implemente integral part of enterprise governance, covering the full end-to-end business and IT functional areas of respons

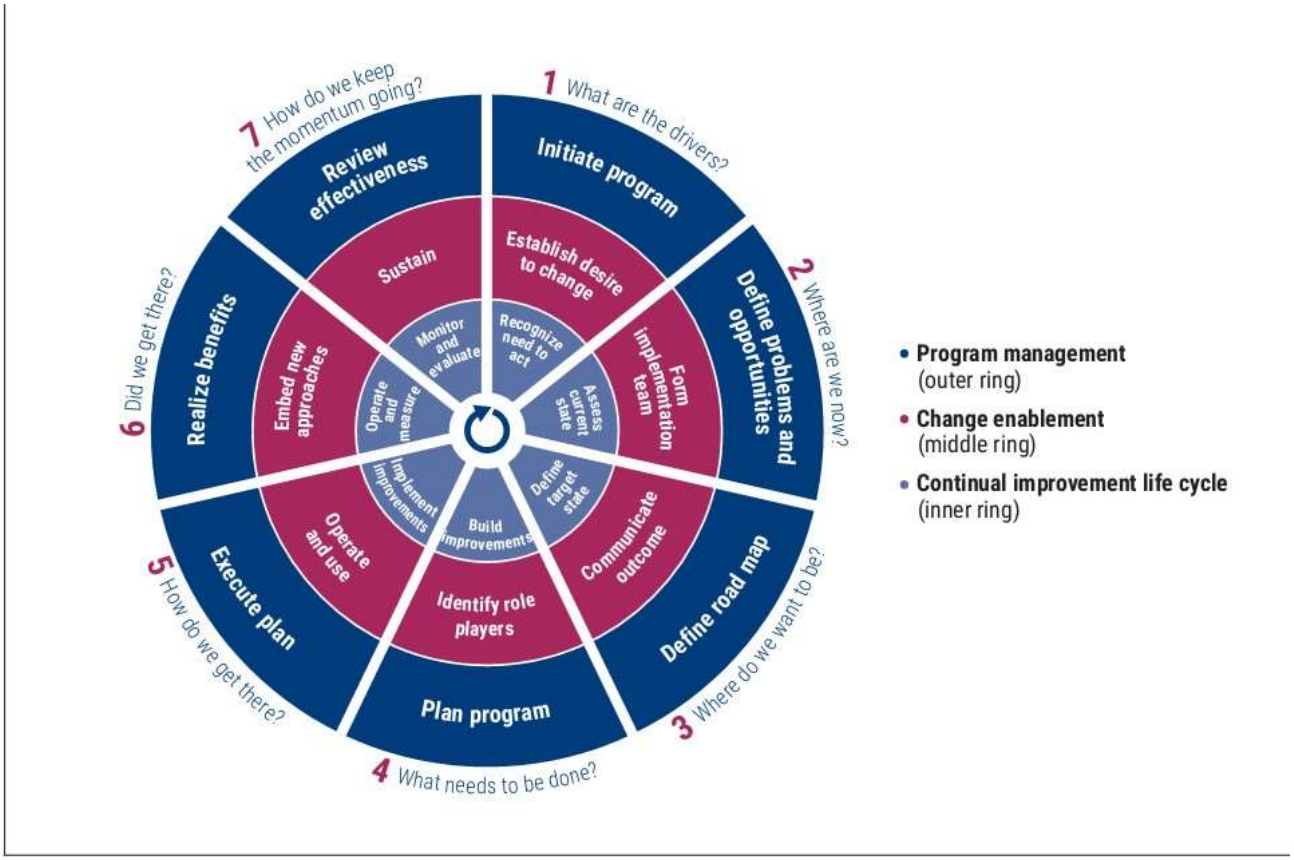
One of the common reasons why some governance system implementations fail is that they are not initiated ar managed properly as programs to ensure that benefits are realized. Governance programs need to be sponsored executive management, be properly scoped and define objectives that are attainable. This enables the enterpris absorb the pace of change as planned. Program management is, therefore, addressed as an integral part of the implementation life cycle.

It is also assumed that while a program and project approach is recommended to effectively drive improvemer initiatives, the goal is also to establish a normal business practice and sustainable approach to governing and managing enterprise I&T just like any other aspect of enterprise governance. For this reason, the implementati approach is based on empowering business and IT stakeholders and role players to take ownership of IT-relate governance and management decisions and activities by facilitating and enabling change. The implementation program is closed when the process for focusing on IT-related priorities and governance improvement is gener measurable benefit, and the program has become embedded in ongoing business activity.

More information on these subjects can also be found in the *COBIT® 2019 Implementation Guide*.

8.2 COBIT Implementation Approach

Figure 8.1—COBIT Implementation Road Map



8.2.1 Phase 1—What Are the Drivers?

8.2.3 Phase 3—Where Do We Want to Be?

Phase 3 sets a target for improvement followed by a gap analysis to identify potential solutions.

Some solutions will be quick wins and others more challenging, long-term tasks. Priority should be given to p that are easier to achieve and likely to give the greatest benefit. Longer-term tasks should be broken down into manageable pieces.

8.2.4 Phase 4—What Needs to Be Done?

Phase 4 describes how to plan feasible and practical solutions by defining projects supported by justifiable bus cases and a change plan for implementation. A well-developed business case can help ensure that the project's benefits are identified and continually monitored.

8.2.5 Phase 5—How Do We Get There?

Phase 5 provides for implementing the proposed solutions via day-to-day practices and establishing measures monitoring systems to ensure that business alignment is achieved, and performance can be measured.

Success requires engagement, awareness and communication, understanding and commitment of top manager and ownership by the affected business and IT process owners.

8.2.6 Phase 6—Did We Get There?

Phase 6 focuses on sustainable transition of the improved governance and management practices into normal business operations. It further focuses on monitoring achievement of the improvements using the performance

metrics and expected benefits.

8.3 Relationship Between *COBIT® 2019 Design Guide* and *COBIT® 2019 Implementation Guide*

The workflow explained in the *COBIT® 2019 Design Guide* has the following connection points with the *COBIT® 2019 Implementation Guide*. The *COBIT® 2019 Design Guide* elaborates a set of tasks defined in the *COBIT® 2019 Implementation Guide*. **Figure 8.2** gives a high-level overview of these connection points. More detailed informa can be found in the *COBIT® 2019 Design Guide*.

Figure 8.2—Connection Points Between *COBIT Design Guide* and *COBIT Implementation Guide*

COBIT Implementation Guide		*COBIT Design Guide*
Phase 1—What are the drivers? (Continuous improvement [CI] tasks)	→	**Step 1**—Understand the enterprise context and strategy
Phase 2—Where are we now? (CI tasks)	→	**Step 2**—Determine the initial scope of the governance system. **Step 3**—Refine the scope of the governance system. **Step 4**—Conclude the governance system design.
Phase 3—Where do we want to be? (CI tasks)	→	**Step 4**—Conclude the governance system design.

Chapter 9
Getting Started With COBIT: Making the Case

9.1 Business Case

Common business practice dictates preparing a business case to analyze and justify the initiation of a large pro and/or financial investment. This example is provided as a nonprescriptive, generic guide to encourage prepar a business case to justify investment in an EGIT implementation program. Every enterprise has its own reason improving EGIT and its own approach to preparing business cases. This can range from a detailed approach w emphasis on quantified benefits to a more high-level and qualitative perspective. Enterprises should follow ex internal business case and investment justification approaches, if they exist. This example and the guidance in publication in provided to help focus on the issues that should be addressed in a business case.

The example scenario is Acme Corporation, a large multinational enterprise with a mixture of traditional, well-established business units as well as new Internet-based businesses adopting the very latest technolog Many of the business units have been acquired and exist in various countries with different local political, cultural and economic environments. The central group's executive management team has been influenced the latest enterprise governance guidance, including COBIT, which they have used centrally for some time

They want to make sure that rapid expansion and adoption of advanced IT will deliver the value expected; they also intend to manage significant new risk. They have, therefore, mandated enterprisewide adoption o uniform EGIT approach. This approach includes involvement by the audit and risk functions and internal annual reporting by business unit management of the adequacy of controls in all entities.

Although the example is derived from actual situations, it does not reflect a specific, existing enterprise.

9.2 Executive Summary

facilitated workshop approach by the members of the EGIT program. The objectives will start with the strategy a enterprise goals of each unit, as well as the IT-related business risk scenarios that apply to the specific business u

The objective of the EGIT program is to ensure that an adequate governance system, including governance structures, is in place and to increase the level of capability and adequacy of the relevant IT processes. The expectation is that as the capability of an IT process increases, so too will its efficiencies and quality. Simultaneou the associated risk will proportionally decrease. In this way, real business benefits can be realized by each busines unit.

Once the process of assessing the capability level within each business unit has been established, it is anticipated self-assessments will continue within each business unit as normal business practice.

The EGIT program will be delivered in two distinct phases. The first phase is a development phase, in which the team will develop and test the approach and tool set that will be used across the Acme Corporation. At the end of phase 1, the results will be presented to group management for final approval. Once the final approval has been obtained, in the form of an approved business case, the EGIT program will be rolled out across the entity in the agreed manner (implementation, phase 2).

It must be noted that it is not the responsibility of the EGIT program to implement the remedial actions identified each business unit. The EGIT program will merely consolidate and report progress as supplied by each unit.

The final challenge that will need to be met by the EGIT program is that of reporting the results in a sustainable manner going forward. This aspect will take time and a significant amount of discussion and development. This discussion and development should result in an enhancement to the existing corporate reporting mechanisms and scorecards.

An initial budget for the development phase of the EGIT program has been prepared. The budget is detailed in a separate schedule. A detailed budget will also be completed for phase 2 of the project and submitted for approval group management.

IT-related business risk will be reported on and discussed as part of the risk management process in the risk re presented to the relevant risk committee.

9.4 Business Challenges

Due to the pervasive nature of IT and the pace of technology change, a reliable framework is required to adeq control the full IT environment and avoid control gaps that may expose the enterprise to unacceptable risk.

The intention is not to impede the IT operations of the various operating entities. Instead, it is to improve the r profile of the entities in a manner that makes business sense and provides increased quality of service and efficiencies, while explicitly achieving compliance not only with the Acme Corporation's group EGIT charter,

also with any other legislative, regulatory and/or contractual requirements.

Some examples of likely pain points include:[25]

- Complicated IT assurance efforts due to the entrepreneurial nature of many of the business units
- Complex IT operating models due to the Internet service-based business models in use
- Geographically dispersed entities made up of diverse cultures and languages
- The decentralized/federated and largely autonomous business control model employed within the group
- Implementation of reasonable levels of IT management, given a highly technical and, at times, volatile IT workforce
- IT's balancing of the enterprise's drive for innovation capabilities and business agility with the need to mana and have adequate control
- The setting of risk and tolerance levels for each business unit
- An increasing need to focus on meeting regulatory (privacy) and contractual (Payment Card Industry [PCI]) compliance requirements
- Regular audit findings about poor IT controls and reported problems related to IT quality of service

9.4.2 Alternatives Considered

Many IT frameworks exist, each intended to control specific aspects of IT. The COBIT framework is regarded by many as the world's leading EGIT and control framework. It has already been implemented by some subsidiaries Acme Corporation.

COBIT was chosen by Acme as the preferred framework for EGIT implementation and should, therefore, be adop by all subsidiaries.

COBIT does not have to be implemented in its entirety; only those areas relevant to the specific subsidiary or business unit need to be implemented, taking into account the following:

1. The development stage of each entity in the business life cycle
2. The business objectives of each entity
3. The importance of IT for the business unit
4. The IT-related business risk faced by each entity
5. Legal and contractual requirements
6. Any other pertinent reasons

If a specific subsidiary or business unit has already implemented another framework, or an implementation is planned in the future, the implementation should be mapped to COBIT for reasons of reporting, audit and clarity internal control.

9.5 Proposed Solution

The EGIT program is being planned in two distinct phases.

12. The final business case and approach are presented, including a roll-out plan to Acme Corporation executi management for approval.

9.5.2 Phase 2. Program Implementation

The EGIT program is designed to start an ongoing program of continual improvement, based on a facilitated, iterative life cycle by following these steps:

1. Determine the drivers for improving EGIT, from both an Acme Corporation group perspective and at the business unit level.
2. Determine the current status of EGIT.
3. Determine the desired state of EGIT (both short- and long-term).
4. Determine what needs to be implemented at the business unit level to enable local business objectives, an thereby align with group expectations.
5. Implement the identified and agreed improvement projects at the local business unit level.
6. Realize and monitor the benefits.
7. Sustain the new way of working by keeping the momentum going.

9.5.3 Program Scope

The EGIT program will cover:

1. All of the group entities. However, the entities will be prioritized for interaction due to limited program resources.
2. The method of prioritization. It will need to be agreed with Acme Corporation management, but could be on the following basis:
   a. Size of investment

The business and IT objectives, as well as the IT-related business risk, are then combined in a tool (based on COE guidance) that will provide a set of focus areas within the COBIT processes for consideration by the business unit this fashion, the business unit can prioritize its remediation efforts to address the areas of IT risk.

9.5.5 Program Deliverables

As mentioned earlier, an overall goal of the EGIT program is to embed the good practices of EGIT into the continuing operations of the various group entities.

Specific outcomes will be produced by the EGIT program to enable Acme Corporation to gauge the delivery of th intended outcomes. These include the following:

1. The EGIT program will facilitate internal knowledge sharing via the intranet platform and leverage existing relationships with vendors to the advantage of the individual business units.
2. Detailed reports on each facilitation with the business units will be created derived from the EGIT program assessment tool. The reports will include:
   a. The current prioritized business objectives, and consequent IT objectives, based on COBIT
   b. The IT-related risk identified by the business unit in a standardized format, and the agreed focus areas fo attention by the business unit based on COBIT processes and practices and other recommended compone
3. Overall progress reports on the intended coverage of the Acme Corporation business units by the EGIT progr will be created.
4. Consolidated group reporting will cover:
   a. Progress from business units engaged with their agreed implementation projects based on monitoring agı performance metrics
   b. Consolidated IT risk view across the Acme Corporation entities
   c. Specific requirements of the risk committee(s)
5. Financial reporting on the program budget vs. actual amount spent will be generated

9.5.7 Stakeholders

The following have been identified as stakeholders in the outcome of the EGIT program:

1. Risk committee
2. IT executive committee
3. Governance team
4. Compliance staff
5. Regional management
6. Local entity-level executive management (including IT management)
7. Internal audit services

A final structure containing the individual names of stakeholders will be compiled and published after consult with group management.

The EGIT program needs the identified stakeholders to provide the following:

1. Guidance as to the overall direction of the EGIT program. This includes decisions on significant governar related topics defined in a group RACI chart according to COBIT guidance. It further includes setting pric agreeing on funding and approving value objectives.
2. Acceptance of the deliverables and monitoring the expected benefits of the EGIT program

9.5.8 Cost-Benefit Analysis

The program should identify the expected benefits and monitor to ensure that real business value is being gene from the investment. Local management should motivate and sustain the program. Sound EGIT should result benefits that will be set as specific targets for each business unit and monitored and measured during impleme to ensure that they are realized. The benefits include:

9.5.9 Challenges and Success Factors

Figure 9.1 summarizes the challenges that could affect the EGIT program during the implementation period of th program and the critical success factors that should be addressed to ensure a successful outcome.

Figure 9.1—Challenges and Planned Actions for Acme Corporation

Challenge	Critical Success Factor—Actions Planned
Inability to gain and sustain support for improvement objectives	• Mitigate through committee structures within the group (to be agree and constituted).
Communication gap between IT and the business	• Involve all stakeholders.
Cost of improvements outweighing perceived benefits	• Focus on benefit identification.
Lack of trust and good relationships between IT and the enterprise	• Foster open and transparent communication about performance, w links to corporate performance management. • Focus on business interfaces and service mentality. • Publish positive outcomes and lessons learned to help establish an maintain credibility. • Ensure the CIO maintains credibility and leadership in building trust and relations. • Formalize governance roles and responsibilities in the business so accountability for decisions is clear.

	accountability for decisions is clear. • Identify and communicate evidence of real issues, risk that needs to avoided and benefits to be gained (in business terms) relating to proposed improvements. • Focus on change enablement planning.
Lack of understanding of the Acme environment by those responsible for the EGIT program	• Apply a consistent assessment methodology.
Various levels of complexity (technical, organizational, operating model)	• Treat the entities on a case-by-case basis. Benefit from lessons learned and sharing knowledge.
Understanding of EGIT frameworks, procedures	• Train and mentor

Figure 9.1—Challenges and Planned Actions for Acme Corporation *(cont.)*

Challenge	Critical Success Factor—Actions Planned
Absence of required IT skills and competencies, such as understanding of the business, processes, soft skills	• Focus on change enablement planning: ▪ Development ▪ Training ▪ Coaching ▪ Mentoring ▪ Feedback into recruitment process ▪ Cross-training
Improvements not adopted or applied	• Use a case-by-case approach with agreed principles for the loca It must be practical to implement.
Benefits difficult to show or prove	• Identify performance metrics.
Loss of interest and momentum	• Build group-level commitment, including communication.

Page intentionally left blank

Chapter 10
COBIT and Other Standards

10.1 Guiding Principle

One of the guiding principles applied throughout the development of COBIT® 2019 was to maintain the positi of COBIT as an umbrella framework. This means that COBIT continues to align with a number of relevant standards, frameworks and/or regulations.

In this context, alignment means that COBIT does not contradict any guidance in the related standards. At the time, it is important to remember that COBIT does not copy the contents of these related standards. Instead, it usually provides equivalent statements or references to related guidance.

10.2 List of Referenced Standards

Standards and guidance used during the development of the COBIT® 2019 update include:

- CIS® Center for Internet Security®, *The CIS Critical Security Controls for Effective Cyber Defense,* Version August 2016
- Cloud standards and good practices:
  - Amazon Web Services (AWS®)
  - *Security Considerations for Cloud Computing*, ISACA
  - *Controls and Assurance in the Cloud: Using COBIT® 5*, ISACA
- CMMI® Cybermaturity Platform, 2018
- CMMI® Data Management Maturity (DMM)℠ model, 2014
- CMMI® Development V2.0, CMMI Institute, USA, 2018

- US National Institute of Standards and Technology (NIST) standards:
  - *Framework for Improving Critical Infrastructure Cybersecurity* V1.1, April 2018
  - Special Publication 800-37, Revision 2 (Draft), May 2018
  - Special Publication 800-53, Revision 5 (Draft), August 2017

- Special Publication 800-53, Revision 5 (Draft), August 2017
- "Options for Transforming the IT Function Using Bimodal IT," *MIS Quarterly Executive* (white paper)
- *A Guide to the Project Management Body of Knowledge: PMBOK® Guide, Sixth Edition*, 2017
- PROSCI® 3-Phase Change Management Process
- Scaled Agile Framework for Lean Enterprises (SAFe®)
- Skills Framework for the Information Age (SFIA®) V6, 2015
- The Open Group IT4IT™ Reference Architecture, version 2.0
- The Open Group Standard TOGAF® version 9.2, 2018
- The TBM Taxonomy, The TBM Council