

Course Book

COMPLIANCE

RULES

LAW

REGULATIONS

STANDARDS

IT GOVERNANCE AND COMPLIANCE

DLMBITGSM02

iu

INTERNATIONAL
UNIVERSITY OF
APPLIED SCIENCES

IT GOVERNANCE AND COMPLIANCE

MASTHEAD

Publisher:
IU Internationale Hochschule GmbH
IU International University of Applied Sciences
Juri-Gagarin-Ring 152
D-99084 Erfurt

Mailing address:
Albert-Proeller-Straße 15-19
D-86675 Buchdorf
media@iu.org
www.iu.de

DLMBITGSM02
Version No.: 001-2024-0126

N. N.

© 2024 IU Internationale Hochschule GmbH
This course book is protected by copyright. All rights reserved.
This course book may not be reproduced and/or electronically edited, duplicated, or distributed in any kind of form without written permission by the IU Internationale Hochschule GmbH (hereinafter referred to as IU).
The authors/publishers have identified the authors and sources of all graphics to the best of their abilities. However, if any erroneous information has been provided, please notify us accordingly.

TABLE OF CONTENTS

IT GOVERNANCE AND COMPLIANCE

Introduction

Signposts Throughout the Course Book	6
Basic Reading	7
Required Reading	8
Further Reading	9
Learning Objectives	10

Unit 1

About IT Governance	11
1.1 Concept and Definitions	12
1.2 The Value of IT in the Organization	15
1.3 Current State and Perceptions of IT Governance	18
1.4 Governance, Compliance, and Risk Management in IT	20

Unit 2

Establishing IT Governance and Compliance	27
2.1 Assessment	29
2.2 IT Strategy	32
2.3 Tactics	36
2.4 Operation	39
2.5 Compliance	43
2.6 Performance	46

Unit 3

The COBIT Framework	51
3.1 Overview of COBIT	52
3.2 The Goals Cascade	58
3.3 The COBIT Governance and Management Objectives	65
3.4 Deploying and Implementing COBIT	70

Unit 4

IT Governance Frameworks	75
4.1 Quality Management as a Foundation	76
4.2 ISO 9000 Family	81
4.3 Maturity Models	88
4.4 Relationship to Service and Architecture Frameworks	93
4.5 Relationship to IT Security Frameworks	102

Unit 5	
Data Protection and IT Security	107
5.1 Data Protection	108
5.2 IT Security Management	111
5.3 IT Security Threats and Attack Scenarios	114
5.4 Countermeasures	118
5.5 Cryptography	123
Appendix	
List of References	132
List of Tables and Figures	136

INTRODUCTION

WELCOME

SIGNPOSTS THROUGHOUT THE COURSE BOOK

This course book contains the core content for this course. Additional learning materials can be found on the learning platform, but this course book should form the basis for your learning.

The content of this course book is divided into units, which are divided further into sections. Each section contains only one new key concept to allow you to quickly and efficiently add new learning material to your existing knowledge.

At the end of each section of the digital course book, you will find self-check questions. These questions are designed to help you check whether you have understood the concepts in each section.

For all modules with a final exam, you must complete the knowledge tests on the learning platform. You will pass the knowledge test for each unit when you answer at least 80% of the questions correctly.

When you have passed the knowledge tests for all the units, the course is considered finished and you will be able to register for the final assessment. Please ensure that you complete the evaluation prior to registering for the assessment.

Good luck!

BASIC READING

Selig, G. (2008). *Implementing IT governance: A practical guide to global best practices in IT management*. North Brabant: Van Haren Publishing. (Database: ProQuest).

REQUIRED READING

UNIT 1

Lucas Jr, R. E. (2018). What was the industrial revolution? *Journal of human capital*. *University of Chicago Press*. 12(2), 182-203. (Database: EBSCO).

Carsten, B. (2008). *Pharmaceutical research in Wilhelmine Germany: The case of E. Merck*. Bonn: Max Planck Institute for Research on Collective Goods. (Database: EBSCO).

UNIT 2

Campbell, F. C. (2011). *Joining: understanding the basics*. Almere: ASM International. (Database: ProQuest).

Teti, R., Jemielniak, K., O'Donnell, G., & Dornfeld, D. (2010). Advanced monitoring of machining operations. *CIRP Annals-Manufacturing Technology*, 59(2), 717-739. (Database: EBSCO).

Pawlowski, L. (2008). *The science and engineering of thermal spray coatings*. Chichester: John Wiley & Sons. (Database: ProQuest).

FURTHER READING

UNIT 1

Müller, J. M., Veile, J. W., & Kiel, D. (2018). *Strategic implications for industry 4.0-platforms -- A social capital perspective*. Proceedings of ISPIM Conferences, 1-24. (Database: EBSCO).

Sommer, L. (2015). Industrial revolution-industry 4.0: Are German manufacturing SMEs the first victims of this revolution? *Journal of Industrial Engineering and Management*, 8(5), 1512-1532. (Database: EBSCO).

UNIT 2

Swift, K., & Booker, J. (2013). *Manufacturing process selection handbook*. Oxford: Butterworth-Heinemann. (Database: ProQuest).

TIP

Should you have any problems logging into the library databases or accessing full texts, please contact the library helpdesk:

lis@iubh-fernstudium.de

LEARNING OBJECTIVES

IT Governance and Compliance are key elements within corporate governance as most modern businesses rely heavily on IT infrastructure for their success. They describe the required leadership and organizational structures for maintaining and extending information technology to meet the business strategies and objectives. Ensuring compliance with the IT governance framework can be a daunting task which requires constant collection, organization, monitoring, analysis, and reporting on event logs to detect and manage control-related activity. Students will learn several different IT governance frameworks, in particular the industry standard model COBIT.

IT governance and compliance encompass tools to achieve organizational goals and satisfy regulatory requirements. Therefore, it is important to be able to set out the processes and policies for administering and managing IT systems for ensuring compliance with these local and international regulatory requirements. After planning and implementation comes long-term management. Professionals must recognize the IT governance and compliance monitoring tools for ensuring that controls for information systems are effectively implemented, monitored, and maintained.

UNIT 1

ABOUT IT GOVERNANCE

STUDY GOALS

On completion of this unit, you will have learned ...

- how to explain IT's role in various organizations.
- the current state of IT governance.
- the role of governance, compliance, and risk management in IT.

1. ABOUT IT GOVERNANCE

Introduction

All organizations are created for the purpose of achieving specific goals. Organizations typically establish a mission and identify business strategies that will allow them to meet these goals. An organization's mission statement details the objectives it is aiming to accomplish and the reasons for selecting specific strategies to pursue these objectives. An organization's strategies are the pathways selected to achieve its mission. In order to successfully accomplish its mission using identified strategies, an organization needs governance.

Governance can be defined as "systems by which an organization makes and implements decisions in pursuit of its objectives" (ISO 26000, 2010). Governance systems include the policies and processes designed to direct and control organizational activities, protect stakeholder interests, and deliver business objectives. A good governance framework helps to ensure the success of the organization, characterized by leadership, accountability, transparency, effectiveness, and efficiency. Governance frameworks are not necessarily uniform; governance styles and components will vary from organization to organization, addressing areas such as management, finance, operations, marketing, and technology. Governance style reflects what the organization considers to be the most important principles that will help it to fulfill its mission.

The modern organization relies heavily upon information and communications technologies (ICT). Information technologies (IT) no longer play a mere supporting role within organizations; they have become embedded in the very infrastructure of the organization itself and therefore need to be understood as generators of business value. Given this growth in significance, IT needs targeted governance systems for three primary reasons: a) optimize its performance within the organization, b) direct and control the organization's IT resources, and c) maximize the benefits and values from investments in IT. IT governance ensures that the information technologies operating within an environment are consistent, reliable, effective, and efficient, and are in alignment with organization's core mission and business strategies.

1.1 Concept and Definitions

IT governance is an integral part of an organization's overall governance, which focuses on IT strategy, IT performance and risk management, and the alignment of IT with an organization's mission and business objectives. There are a range of definitions of IT governance cited in IT communities, each incorporating different angles and perspectives.

The international professional association for IT governance ISACA (formerly known as Information Systems Audit and Control Association) established a framework called COBIT (originally published under the full name "Control Objectives for Information and Related

Technologies” but now only known as COBIT), which aims to describe best practice in IT governance and IT management. COBIT defines IT governance as the “governance (that) ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives” (ISACA, 2012, p.10).

The IT Governance Institute (ITGI), an affiliate of ISACA, defines IT governance as “the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives” (IT Governance Institute, 2003, p.10).

Research firm Gartner defines IT governance as “the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals” (Gartner, 2019). Researchers De Haes and Van Grembergen (2015) state that IT governance is “an integral part of corporate governance and addresses the definition and implementation of processes, structures, and relational mechanisms in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled business investments.”

Another commonly referenced IT governance definition states that IT governance is a “framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensure that an organization’s IT supports and enables the achievement of its strategies and objectives” (Sciforma, n.d.).

The exact definition of IT governance is a topic of academic debate. Therefore, one should not view IT governance in exact terms or as a prescriptive science but rather treat IT governance as a general framework. When discussing IT governance, the focus should always be on the big picture of how IT operates within an organization and the relationship of IT governance with general organization governance. While each of the preceding definitions vary in some aspects, all generally address the idea that IT governance is the link between an organization’s strategic mission and objectives and its information technology-related strategy. The key focus here is on alignment between and organization’s IT and its business objectives.

The main goal of IT governance is to ensure that an organization’s IT resources deliver value to the organization’s stakeholders. Specifically, IT governance establishes IT policies and monitors their implementation, oversees the performance of information technologies, and mitigates risks associated with IT. According to COBIT, IT governance must direct, monitor, and evaluate an organization’s IT strategy and operations. Other organizations that publish IT standards take somewhat different approaches. For instance, the IT Governance Institute (ITGI) summarizes IT governance into five focus areas: strategic alignment, value delivery, resource management, risk management, and performance management.

The need for IT governance grew out of several factors, including the increasing complexity of technology, the increasing critical dependences of organizations on the technologies they utilize, and the maturities of the business-technology relationship. With the growing

maturity of the business-technology relationship, organizations began to recognize that IT needs to be governed at much higher level within the organization governance and management structures.

A number of factors act as “drivers” or “principles” of IT governance, specifically business needs, shareholder expectations, sources of authority, regulatory requirements, and business pressure.

- Business needs: IT governance is driven by an organization’s business needs. Of these needs, the most primary one is to create value. One of the key concerns of IT governance is how should IT resources meet the organization’s business needs. Irrespective of how advanced a specific technology might be, if it does not align with business needs, it should not be utilized.
- Stakeholder expectations: Stakeholders are ultimately responsible for an organization’s success. Therefore, IT governance must address and align with the business mission and objectives as laid out by the stakeholders.
- Sources of authority: IT governance must address sources of authority within an organization and the specific chain of command that specifies who the final decision makers are within the organization must be clearly identified. Who is the governing body that has the final responsibility to monitor, evaluate, and direct IT resources? This should be clearly identifiable in the IT governance structures.
- Regulatory requirements: Organizations need to meet various regulatory requirements such as legal, financial, operational, risk management, and audit requirements. Working in conjunction with IT governance, IT compliance focuses on establishing appropriate controls on IT operations that meet and satisfy regulatory requirements.
- Business pressure: The changing competitive landscape and regulatory environment continually forces organizations to adjust their IT resources in order to respond to changes in the business environment more efficiently and effectively.

From a management point of view, several key questions must be answered through IT governance:

- How would IT investment align with our organization’s mission?
- How would IT create and return value to our organization?
- How would IT be controlled in our organization?

A number of international standards on IT governance have been proposed and adopted:

- The COBIT framework works with other standards both on IT governance as well as general industry best practices such as PMI-PMBOK and PRINCE2. COBIT is considered a broad framework and as such has been adopted beyond IT governance.
- The International Standard for Corporate Governance of Information Technology (ISO/IEC 38500) was jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 38500 provides a framework for effective governance of IT to assist organizations’ top leadership to understand and to fulfill their legal, regulatory, and ethical obligations with respect to their organizations’ use of IT.

- The Information Technology Infrastructure Library (ITIL) originated from United Kingdom and is a framework that addresses best practices in IT service management (ITSM).
- ISO/IEC 20000 is an international standard that covers similar topics to ITIL but expresses this content as verifiable properties and can therefore be used as a basis for auditing and certification.
- The Capability Maturity Model Integration program (CMMI) is a process improvement and appraisal program with an origin in software development. The main goal of the CMMI program is to establish and measure the maturity levels of IT within an organization.
- Other frequently referenced and adopted standards include ISO 9000, a series of standards on Quality Management Systems (QMS), as well as ISO/IEC 27001 which is an Information Security Management System (ISMS) standard.

The demands placed on information technologies continue to grow at an ever-increasing pace and will continue even more rapidly in the future. IT governance is essential to help an organization to best monitor, evaluate, and direct its IT resources to be optimally aligned with the organization's mission and objectives.

1.2 The Value of IT in the Organization

One of the primary objectives of IT governance is to maximize the benefits and values from IT investments. IT being responsible for delivering value represents a significant departure from its previous role within an organization. With this new role, the position of IT has been elevated to one of significant strategic importance, thus explaining why it is necessary for IT to have its own governance.

Traditionally, within the value chain model of a business, IT was seen as a part of an organization's supporting infrastructure without having any strategic significance for the organization's mission and objectives. In other words, IT has traditionally been treated as a line-item necessary for supporting an organization's operations, but not as a value generator. After the "dot-com bubble" burst in the late 1990s, some in the business landscape claimed that "IT doesn't matter" (Carr, 2003), arguing that while IT has introduced new ways of running businesses, IT in many cases is a commodity like electricity and does not in itself generate true, lasting business value from investment. The challenge for an organization here is to distinguish between IT for standard processes that should indeed be treated as a commodity, and IT for non-standard processes where the organization's strategy is to be significantly better than the competition.

The value of IT is a complex issue as it often requires the organization to examine the intricate relationship between its IT environment and its mission, business strategy, and business operations. Adding further complexity is the fact that IT often requires large initial capital investments, requiring organizations to explain to shareholders how business value is being created through these investments and by what extent. It is thus essential to have a strong shared understanding of the value of IT within organizations.

There are several key questions regarding the value of IT in the organization that require further discussion. To begin with, what is value? In the investment sense, value is “a fair return or equivalent in goods, services, or money for something changed” (Merriam-Webster, 2019) or “the determination of the prices of goods and services” (Encyclopaedia Britannica, 2019). Next, we need to ask how an organization determines the value, i.e., the return or price, of its investment in IT. There are a number of different approaches that an organization could take to measure the value of IT **investment**.

Investment

Allocating money to some effort or property, expecting to get a higher benefit in the future.

1. Where and how would IT investment directly increase our organization’s value including general business revenue?
2. Where and how would IT investment directly reduce our organization’s cost?
3. Where and how would investment in IT improve our organization’s efficiency and productivity, thus indirectly reduce cost?
4. Would IT investment open up new business opportunities for our organization through new products and services, thus generating new revenue streams?
5. Would investment in IT improve the quality of our existing services as measured by external and internal customer satisfaction?
6. Would IT investment help to improve our organization’s risk management and compliance, e.g., improving business continuity and ensuring quicker disaster recovery?

All of these questions essentially ask how investment in IT assists an organization to achieve their core business objectives, either directly or indirectly. However, when evaluating potential investments in IT, it is not always possible to utilize traditional methods of evaluating business value, as IT often provides intangible as well as tangible benefits to an organization. While sometimes methods such as return on investment (ROI), net present value (NPV), and internal rate of return (IRR) can be used to evaluate IT investments, often the intangible aspects of IT investment defy precise measurement.

So how does an organization measure less tangible value? Perhaps the easiest starting point is looking at an organization’s productivity and efficiency. Modern business applications have significantly improved the efficiency and effectiveness of most business operations. For example, enterprise resource planning (ERP) tools, including those used for supply-chain management (SCM), customer relationship management (CRM), and human resource management (HRM), have revolutionized the entire chain of business operations. ERP systems enable management to have a complete view of the entire operation in real time, making just-in-time operation a possibility for many businesses. For an organization’s decision makers, this means business decisions can be made quickly and thus reflect the true and changing business environment. ERP systems also directly reduce the cost of operations, e.g., reducing inventory requirements by deploying just-in-time supply-chain management.

While not every organization will become an industrial “disrupter” by using new technology (e.g., Facebook, Uber, Lyft), IT has proved to enable new opportunities. Using IT, innovation is possible for almost any organization regardless of what, where, and how the organization delivers its core competences. Over the past few decades, the world has seen rise to new business models that were not even conceivable prior to the Internet revolution. On the flip side, legacy companies such as Kodak and Sears who failed to adapt their business models for the new information age have all but disappeared.

If a new IT system opens up new opportunities for an organization, one would imagine that the business value realized as a result of such opportunities could be easily measured. However, since IT is a key component of business infrastructure in most organizations, the actual contribution made by newly-introduced IT needs to be carefully analyzed. Baseline and subsequent analyses, i.e., comparing before and after the introduction of an information technology, can provide quantitative data regarding the value of particular technologies. Direct or indirect increases in revenue, direct or indirect reductions in costs, and increases in user productivity all require different types of analysis to produce firm data to support any conclusions about the value of IT. End-user perceptions, known as social factors, also influence the value of IT to a business. For example, IT supporting automation may lead to job-security concerns for some employees. In other cases, IT systems may provide equal access for users regardless of their sex, age, education, disability, etc. and facilitate a sense of belonging, while in other circumstances, IT systems may evoke competitiveness among users. The impact of human perceptions and other social factors is difficult to evaluate but nevertheless should be considered when measuring the value of IT.

The primary question regarding the value of IT is often a simple one: For a specific amount of investment in IT, how much is the return (ROI)? Theoretically, one could begin calculating the ROI by first defining an IT system that fulfills a set of desired functions. The next step is to calculate or estimate the **total cost of ownership (TCO)** of the system. The third step is to evaluate the value that the system has brought in or will bring in if not yet implemented. Finally, one can then calculate the ROI by comparing the calculated or projected value against the TCO. However, in reality, the situation is often more complicated. Since IT does not operate in isolation, to actually quantify the value generated can be very difficult. Numerous studies by academic researchers attempting to answer the question of what value specific IT investments can or have brought to organizations have been conducted, but with only limited success. Unfortunately, the complexity of analyses such those conducted by academics is often beyond the capacity of the average organization.

An alternative method to evaluate the value of IT is to use qualitative measures instead, using relevant metrics to illustrate the relationship between business objectives and IT functions. For example, a video-conferencing system can satisfy some of the organization's networking and meeting requirements. The potential time savings and improvements in efficiency may be hard to quantify, but the system can nevertheless be qualified as a value generator, especially for a geographically dispersed organization. By attaching specific IT system functions to individual business objectives, business requirements, competitive advantages, etc., a picture of business-to-IT alignment can emerge. This alignment, i.e., the organization's ability to utilize IT to achieve its business objectives, is exactly what IT governance seeks to provide. Even though this type of analysis does not usually yield quantified values, it nevertheless can provide solid and qualified results to support IT value evaluations. For example, one could examine a specific business function such as human resource management (HRM), which will typically have **key performance indicators (KPI)**. The next step is to research a specific IT system that supports HRM in the organization and understand its capabilities and performance. By investigating the alignment between the two, including functions, capability, effectiveness, and cost, among other KPIs, a number of metrics could emerge that support an evaluation of IT value.

Total cost of ownership (TCO)

Approach to estimate the financial cost involved in some activity, making sure to include all long-term and external costs.

Key performance indicators (KPI)

Measurable values that indicate the success of an organization's performance against predefined objectives.

A different approach to evaluating investments known as the balanced scorecard developed by Kaplan and Norton has been used for IT investment analysis (Kaplan & Norton, 1992). The original idea was that the evaluation of a company should not be restricted to the traditional financial performance measures but should be supplemented with measures concerning customer satisfaction, internal processes, and the ability to innovate. Utilizing these additional perspectives, results could be obtained to assist future financial forecasting. The basic idea of the balanced scorecard is that there is a three-layered structure (including a mission, objectives, and measures) for each of the four perspectives (business contribution, user orientation, operational excellence, and future orientation).

In general terms, the value of IT within an organization essentially comes down to its effectiveness and efficiency relative to the organization's mission and objectives. The role of IT governance is to align information technologies with an organization's mission. Thus, any IT value propositions must be judged within the framework of IT governance, as one of the key IT governance is to realize the business value of IT. The more advantages of IT that are aligned with an organization's strategic objectives, the greater the value of IT. Such value may be quantified but owing to the complexity of measuring both tangible and intangible value, in many cases, it is simply just identified. A comprehensive understanding of IT value, direct or indirect, tangible or intangible, and its alignment with organization's core business, helps an organization to best utilize and improve its information technologies.

1.3 Current State and Perceptions of IT Governance

A number of studies have strongly suggested that the financial performance of organizations is positively correlated with governance (Darweesh, 2015). However, research on the current state of organizational governance around the world has indicated that, despite recognizing the importance of governance frameworks, actual governance practices have generally received less attention from organizations than they deserve (Asgarkhani et al., 2018).

The establishment of governance frameworks within organizations is the result of many factors. Whether or not broader governance frameworks have been adopted by an organization is largely dependent on organizational culture. For example, if organizations operate in a culture where there is a high concentration of leadership power (i.e., decisions are predominantly made by a small group of executives), governance frameworks typically have a limited influence. Often family-run organizations and those led by charismatic leaders show this type of governance pattern. However, if an organization is characterized by high levels of "individualism" and diversity among its leaders or there is a culture of "low power distance" between employees and management, organizational governance structures tend to be much stronger. Successful start-up technology companies often demonstrate this pattern of governance.

The varied adoption of broader governance frameworks is naturally reflected in the adoption of IT governance practices. This is no surprise given that IT governance is not only tied to but also governed by a broader level of organizational governance. On a positive note, there certainly appears to be a growing awareness and acceptance of corporate IT governance standards. More and more organizations are recognizing that IT governance is important for them to control of their IT systems, improve their effectiveness, create efficiencies, ensure maximum benefits to the organization, and adequately manage associated risks.

For organizations seeking to establish and improve their IT governance practices, one obvious place to start is focusing on the alignment between IT and core business. To do so, organizations need to examine the strategic alignment between IT and their business mission and objectives, look at how IT generates value, examine how to adequately manage IT resources and mitigate risks associated with IT, and lastly decide how to measure the maturity level of their IT systems. Misperceptions and resistance to change that could affect IT governance adoption, implementation, and improvement need to be addressed and resolved at this point, especially at the executive levels. General organizational culture and user acceptance must also be addressed as successful implement depends upon these factors.

A significant challenge to IT governance comes from IT itself. The landscape of IT is constantly changing at an ever increasing pace. Many well-known technology “disruptions” have become mainstream and IT governance has had to constantly evolve in order to keep pace with such rapid and significant changes in the industry. For example, for many decades, data have been structured into databases which are managed through database management systems (DBMS). For the most part, this remained the status quo until the emergence of “**big data**”. Big data refers to large, complex, unstructured datasets that have become available due to high speed Internet connections as well as large volumes and variety of data. Big data and its analysis have penetrated the field of data management where traditional DBMS used to dominate. Unstructured data are now becoming the main sources of data. Many in the industry are predicting that in the not-too-distant future, the majority of data will fall into this unstructured category and older methods of data management will become insufficient, if not fully obsolete. In the same way, social networks have disrupted communications and introduced a whole new set of governance issues. The proliferation of social media platforms such as Facebook has already impacted society in a profound manner. The impact of such platforms on organizations has forced IT executives to seriously consider policy and procedure changes to control and manage positive and negative effects of social media. IT executives understand that the speed of information propagation via social media is ferocious and without proper governance, it can have unpredictable consequences for organizations and their normal business operations.

Big Data

This is characterised by the “three (or four) V” of data: velocity, variety, volume, and veracity/data quality.

A number of other emerging technologies are set to change the IT landscape for organizations and need to be accommodated into IT governance structures. Developments within the scope of Internet of Things (IoT) have recently picked up pace, indicating that we are quickly moving into a highly-connected world where everyday objects are increasingly linked together. With the IoT, we are expecting a lot of device-to-device and sensor-to-sensor type of operations to emerge that do not require human intervention. The fast-pace of

development in the field of robotics has shortened the timeline for the wide-scale adoption of automation. Artificial intelligence (AI) is another area which has attracted a significant amount of attention. AI is exploring technological capabilities that include learning, reasoning, and problem solving. AI will surely impact society in profound ways. Other emerging technologies, such as software-defined infrastructure, will soon bring big changes to organizations' IT operations.

What does the emergence of these new technologies mean for organizations? Many current business leaders, even IT leaders, are having trouble adjusting to the pace of change and understanding the opportunities and risks associated with the proliferation of these new technologies. In this climate of change, the IT executive must be a champion for IT governance, establishing a clear strategic vision of IT in the organization and inserting it into the organization's governance structures and wider culture. To do so, the vision needs to be accepted and adopted by the organization's top leadership. Only with robust strategic vision can a business-IT alignment be formulated, based on a detailed understanding of the organization's mission and objectives, financial status, risk management policies, and operational environment.

A significant amount of research has been done on business-IT alignment (Buckby, Best, & Stewart, 2009). Key findings from this research are that there is a positive correlation between business-IT alignment and IT usage and its governance, better understanding between IT departments and the rest of the organization (which then leads to better IT performance), identifying key success factors for IT, and measurable IT maturity levels. Studies also indicate that although not necessarily guaranteed, value delivered via IT is possible, provided that there is effective implementation of IT governance.

The reality is, when it comes to IT governance, one needs to treat it as a living framework that will address any changes that may impact the alignment between business and IT. Such changes may arise from the business environment, but may also emerge from the technology front. Thus IT governance needs to change as required, to adapt to new requirements of the organization.

1.4 Governance, Compliance, and Risk Management in IT

In recent decades, organizations in every industry have increased their dependencies on IT infrastructure. Accompanying these increasing dependencies has been the vast exposure of organizations to IT-related risk and growth in regulatory requirements globally. As a result, two areas of IT operations have become absolutely critical to the functioning of modern organizations: IT compliance management and IT risk management.

Regardless of which industry an organization operates in or the exact nature of its business, compliance is an essential requirement. In general, compliance refers to conformity with laws, regulations, standards, ethics, and any other requirements that apply to the organization. IT compliance is a part of overall organizational compliance requirements. IT

compliance management aims to ensure that an organization's IT activities follow relevant rules and regulations, meet policies and procedures set forth by the organization, meet standards established by industrial and governmental bodies, and follow best practices in the industry, which are typically incorporated into policies or regulatory requirements. IT compliance seeks to guarantee that organizations maintain appropriate control over information and related technologies, including how are they managed and protected. Internal compliance functions typically include the policies, goals, and organizational structure of the business. External considerations may include meeting customer requirements. In short, IT compliance means that the resources, processes, and procedures that address an organization's business needs must be reported upon to provide evidence of adherence to internal policies and external laws, regulations, requirements, and guidelines.

IT risk management refers to managing and controlling risks associated with IT. Risk, as defined by risk management standard ISO 31000, is an "effect of uncertainty on objectives" (ISO 31000). The standard explains that an effect "is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats." Risk management is comprised of "coordinated activities to direct and control an organization with regard to risk." In practice, people most commonly associate risks with events that have negative impacts. Risk can be calculated by combining the likelihood of an event happening with the severity of its impact should the event. This is represented by the following formula: $\text{risk} = \text{likelihood} \cdot \text{impact}$.

There are several commonly accepted risk response strategies.

- Avoidance or elimination: This involves not starting or continuing with the activities that give rise to the risk, e.g., canceling a migration project of an ERP system from one vendor to another.
- Acceptance or retention: This involves accepting the loss incurred by a risk when the event occurs, e.g., accepting a potential electrical power loss because adding a redundant power source is too expensive.
- Transferring or sharing: This involves having another party share the burden of a loss, e.g., purchasing an insurance policy against equipment failure.
- Mitigation or reduction: This involves reducing the severity of the loss or the likelihood of it occurring, e.g., adding a redundant communication line to prevent outages caused by a single communication line failure.

IT risk management is the process of identifying, analyzing, and responding to uncertainty associated with IT operations. Negative IT uncertainty (i.e., risk) arises from various threats that could adversely impact organization's normal business operations, with potentially significant financial and other consequences. For example, IT infrastructure failures such as system and network downtime have become far too costly for organizations to bear. Data loss is another common and costly risk, both in real financial terms and in terms of business reputation. Most organizations have mechanisms for general risk management but do not always have adequate measures to deal with IT-related vulnerabilities.

IT governance, compliance, and risk management work closely together. It is worth noting that in many organizations the exact boundaries between them are often blurred as there are significant overlaps of functional coverage as well as management structures. In some circumstances, compliance and risk management could be considered part of IT governance, since both contribute to the alignment of IT and business objectives. In any case, IT governance, compliance, and risk management should not be treated as independent components of an organization's overall governance. For some organizations, a combined governance, compliance, and risk management (GCR) department is part of the overall organizational structure, allowing such organizations to coherently and effectively oversee the three operations together.

The impetus to establish IT governance does not always arise from within organizations. For the most part, compliance requirements are generated by external sources such as regulatory authorities, business partners, and business clients. To create business-IT alignment, IT governance must understand the business environment that the organization is operating within, which often demands the organization to comply with specific obligations. IT governance is an integral part of overall organizational governance; as any organization will have various compliance requirements, IT governance has an integral role to play in general compliance. Specifically, IT processes are part of the majority of an organization's business processes. Thus, in order for any business process to be in compliance with regulations, the underlying IT processes must also comply. For example, in order for a business supply chain process to be in compliance with regulatory mandates regarding security, the supporting and the underlying ERP operations must do so as well. An ERP operation consists of many components, such as the ERP system, ERP operational procedures, the related data flow, and data storage; all of these must meet the related security compliance obligations.

What does IT risk management look like in an organization? Historically, a significant number of IT compliance requirements have related to IT risk management. Nowadays, many compliance requirements are associated with standardization, but managing risk remains a significant part of general compliance activities. Thus, IT risk management within an organization represents a large portion of general risk management undertaken by an organization. In general terms, information technologies are associated with a wide range of risks. Risk factors include a wide spectrum of external threats, such as cybercrime and fraud, and internal threats, such as errors and omissions. These threats can be intentional or unintentional and can have different degrees of potential impact on business. Severe impacts could include major disruptions to an organization's normal business operations, security breaches such as data loss, financial loss due to interruptions, and damage to business reputations.

The process of managing IT risk is the same process utilized for general risk management. There are four stages of the risk management process: risk identification, risk evaluation, risk prioritization, and risk response.

- Risk identification: This first step involves identifying all possible events that may have an impact on IT. The identification stage is broad; the aim is to generate a comprehensive list of risks without going into too much detail. Organizing and categorizing identified risks then helps with further analysis.

- Risk evaluation: This is probably the most challenging task. Risk evaluation involves in-depth analysis of the severity of potential business interruptions and their associated financial costs, calculating the likelihood or probability of such risks occurring, and determining the probable causes of risk. At times qualitative analysis, i.e., categorizing risk without quantitative analysis, is sufficient. That said, numerical or quantitative analysis is a superior but more complex way to evaluate risks.
- Risk prioritization: During this stage, risks are prioritized by comparing their level of risk against the organization's predetermined risk target and tolerance levels, in order to take actions on the most urgent or highest impact ones. Information such as the combined financial impacts, probability, along with other subjective criteria that is important to the organizations such as safety concerns, reputational impact, vulnerability, etc., are used to categorize risks into priority classes for action.
- Risk response: At this stage, appropriate responses to risks are determined. As discussed earlier, there are four common methods to respond to any risks: avoid, accept, transfer, or mitigate.

There are various frameworks and methodologies for IT risk management. For example, the COBIT framework contains a risk management element that fills the gap between generic risk management frameworks and detailed IT risk management frameworks (primarily security-related). It provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the organizational culture right through to operational issues. The importance of IT risk management is recognised by various frameworks: the COBIT framework specifically identifies risk optimization as one of its top governance objectives while the IT Governance Institute considers risk management as one of the five focus areas of IT governance. Sometimes organizations have separate risk management departments to oversee all risks including IT risk management, while other organizations situate IT risk management whilst their IT department.

Governance, risk management, and compliance can be viewed as an umbrella framework that integrates three key areas that affect an organization's IT governance objectives. Focusing on these three areas is a recent trend adopted by many in the IT industry, and new practices and tools have been developed to support it. When effectively addressed, these three aspects work together to ensure that an organization's IT activities and functions maximize return on investment and deliver business value. By combining governance, risk management, and compliance into a unified view, the three closely-related aspects can work in unison to utilize an organization's IT investments in the most effective and efficient way. In this way, one should not view IT governance as an isolated perspective. Rather, components such as compliance and risk management will work in conjunction with IT governance structures to ensure that an organization's IT strategy and the resources allocated to implement it will maximize value for the organization.



SUMMARY

The main objective of IT governance is to ensure that an organization's information, related technology resources and investments are closely aligned with its mission and business objectives. The main functions of IT governance are to evaluate, direct, and monitor all IT within the organization.

IT governance establishes an organizational level of IT strategy, resource, and control activities. The governance is an integral part of an organization, providing oversight and accountability of all IT related policy, management, compliance, and risks. It is a framework aimed at ensuring that all IT systems, resources, and practices work together to achieve the organization's mission and strategic objectives.

The purpose of IT governance includes: alignment between business and IT, delivery of IT values to the organization, management of IT related risks, improvement of overall IT performance, and establishment of responsibility and accountability. One of the key issues that relates to IT governance is the value of IT, and how that aligns with the organization's strategic objectives.

There are many challenges that lie between IT governance and its successful implementation, but the most important challenge is the necessary recognition of its critical significance. As organizations have become heavily dependent upon information and related technology, IT success directly impacts organizations' success. Even though most organizations recognize the importance of IT, successful IT governance adoption and implementation are still required to overcome obstacles within the organization.

To fully develop solid, meaningful, and reliable IT governance, the organization is required to have a thorough understanding of several key aspects of IT. This includes the business environment in which IT is operated, current governance status, desired strategies, compliances and other regulatory requirements, along with other stakeholders' needs. A solid governance model will require incorporation and adaptation of the current industry's best practices as well as various relevant technology and management standards. A good knowledge of IT fundamentals is another necessity needed to align technology with organizations' business objectives. Finally, a solid understanding of information security is a must-have component in any IT governance model.

It must be emphasized that IT governance is not a set of rules or prescriptions, it is a framework. Organizations must adapt to best suit their own mission, strategy, organizational structure, and business environment in order to have the most effective governance in place.

UNIT 2

ESTABLISHING IT GOVERNANCE AND COMPLIANCE

STUDY GOALS

On completion of this unit, you will have learned ...

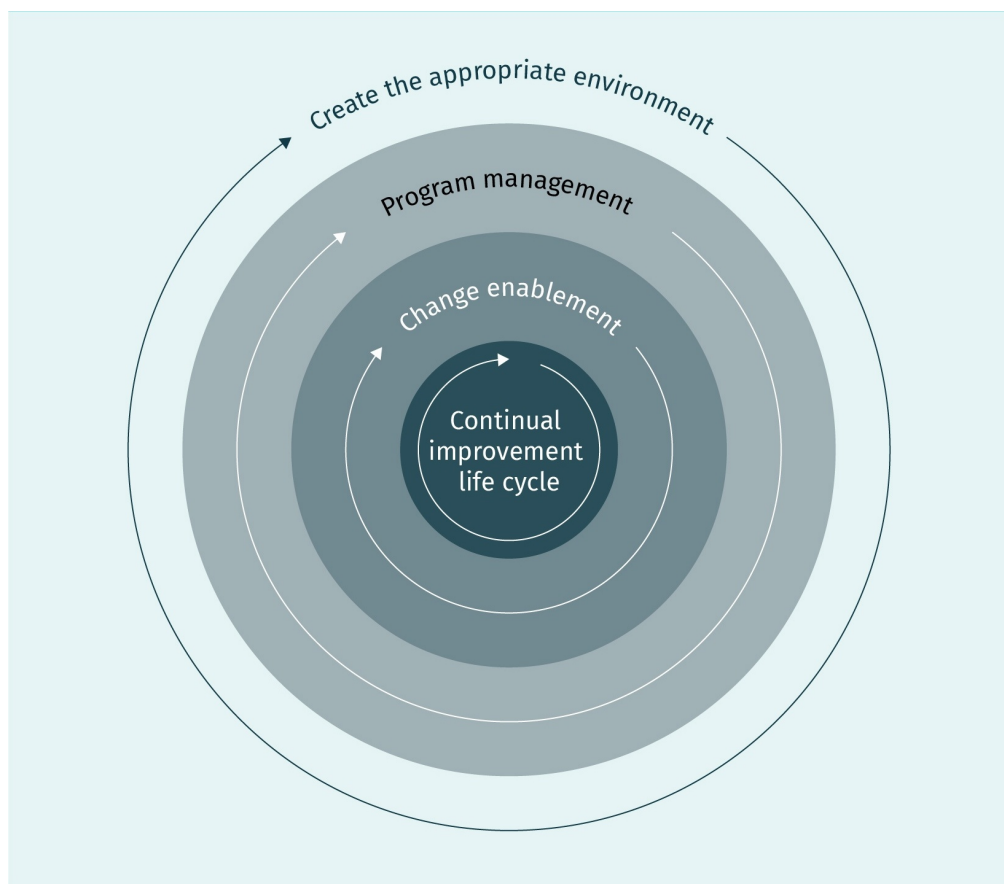
- to apply assessment methods in different contexts.
- IT strategy and tactics.
- how to measure performance through auditing and the IT balanced scorecard.
- the components of IT governance and compliance operations.

2. ESTABLISHING IT GOVERNANCE AND COMPLIANCE

Introduction

IT governance is a framework with its own life cycle, just like any other IT product. It is established using a similar methodology to the system development life cycle (SDLC) typically employed to develop IT products. IT governance is a living product and is constantly evolving, with each life cycle bringing about improvements and system maturity. As COBIT describes, the life cycle can be divided into phases that follow on from one another.

Figure 1: IT Governance Implementation Life Cycle



Source: Created on behalf of IU (2019).

A successful roadmap for IT governance involves several phases. To begin with, a full assessment of an organization's current IT, along with a thorough understanding of the organization's vision, mission, and strategic objectives form the foundation for the life cycle. With that knowledge, the next step in the process of establishing IT governance

focuses on the strategic alignment between business and IT. Once the alignment is clear, the rest of IT governance need to tackle issues in performance monitoring, compliance monitoring, and continuing improvement.

2.1 Assessment

Establishing IT governance begins with a thorough assessment of the current IT environment in an organization, regardless of whether the task at hand is to establish a brand-new framework or improve an existing framework via a renewal cycle. The main purpose of the assessment is to establish a baseline for existing IT operations which then facilitates an analysis of requirements. Undertaking an assessment therefore involves taking a complete snapshot of current operations. If an IT governance framework is already in place, then the assessment essentially becomes a performance review with a focus on identifying potential for continuous improvement. Other objectives might include assessing key governance requirements and governance control measurement, streamlining and simplifying controls, reviewing governance maturity, and assessing governance knowledge management, awareness, and engagement.

There are two key decisions that need to be made regarding the assessment of IT governance in an organization: (1) which topics/subjects/areas to assess (assessment content) and (2) how to conduct the assessment to yield the most useful results (assessment methodology).

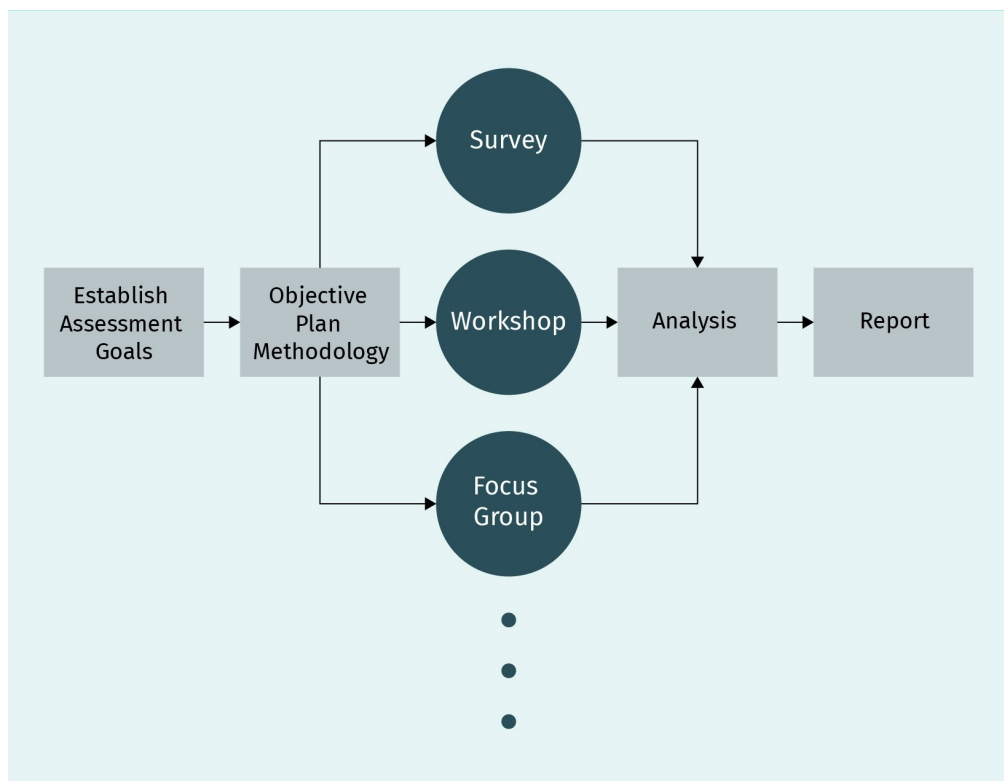
Let us start with what to assess. The first part of IT assessment is generally focused on structure and process, sometimes referred as “hard” governance (as opposed to other “soft” governance areas such as organizational behavior) (Smits & van Hillegerberg, 2018). When assessing IT structure, the focus is on how roles and functions as well as management networks are structured. This area of assessment should result in a clear picture of the existing IT organization map. When assessing process, the focus is on IT decision-making, planning, and monitoring processes. It should be noted that the aim of assessment is not to understand detailed IT operational processes such as how an enterprise resource planning (ERP) system is set up. Rather, the purpose of assessment is to discover “how” IT operations are governed. In other words, the focus is more on the policy level rather than the operational level.

Besides structure and process, organizational behavior is another area which requires close attention. The assessment should focus on leadership, more generally at the organizational level as well as IT-specific leadership. It is important to understand the relationship between leaders and their level of understanding of and trust with one another and the entire organization. Other organizational cultural conditions such as the general environment, atmosphere of collaborations, attitudes, participation levels, and communication regarding the continuing improvement of IT operations, are potential foci for assessment that could have a significant effect on IT governance. Finally, in addition to these hard and soft governance areas, external factors such as the competitiveness of the business environment, features of the general industry sector in which the organization is situ-

ated, and the legal and regulatory requirements surrounding the organization, must also be included in the IT governance assessment in order to be reflected in the governance itself.

The methodology chosen for assessment varies depending upon the organization as well as the topics to be assessed. Common methodologies include direct surveys, workshops, focus groups, and interviews. The following figure illustrates that while the methodology chosen to assess the IT governance can vary, the phases of the assessment are the same.

Figure 2: General Assessment Process Flow



Source: Created on behalf of IU (2019).

Survey

Survey is the most common assessment tool and can be used to assess a large population. However, depending upon the survey topics and organizational structures, rather than surveying the entire organization, often a selected sub-population, i.e., sample, is used to save time and reduce effort without drastically affecting the validity of the results. Surveys can be verbal or written where participants answer a predetermined set of questions, known as a questionnaire. Questionnaires can be structured according to a number of different several formats. Commonly used formats include dichotomous questions where the participant is asked to indicate their answer to a question in the form of yes or no or forced

choice questions where the participant may select an answer from a number of listed responses, e.g., multiple choice questions. Other question formats such as ratings, rankings, staple scale, semantic differential scale, etc., are also commonly used.

True survey design and result analysis can be rather complex, especially if the survey is used with a large population. In those situations, careful planning and detailed statistical analysis are required. There are two steps involved in designing a large survey.

1. Developing a sampling plan: A sampling plan details how to select a set of samples from the general population, varies in methodology from totally random selection to identifying representative portions of different departments.
2. Establishing procedures: Important procedures include deriving population estimates from the sample data and estimating the reliability of these population estimates.

A key element of any survey is to have survey questionnaires that produce “answers that are reliable and valid measures of something we want to describe” (Fowler, 1995, p.2). Survey questions can be open-ended, which allow the respondents to use their own words, or close-ended, which ask respondents to choose from a given set of responses.

Workshop

A workshop involves gathering and recording a group of people engaging in discussion on a particular subject. This methodology is frequently used for training and information-sharing as well as various assessment purposes. Holding a workshop allows participants to interact with one another in real time and thus can produce collective outputs. In its typical format, a workshop progresses in stages, starting with opening of the workshop, followed by different working sessions, and finally finishing with conclusions. When a workshop is used for assessment purposes, the assessor is a facilitator rather than a chairperson. Assessment workshops are largely open-ended, especially when compared to focus group discussions where facilitators guide the discussion. At the end of the workshop, a debriefing should take place to clarify any possible misconceptions or misinterpretations and reaffirm the results of the assessment.

Focus Group

A focus group is another way to have a number of participants discuss a specific topic. The main difference between a focus group and a workshop is that a focus group has a specific “focal” point and the discussions are led by the facilitator. A focus group has a narrowly-defined topic and each participant is invited to respond to specific questions. The facilitator has a set of questions prepared and outcomes from a focus group are centered on the questions. Participants may well influence each other, as in a workshop setting, but the discussions are not open-ended. A focus group does encourage discussions or interactions where individuals are invited to explore topics in relation to others and have the input of others shape their thoughts.

Interview

One-on-one interviews often produce the most in-depth assessments. However, as this is the most time-consuming method, it is often reserved for only key personnel. The major advantage of an interview assessment is its dynamic nature, when the interviewee can reveal information not anticipated by the interviewer. Like any other assessment method, a well-prepared outline provides the foundation for the process. The outline can even be sent to interviewees ahead of the meeting so that they have more time to prepare.

After data are collected, the next step is data cleansing, which involves removing irrelevant or extraneous information, reducing the data to only essential sets, and organizing it into a structure required for analysis. There are two main approaches to analyzing data: qualitative and quantitative. Qualitative analysis is used to interpret data to derive a more descriptive picture. Some commonly used qualitative techniques are metrics and narrative descriptions. Quantitative analysis involves applying numerical and statistical analysis methodologies to generate relevant numerical measurements and indicators.

Throughout the assessment process, one should always keep an open mind and be reminded that this is a process of data collecting, not active change management. This means collecting information without necessarily trying to correct and implement new processes. The outcome of any assessment is a picture of the current status and baseline of the IT environment that can then be analyzed to establish and/or improve IT governance.

2.2 IT Strategy

Before IT governance can take shape, the first step is to fully understand the organization's vision and mission. As discussed earlier, the purpose of IT governance is to align organization's IT resources with organization's mission and strategic business objectives. IT governance is under the general framework of organization's broad governance, and therefore is governed by the organization's top stakeholders.

A vision is a picture of the future, and the vision of an organization is a credible, attractive, yet realistic picture of what the organization sees itself in the future. Vision represents the ideal futuristic image of the organization. Simply stated, a vision is a dream that needs to be communicated with all stakeholders as well as affect communities. Vision should be easy to understand and covers a broad base. Vision serves as a focal point for establishing organization mission and planning its long-term business strategy. Vision allows organization's governing principles to be developed. Here is a case of vision statement from Vodafone (Vodafone, 2013): "Our vision sets out our ambition to deliver connectivity and innovative services to improve people's livelihoods and quality of life."

A mission is the very reason for an organization to exist. An organization's mission statement describes what it is going to do, and why it is going to do that. Mission statements are similar to vision statements, but more specific and concrete. A mission statement defines the organization's uniqueness, its business objectives, and its strategy to reach

those objectives. Mission statements focus on actions, as opposed to vision statements, which focus on an end-goal. An example of mission from Google reads (Google, 2014): “Our mission is to organize the world’s information and make it universally accessible and useful”

Mission statements often are viewed by stakeholders as the starting points of an organization’s strategic planning process. Mission statements inform the stakeholders, both internal and external, what the organization's goals are, and how it is attempting to accomplish those goals. Another example of mission statement from Coca Cola reads (Coca Cola, 2013):

Our mission is:

- To refresh the world in mind, body and spirit
- To inspire moments of optimism and happiness through our brands and actions
- To create value and make a difference.

The strongest organizational impact occurs when mission statements contain the following essential dimensions (Bart, 2002):

- Key values and beliefs
- Distinctive competence
- Desired competitive position
- Competitive strategy
- Compelling goal/vision
- Specific customers served and products or services offered
- Concern for satisfying multiple stakeholders

Strategies are one or more ways to use the mission statement in order to achieve the vision statement. Strategies explain how to reach organization's mission. Although an organization will have just one vision statement and one mission statement, it may have several strategies. These strategies can range from a very broad approach to a variety of operations, to the very specific objective in a narrowly defined area. However, more often strategy planning starts at a broad, organization level, objectives.

The mission statement is the starting point of organization's strategic planning process. Strategic planning is a process of decision-making rules to direct organization's main activities over the long-term. Specifically, strategic planning lays out these activities logically in sequence, and often centralized to allow management to analytically determine strategic paths for the entire organization. The actual paths to accomplishing strategic objectives are typically outlined in tactic plans.

Strategy for IT is a framework focusing specifically on information and related technology within the organization. It is a set of objectives and formal decision making process of the critical and essential components of IT and their inter-relationship, required to contribute values of IT towards the organization business value. IT strategy can define strategic IT in

general terms, or it can relate to a specific IT strategic solution. IT strategy focuses on those which are absolutely necessary and sufficient, towards achieving organization's business objectives.

Again it is necessary to emphasize that the fundamental concept of IT governance here, that is, IT governance is to align IT with organization missions and business objectives. This leads to the first stage of establishing IT strategy: aligning IT with business strategy. During this stage, key objectives in relationship with business objectives need to be defined that form the foundation of IT strategy. This includes defining overall scope and goals, identifying stakeholders needs and requirements, identifying constraints and making proper assumptions.

The next stage of establishing IT strategy is to analyze the current IT baseline, including resources, operation, and knowledge. There are several tasks involved during this stage. A full background investigation or assessment is often the best starting point of discovery process. This encompasses existing IT organizational structure, decision making process, operational procedures, key performance indicators, strengths and weaknesses, industry-wide technological, political, economic, and social factors, as well as specific emerging technology trends that may impact organization business in the future.

With a full understanding of IT baseline on hand, the next stage is the gap analysis on the alignment between IT and business. It begins with an assessment on the alignment between IT and business, by examining the two sets of objectives and potential gaps. More specifically, a number of key questions need to be analyzed:

- Can each business objective be adequately met by the current IT objectives, with required KPIs?
- Are the IT strategic goals in line with organization's business strategic goals?
- Are there any missing IT components, plans, policies, or procedures which are necessary to deliver desired IT values?
- Are there any ongoing or planned IT projects and how do they match with the business needs now and in the future?
- Are there any skill gaps of IT organization to adequately support IT operations?
- Does the IT decision making process reflect the governance?

At the end of this stage, a clear understanding of the existing gaps, along with appropriate recommendations, should emerge as the results.

The final stage of establishing an IT strategy should follow with a final strategy document. IT strategies can be broad as in most cases, or be specific. The discussion focus here will be on the broad strategy at high-level. There are a number of issues that a strategy should cover, with the variations from organization to organization. A broad-based strategy should include the following:

- Long-term plan and roadmap
- Decision making process
- Service offerings
- Cost analysis methodology

- Organization structure
- Knowledge management
- Project management
- **Change management**
- Risk management

Change Management
Management discipline concerned with implementing changes in an organisation successfully, preventing negative side effects of the change.

In reality, any strategy is heavily influenced by the culture within an organization, which can vary significantly from one organization to another, even from one department to another within the same organization. IT strategy should organically incorporate organizational culture into the framework for it to be more effective.

Organizational culture refers to the beliefs and behaviors that determine how an organization's employees and management interact and manage business operations. Organizational culture is implied, not defined, carries history, and develops organically over time. An organization's culture may be reflected in its dress code, business hours, office setup, employee benefits, turnover, hiring process, dealing with business partners, and treating customers.

Organizational culture are often categorized into four types: control or hierarchy, compete or market, collaborate or clan, and create or adhocracy.

- Hierarchy culture is a formalized and structured work environment, where formal policies and procedures are the keys to keep the organization together. Leadership is focused on efficiency-based coordination and organization. Formal rules and policy keep the organization together. The long-term goals are stability and results.
- Market culture is a results-based organization that emphasizes getting things done, and the organizational style is based on competition. Leadership is focused on producing results. Employees are competitive and are given high expectations. The emphasis of organization is on winning.
- Clan culture provides a friendly working environment. People have a lot in common, akin to a large family. The leaders are often seen as mentor figures. The organization focuses on loyalty and tradition, and promoting teamwork, participation, and consensus. Success is defined as addressing the needs of the customers.
- Adhocracy culture is a creative working environment. Leadership focuses on innovation and employees are encouraged to take risks. Innovation is the bonding force within the organization. The long-term success goals are to create new resources and new products.

Naturally, organizational culture greatly influences organization IT and its culture. One can easily see, for example, that IT strategy in an adhocracy culture has to be more cutting-edge, with significant emphasis on emerging and possibly unproven technologies. In contrast, IT strategy in a hierarchy culture requires to be more structured with set policies and procedures in order to make the operations smooth and predictable. Such a variation of IT culture will need to be considered during the development and establishment of IT strategy, to have one that truly reflect the organizational culture, as required by the business-IT alignment. The organization culture should be captured during the initial stage of IT

strategy development planning, when organization's needs and requirements are being gathered. These requirements can then be analyzed during the gap analysis phase to generate the desired IT strategy.

To conclude, here are the excerpts of IT strategic plan from U.S. Federal Election Commission, on IT strategic objectives and activities (FEC, 2018):

IT Objective 1: Implement an Information-Centric Approach

Strategic Activity 1.1: Develop an API Library An information-centric approach separates information from its presentation. Instead of building a web page specifically to house data or information, an information-centric approach asks organizations to put the information itself first, making data available in a machine-readable format—a web API—that can be accessed by any number of computers in any number of ways. By leveraging the power of the API, organizations can create content once and use it everywhere.

Another excerpt of an IT strategic plan example is from Stanford University IT services (Stanford, 2017):

Create an environment that attracts, develops, and retains world-class staff

- Talent Development
Integrate our talent management initiatives with Business Affairs
- Employee Survey
Conduct IT Services employee survey to help create alignment and set goals for organizational improvement
- **360 Feedback**
Conduct 360 survey for managers to help set development goals to improve the workplace
- Succession Planning
Evaluate talent pool of management and key individual contributors; establish succession planning

360 Feedback

Process where feedback on an employee's performance is collected from subordinates and colleagues as well as supervisors of the employee.

2.3 Tactics

After an IT governance strategy has been adopted, the next step in implementation it is to have sound tactics that fully support the strategic objectives. Strategic planning focuses on defining the overall objectives of an organization and outlining the strategies that will be utilized to achieve them over the long-term. The strategy plan defines an organization's strategy or direction and the decision-making processes that will support the organization to pursue their mission, but the actual measures taken to reach the objectives are typically left to the tactics plan. It can be said that strategy focuses on "what" while tactics focus on "how". Tactic planning has a shorter time horizon and focuses on actions that aim to achieve the goals. Tactic plans are individual to each organization as they accommodate the different objectives of each organization. Tactic plans are also flexible, that is, they can be quickly adapted to address changes in the environment.

The following table summarizes the main differences between a strategic and tactical plan. One can see from this table that tactical plans are associated with lower risk than strategy plans due to their smaller scope and reduced time horizon.

Table 1: Comparisons Between Strategic and Tactical Plans

	Organizational hierarchy	Risk level	Time horizon	Scope
Strategy	Board member executive	High	Long	Broad
Tactic	Executive department	Medium	Medium	Medium

Source: Created on behalf of IU (2019).

In order to accomplish its strategic objectives, an organization needs tactics in the form of detailed plans that outline how to deliver each component of the objectives. The tactical planning process includes multiple phases and is more detailed than the strategic planning process. While the tactical planning process will vary from one organization to the next, there are some general steps and guidelines considered good practice that include: (1) understanding the governance strategy, (2) building a team, (3) establishing a project plan, (4) testing and improving, (5) expanding the time horizon, and (6) involving the entire organization.

Understanding the Governance Strategy

During the process of developing, implementing, and integrating IT governance and establishing an IT strategy, the alignment between IT and business should remain the key priority. But who exactly is responsible for maintaining this as a priority? The strategy process typically involves top management and board members only, whereas the tactical process typically involves mid-level management figures who are responsible for converting strategies into general business and IT-specific actions. The principles, goals, and assumptions that are the foundations of the strategy need to be passed onto the next level within the organization. The business needs and the interrelationship between these needs must be identified and aligned with the IT governance strategy. Knowledge gaps need to be filled and the organization's vision, mission, and business objectives understood by all those involved in setting up governance tactics.

Building a Team

To align business and IT, one obvious tactic is to start by fully understanding both business needs and abilities and IT needs and abilities. Although it sounds simple, understanding both business and IT needs is difficult as both areas can be quite complex and there are typically gaps in understanding from both sides. It is therefore critical to bridge business knowledge with IT knowledge early in the process. What does this look like in practice? In many cases, an IT strategy committee or an IT steering committee or council is formed to oversee IT governance. The two different types of committees have a slightly different emphasis: an IT strategy committee usually consists of higher executives within the organization and advises board members whereas a steering committee usually consists of busi-

ness and IT managers and focuses on delivering the actual strategy or action plans. Regardless of these differences, the main purpose of these formalized committees is to bring both business and IT together during the process of establishing IT governance. Many times, such committees will live on as perpetual bodies charged with the ongoing monitoring and revision of IT governance.

Establishing a Project Plan

The next task in implementing IT governance strategies is building a project plan, which includes a timeline, deliverables, and milestones, in accordance with the standard project management process. The focus here is on integrating IT processes with existing business processes and vice versa. A critical issue to identify early on is who within the organization has strategic IT decision-making authority. If relevant authorities are not supportive of the IT governance strategy, this will very quickly create issues when it comes to implementation.

A number of analytical tools may be applied at this stage of tactical planning such as strength, weakness, opportunity, and threat analysis (SWOT), balanced scorecard (BSC), and scenario analysis. The purpose of utilizing such tools is to optimize the alignment between IT and business based on the available information. The actual business to IT alignment process can be undertaken in various ways. The actual actions designed to align the business with this objective could include the following: (1) setting limits for the number of exceptions to architecture standards and baselines applied for and granted, (2) sourcing level of architecture customer feedback, and (3) establishing an evaluation mechanism where those project benefits realized can be traced back to the relevant IT architecture. Further planning efforts can then focus on ensuring that these actions are implemented.

Testing and Improving

To expand the input from sectors of the organization when establishing IT governance, utilizing agile methods, piloting methods, or other similar techniques can be used to get broad and quick participation from a variety of stakeholders. Agile methods typically involve developing small sections individually and releasing them as soon as feasible to stakeholders for testing. Piloting involves developing an incomplete product that can be shared with stakeholders for review and testing. Both of these techniques have the advantage of sourcing feedback quickly by getting products to stakeholders as soon as possible. In this context, these approaches can be used help to narrow down governance-related inclusions and exclusion criteria, source feedback, and identify mistakes very quickly. Why is this important? The idea is to develop IT governance with substantial input from business and IT sectors as well as major stakeholders as soon as possible. By releasing sections of the proposed IT governance framework in order to source feedback, participation in the feedback process is easier as stakeholders have something tangible to evaluate.

Expanding the Time Horizon

For the IT-business alignment to occur, one also needs to examine plans for the future. IT governance aims to enable the organization to realize its vision, which relates to how the organization is realistically operating in the future. As such, the process of developing a governance strategy should not be constrained by existing parameters, but rather make inclusions that could facilitate the creation of future opportunities as well. For example, technologies based on open concepts and open standards are much more flexible and can be more easily adapted for future applications, as opposed to proprietary technologies that may be popular at the time but are relatively static and inflexible.

Involving the Entire Organization

A critical area of IT governance that sometimes overlooked is human capital, that is, the actual people who will carry out the daily business of the organization. The capabilities, knowledge, skills, and experiences of individual employees and managers should be cultivated to facilitate IT-business alignment.

During the IT governance development and implementation process, the specific human resource requirements (including the necessary qualifications, skills, and experience of employees) should be examined. The recruitment of qualified employees, the retention of experienced employees, and the retraining of existing employees who lack necessary skills are three focus areas of knowledge management that warrant attention. Ultimately, an organization's success or failure will be dependent upon its workforce. Thus, in order for an organization to optimize their IT operations, developing skills, knowledge, and a culture of continuous learning must be addressed via IT human resource management.

In summary, once a strategy is determined and the organization knows "what" it wants to accomplish, the next step is to formulate corresponding tactics to address the question of "how" to accomplish the strategic objectives. Developing a tactical plan involves translating a strategy into actionable steps that pave the way towards the successful implementation of the strategy. Tactics such as forming management structures, aligning IT operations with business processes, and managing the learning, training, and knowledge sharing of employees, are all aimed at making IT governance an integral part of an organization's culture and positioning IT as a driver of business value that supports the organization's mission and strategic objectives.

2.4 Operation

The result of IT governance is ultimately reflected in the quality of services and products generated from IT operations. The operations are directed by tactics, which are based on the strategy. The relationship between strategy, tactics, and operations is illustrated below.

Figure 3: Strategy, Tactics, and Operations



Source: Created on behalf of IU (2019).

To understand how effective IT governance is in an organization, the organization needs to examine which goals and targets have been achieved and to what degree. In order to assess the effectiveness of IT governance, the organization needs to understand how its mission, strategic objectives, and drivers of business value are incorporated into actual operations and targets within the framework of IT governance. The focus needs to be on how to set operational targets, how to assess whether these targets have been reached, and how to improve outcomes in the future.

Below is some clarification for key terminology discussed in this section.

- “Mission” is the purpose for which an organization exists.
- “Objectives” are what an organization wants to achieve in order to support its mission.
- “Targets” are indicators established to establish the degree of achievement regarding objectives.
- “Goals” are indicators of whether or not objective has been achieved.

The main difference between targets and goals is that the targets are measurable, whereas goals have only a “yes-or-no” status. The following discussion focuses on targets and how they relate to operational performance.

There are different approaches that can be taken to translate an organization’s strategic objectives and business drivers into IT-specific objectives and targets. One widely-adopted path is that outlined by the framework COBIT, which involves examining control processes and formulating appropriate IT targets. As an IT governance framework, COBIT is not designed to be prescriptive but rather adapted by organizations to match their unique business objectives. Nevertheless, it can be utilized to provide some structure to the process of setting up IT governance in an organization.

COBIT defines three governance objectives: benefit realization, risk optimization, and resource optimization. These objectives can be translated into specific operational targets. For example, take the following operational target associated with benefit realization: deployment of a new ERP system should be complete within a three-month time frame, available to a target group of users in finance and budgeting and achieve a 90 percent level of satisfaction, with a targeted saving of 25 percent over the previous ERP system. Note that all of these parameters are measurable, meaning that the success of the deployment can be easily assessed. Another example of an operational target, this time

related to risk optimization, is as follows: Within the next year, the overall organizational IT resource availability should reach 99 percent. Here the target does not refer to a specific IT system such as an ERP system, rather it groups together all IT resources.

A different, more specialized method of establishing IT targets involves converting the concerns of different stakeholders into performance-related objectives and targets. For example, management may question whether IT costs are being managed effectively. The relevant target might then be: Improve the overall IT cost ratio by 30 percent over next two years. Another question raised by management might be whether IT risks are being identified and managed. The relevant target in this case might be: Identify major IT operations risks, categorize the severities, and establish mitigation plans within the next six months. The advantages of using this approach over the COBIT framework is that a more direct set of targets can be established that directly address the most relevant areas of IT performances in the eyes of key stakeholders.

Key Performance Indicators

In order to have more objective measures of the performance of IT operations, organizations need to utilize benchmarks and establish key performance indicators. Benchmarks indicate the performance of products and services relative to the best performers operating within the industry. That is, they allow an organization to measure their performance against unofficial standards of excellence established by leading organizations in a particular industry. Key performance indicators (KPIs) are measurable values that indicate the success of an organization's performance against predefined objectives. A simple example of a KPI that measures the performance of the IT incident escalation process as the number of incident escalations, possibly distinguishing between different types of incidents and levels of escalation. Since the absolute number of incident escalations can mean very different things depending on the total number of incidents, a far better KPI would be the percentage of incidents that were escalated.

As they relate to IT performance, KPIs are designed to answer the following questions:

- Are stakeholders expectations from IT being achieved?
- Are business goals being achieved?
- Are IT resources being utilized efficiently and to what degree?

KPIs as a governance mechanism ensure that stakeholder needs and conditions are formulated into organizational objectives. When utilized as a component of IT governance, KPIs facilitate the creation of directions that inform the organization's decision-making and prioritization; performance and compliance can then be monitored in relation to these directions.

KPIs and performance metrics are not only used to gauge how successful IT operations are but also for the purpose of making continuous improvements. The performance of an organization relative to its KPIs indicates the current status of an organization's IT operations. When these results are compared to industry-wide performance levels, any gaps

between the current performance level and that of leaders in the industry are revealed. In the framework of IT maturity model, KPIs are also useful to assess the current level of IT maturity in the organization and create related improvement objectives.

Regardless of whether the level of KPI attainment indicates deficiencies in IT operations or instead reflects the organization's desire to advance IT maturity levels, improving IT operations begins with the building blocks of IT operations: IT processes. A process is defined as "a set of interrelated or interacting activities that use inputs to deliver an intended result" (ISO/IEC 9001). The following figure is an example of an IT process related to incident escalation.

Figure 4: Incident Escalation Process



Source: Created on behalf of IU (2019).

Even the simplest of processes needs to have the basic elements seen in the previous figure: an input, an operation, and an output. Just like an IT system, an IT process has its own life cycle. Therefore, processes should not be viewed as static objects; they are always subject to assessment and continuous improvement. A process can be assessed in two ways: either according to its category or its capability. The process category relates to the type of governance that controls the process. For example, a process may belong to the benefit realization category or the risk management category.

The capability dimension provides a measure of a process's capability to meet an organization's current or planned business objectives for the process. Capability can be measured using various industry models and standards. The ISO/IEC 15504 standard has six levels of process maturity, from incomplete (level 0) to optimized (level 5). The Capability Maturity Model Integration model (CMMI), developed by CMMI Institute which became a subsidiary of ISACA in 2016, measures capability and maturity levels with different approaches. It views capability as an indication of an organization's performance and process improvement achievements in individual practice areas, and measures it in relation to four levels, from incomplete (level 0) to defined (level 3). CMMI also defines maturity as a staged path for an organization's performance and process improvement efforts, ranging from incomplete (level 0) to optimized (level 5).

What does this look like in practice? The following example describes how a process can be assessed. Let's say an IT security process has been implemented, but it has only achieved 50 percent of the desired security level. This outcome indicates that the process will need to be reengineered in order to reach the next target level which, in this case, is a 90 percent security level. The process is also implemented in an ad hoc manner. In order to advance to the next maturity level, the process will need improvement so that it can be

adequately managed via planning, monitoring, and adjustment. When we look at this example, we can see that the first part of this example focuses on process capability level and the second part focuses on process maturity level.

Improving processes requires one of the following three options: simple readjustment, partial redesign, or total reengineering. Reengineering is a radical measure that allows an organization to start from a blank slate because the previous process and its core operations are discarded. Reengineering focuses on the desired outcome, rethinking how to achieve the objectives, utilizing lessons learnt from previous designs, and making sure the new process aligns even closer with the objectives. In reality, not all reengineering starts from scratch. Typically, a new design will emerge from analyzing the previous process, retaining the parts of the previous process that are performing well, and replacing the underperforming parts of the process with a new design. The obvious risk associated with reengineering is that a new process might not actually achieve the primary objective which is to perform better than the previous process and meet a set of predetermined goals.

In summary, IT operations are carried out via IT processes, which generate desired outcomes and support the fundamental notion that IT operations contribute business value to an organization. IT operational performance provides critical feedback regarding the success of IT strategy implementation and therefore need to be evaluated regularly based on set goals and targets. Assessing IT processes using KPIs and making subsequent improvements to their processes to optimize IT operational performance is a core objective of IT governance.

2.5 Compliance

Compliance is the degree of conformity with established guidelines or specifications, or the fulfillment of official requirements. Compliance management is the process by which the state of compliance can be reached. Under the COBIT framework, compliance with relevant laws, regulations, contractual agreements, and internal policies is viewed as both an enterprise goal and IT-specific goal.

In order to ensure compliance, many organizations will have a specific compliance management system, which typically consists of three main components: board or management oversight, a compliance program, and compliance audit processes. Since top management is ultimately responsible for compliance, adopting policies and advocating for compliance, establishing compliance programs, and conducting periodic audits, are some of the critical administrative oversights and controls that a board and management typically exercise.

A compliance program usually consists of policies and procedures, monitoring, and training, and is an internal resource for the entire organization. A compliance audit is an independent review of an organization's compliance with laws and regulations, adherence to internal policies and procedures, and history of abiding by standards and following best

practices. An audit helps management to ensure ongoing compliance and identify compliance risk conditions. It is usually management that determines the scope and frequency of audits.

A key area of IT compliance pertains to IT-related law. IT laws provide the legal framework for collecting, storing, and disseminating electronic information. The most prominent among IT laws deal with data privacy and security. Different countries and regions have established legal frameworks and boundaries regarding information and computer and communication technologies. When dealing with IT compliance and related laws, organizations need to be very careful about where IT systems are located, where information is transmitted to and from (known as “data in transit”), and where it is stored (known as “data at rest”). It is the responsibility of organizations to understand under which jurisdiction and sovereignty the organization operates and therefore which IT-related laws are enforceable. We will now examine a few examples of major laws around the world that regulate IT operations, especially in the areas of information privacy and data protection.

- United States of America
 - Privacy Act 1974: This act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.
 - Electronic Communication Privacy Act (ECPA) 1986: This act updated government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer, and added new provisions prohibiting access to stored electronic communications.
 - Health Insurance Portability and Accountability Act (HIPAA) 1996: This act requires the establishment of standards for the electronic exchange, privacy, and security of health information.
 - Gramm-Leach-Bliley Act 1999: This act requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.
 - Federal Information Security Modernization Act (FISMA) 2014: This act provides several modifications that modernize Federal security practices to address evolving security concerns.
 - Other laws in the United States of America that contain IT-related legal requirements include the Foreign Intelligence Surveillance Act (FISA) 1978, the Sarbanes–Oxley (SOX) Act 2002, the Homeland Security Act 2002, and the Intelligence Reform and Terrorism Prevention Act 2004.
- European Union
 - General **Data Protection** Regulation (GDPR) 2018: This law provides regulations on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.
- Canada
 - Personal Information Protection and Electronic Documents Act (PIPEDA) 2000: This act governs how private sector organizations collect, use, and disclose personal information in the course of commercial business.
- India
 - Information Technology Act 2000: This is the primary law in India that deals with cybercrime and electronic commerce.

Data Protection
protection of individuals
(not data!) from inadequate use of their personal data

In addition to laws, many countries publish regulations that are based on laws but supplemented with detailed interpretations. Regulations further extend the laws into actionable items. Regulations are typically issued by regulatory entities that have been charged with the task of implementing the laws. Some regulations are established by industry associations. For example, Basel III is a set of international banking regulations developed by the Basel Committee on Banking Supervision to facilitate stability in the international financial system.

IT-related standards are frequently used as criteria for compliance. There are various standard organizations that have been recognized as leading authorities in different areas of the IT industry. The following are examples of such organizations:

- The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have a large number of standards specific to IT governance and compliance that have been widely adopted.
- The Institute of Electrical and Electronics Engineers (IEEE) is a professional association which has a long history of establishing IT hardware standards.
- The National Institute of Standards and Technology (NIST), originally a physical sciences laboratory, is a non-regulatory agency of the United States Department of Commerce. NIST has published a number of IT standards that are used extensively in the United States.

Some of the commonly adopted best practice frameworks for IT governance, risk management, and compliance include the following:

- COBIT, published by ISACA
- Information Technology Infrastructure Library (ITIL) by the Office of Government Commerce (OGC) in United Kingdom and now by AXELOS
- Capability Maturity Model Integration (CMMI) by the CMMI Institute/ISACA
- ISO/IEC 38500, ISO/IEC 17799, ISO/IEC 20000 and 27001
- Basel III Accord by Basel Committee on Banking Supervision

In addition to these IT-specific frameworks, the Project Management Body of Knowledge (PMBOK) by Project Management Institute (PMI) and PRojects IN Controlled Environments (PRINCE2) by AXELOS/OGC provide structured project management methodologies that are standard approaches used in IT project management.

IT compliance often overlaps with other areas of compliance within an organization. IT compliance can be addressed under the umbrella of IT governance, but also under general organization compliance. Regardless how it is structured in an organization, IT compliance must work closely with the IT governance system as well as general and IT-specific risk management systems.

2.6 Performance

As part of IT governance, monitoring IT performance provides feedback about the alignment of IT and business. Monitoring IT governance and the delivery of operations are necessary to ensure that IT governance is indeed aligned to the organization’s business objectives. The benefits of such monitoring include making the contribution of IT to business value explicit, ensuring the efficiency of IT resource allocation, and keeping tabs on the effectiveness of IT activities. By measuring IT performance, i.e., the effectiveness, efficiency, quantity, and quality of IT operations, an organization can identify the areas that need improvement as well as gauge the capability and maturity levels of various IT operations. Performance measurement related to IT governance involves tracking and monitoring IT strategy implementation, IT resource utilization, IT risk management, and IT process performance and service delivery. IT governance performance is measure in an aggregated fashion, i.e., the focus is on the overall IT system rather than individual IT operations.

Measuring IT performance is done through monitoring and auditing. Monitoring is the ongoing process of ensuring that operations (or other governance items) are working as designed and intended. Monitoring is effective control over an operation while in action. Monitoring is typically carried out by an operations team and often unstructured. Monitoring utilizes similar methods and tools to auditing and the outcome of monitoring is often auditing. The ISACA defines an audit as a “formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met” (ISACA, n.d.). Auditing is a formal, systematic, and disciplined approach to evaluating and improving the effectiveness of processes and related controls for performance and is governed by predefined standards and usually carried out by individual who is independent from operations to ensure objectivity in reporting. Auditing is a validation measure that involves examining the performance history of a process or other governance items. Thus, if there is little or no history of a specific operation, then there is nothing to audit but rather something to monitor.

Because of the distinction between monitoring and auditing, an organization can use these two measuring methods to achieve different purposes. Monitoring allows the entire organization, from the board to management to operations, to have real time performance views from different perspectives, therefore facilitating control mechanisms to exercise modifications, corrections, adjustments, improvements, and optimizations in real-time. Monitoring is one of the key control objects within the COBIT framework which considers monitoring an IT governance function. An example of monitoring IT services is illustrated in the following table.

Table 2: Monitoring IT Services

IT-Related Goal	Related Metrics
Delivery of IT services in line with business requirements	<ul style="list-style-type: none"> • Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets established service levels • Percent of users satisfied with the quality of IT service delivery

Source: Created on behalf of IU (2019).

In order to accurately measure IT governance performance, performance indicators attached to IT processes have to be properly defined. As discussed earlier, key performance indicators (KPIs) measure whether an IT process is achieving its designed business requirements. For example, delivery of IT services with respect to business requirements, IT strategy decision-making, delivery of IT projects on time, on target, and on budget, ROI on IT investments, and IT budget transparency are all closely associated with IT-business alignment.

One problem that can occur with the use of KPIs is that there may not be any relationship between different KPIs, as each KPI provides its own individual results. In the case that there are a significant number of KPIs, measuring these KPIs simultaneously can become extremely complex and it can be difficult to reach meaningful conclusions. To help monitor and measure IT performance without becoming overwhelmed by the large amount of individual measurement data, an organization may benefit from organizing KPIs into sensible metrics, as in the case of the balanced scorecard (BSC). The BSC was originally introduced to expand the evaluation of an organization beyond traditional financial analysis to include customer satisfaction, internal processes, and the ability to innovate (Kaplan & Norton, 1992). This concept has been adopted by the IT industry to evaluate IT performance and is included in the COBIT framework.

The fundamental idea behind the BSC is that, while finance is integral to an organization's success, it only measures historical success; financial reporting alone can't illuminate the future performance of the business. To better understand the current standing of a business and transform that understanding into a gauge of future success, the BSC measures strategic performance. But strategy isn't necessarily something that can be easily translated into numbers and metrics. The main objective of the BSC is therefore to translate the business mission and strategy into tangible objects that can be measured and prioritize which of these measurements are most meaningful.

The BSC focuses on four areas of performance: finance, customer satisfaction, internal business processes, and learning and growth. There are some other variations of these four BSC dimensions, however the COBIT framework follows these original dimensions:

1. The finance dimension tracks financial requirements and performance.
2. The internal business dimension measures critical customer process requirements.
3. The customer dimension measures the satisfaction and performance requirements of customers for products or services.
4. The learning and growth dimension measures an organization's learning culture and expectations of its employees, the growth in employee knowledge, and the business competitiveness that is a consequence of the organization's focus on learning and growth.

The BSC offers a more holistic and hence "balanced" approach to measuring IT performance. It has the flexibility to cater for specific business objectives which means an organization must decide how to utilize the BSC in the most beneficial way given its unique busi-

ness model. The COBIT framework provides two sets of BSC recommendations: one for enterprise level goals and one for IT goals. An example of the BSC being used for enterprise goals is illustrated in the following figure.

Table 3: COBIT BSC for Enterprise Goals

BSC Dimension	Enterprise Goal
Financial	<ol style="list-style-type: none"> 1. Stakeholder value of business investments 2. Portfolio of competitive products and services 3. Managed business risk (safeguarding of assets) 4. Compliance with external laws and regulations 5. Financial transparency
Customer	<ol style="list-style-type: none"> 6. Customer-oriented service culture 7. Business service continuity and availability 8. Agile responses to a changing business environment 9. Information-based strategic decision making 10. Optimization of service delivery costs
Internal	<ol style="list-style-type: none"> 11. Optimisation of business process functionality 12. Optimisation of business process costs 13. Managed business change programmes 14. Operational and staff productivity 15. Compliance with internal policies
Learning and Growth	<ol style="list-style-type: none"> 16. Skilled and motivated people 17. Product and business innovation culture

Source: Created on behalf of IU (2019).

Since the BSC is specific to each organization that utilizes it, there is no one format, style, or set of KPIs that will fit all organizations. In order to custom-build a useful measurement of IT performance using the BSC and related KPIs, the following guidelines are considered good practice:

1. Provide an objective measure of strategy alignment.
2. Take a holistic view of all BSC dimensions.
3. Provide historical comparisons of performance change over time.
4. Analyze scorecard results from a forward-looking perspective.
5. Focus on key objectives and the ways to improve.
6. Communicate with clear and unambiguous language.

The timing and frequency of monitoring and measuring IT performance should not be arbitrary, it needs to reflect the specific IT and business operations in conjunction with the IT governance. The purpose of monitoring and measuring is ultimately to better align IT operations and business strategy. The results of this type of analysis should therefore be studied not only to improve performance but also to gauge the maturity level of the business. The entire process should follow the life cycle model, moving through cycles of analysis, design, implementation, review, and improvement.

The second aspect of IT governance related to measuring IT performance is auditing. An audit is “a formal inspection and verification” (ISACA, n.d.) to validate conformity. In the context of performance, auditing is aimed specifically at identifying whether IT control goals are being reached. The typical auditing process consists of three phases: the planning phase, the fieldwork phase, and the reporting phase.

- a) Planning phase
 1. Determine the audit subject by identifying what needs to be audited, e.g., a communication system or back-up process.
 2. Define the audit objective by identifying the specific purpose of the audit, e.g., examining whether the ERP system performs as designed.
 3. Establish the audit scope by defining the actual auditing actions, e.g., the scope limits the audit to the ERP system security functions only.
 4. Perform pre-audit planning by organizing the audit, covering areas such as discovery, risk assessment, compliance requirements, etc.
 5. Determine audit procedures by laying out the detailed procedures and steps to be taken.
- b) Fieldwork phase
 1. Acquire data by going through the auditing subject using the established procedure.
 2. Test controls using various tools and instructions and record the results.
 3. Discover issues and validate compliance.
 4. Organize data and document results.
- c) Reporting phase
 1. All discoveries and conclusions are organized into the required reporting format.

IT auditing provides evidence of whether the performance of IT operations has met the goals of IT governance. An audit will not only identify areas for improvement but also highlight aspects of IT performance that are performing well and warrant credit. Auditing is typically conducted on a predefined schedule, e.g., annually, or triggered by a specific event, e.g., a compliance process.

The effectiveness of IT governance, strategy, and operations can only be assessed through adequate performance reviews, i.e., through performance monitoring and auditing. Although monitoring and auditing have different purposes and work according to different methods, together both can provide the necessary measurements to determine the success of IT performance, indicate the degree of IT and business alignment, and identify where and how to improve and to mature that alignment.



SUMMARY

Establishing IT governance is similar to any other IT project, with different stages that, together, form a project life cycle. The process begins with a full assessment of current IT operations within the organization to establish a baseline. Next, a solid understanding of the organization's vision, mission, and strategic objectives is required in order to formulate

an IT governance that is in alignment with the organization's core business. Other topics that need to be considered are compliance and risk management, which must be integrated into IT governance.

To measure the effectiveness of IT governance and related strategies, all IT operations need to be monitored and periodically audited. The outcomes will not only help to assess the success or the lack of it, but it will also provide ways to improve and to mature IT governance. IT governance is a complex framework with many components working together. The governance must be adopted, as well as adapted, in order to gain the optimum benefits from it.

Information technology is a fast moving train, therefore its governance must also reflect the evolving nature as well. Establishing IT governance represents a continuous journey towards better alignment between IT and business, and a better value generator for organizations. IT governance improvement and maturity should be constantly kept in mind by both business and IT leadership.

UNIT 3

THE COBIT FRAMEWORK

STUDY GOALS

On completion of this unit, you will have learned ...

- the principles of COBIT.
- how to use the COBIT goals cascade.
- how to properly deploy COBIT.

3. THE COBIT FRAMEWORK

Introduction

IT governance is the link between an organization's strategic mission and objectives and its IT-related strategy. There are several governance frameworks that support the establishment and continuous improvement of IT governance in an organization. These include the Control Objectives for Information and Related Technologies (COBIT), the International Standard for Corporate Governance of Information Technology (ISO/IEC 38500), the Information Technology Infrastructure Library framework (ITIL), and the Capability Maturity Model Integration program (CMMI). Of these frameworks, only COBIT and ISO/IEC 38500 cover IT governance completely, while the other two focus on certain aspects of IT governance. Since COBIT is used far more widely than ISO/IEC 38500, this unit will focus on COBIT as a framework for IT governance.

COBIT has been widely recognized by the global IT community as a broad-ranging, standard agnostic and, more importantly, standard inclusive framework for IT governance. In other words, COBIT provides a framework for the entire IT organization. The organization may then decide to add other standards such as ITIL or PRINCE to provide more detail for selected topics, and "slot in" these standards into the COBIT framework. COBIT provides a collection of components and tools that can be used to establish and sustain sound IT governance within an organization. COBIT is published by the ISACA association, which originally stood for "Information Systems Audit and Control Association" but the association now only goes by its acronym. Originally, when COBIT was published in 1996 as the "Control Objectives for Information and Related Technology", it defined the criteria to be used by financial auditors when auditing the IT component of companies. Over the years, the framework has moved from strictly an auditing tool to a framework for IT governance. When COBIT 5 was published in 2012, the original name was dropped and now only the acronym "COBIT" is used. Over the years, in particular following the publication of version 5, COBIT has become the de facto standard for IT governance and is now used by a significant part of IT industry.

3.1 Overview of COBIT

At the end of 2018, initial documents from the new version of COBIT, known as COBIT 2019, were released, replacing the former version of COBIT, known as COBIT 5, originally released in 2012. As it will take several years for this new version to become widely used, the following exploration of the framework will address both COBIT 5 and COBIT 2019.

The core of COBIT 2019 is described in the two documents which are available to registered users from the ISACA web site: COBIT 2019 Framework: Introduction & Methodology and COBIT 2019 Framework: Governance and Management Objectives.

The main goal of this new version of COBIT is to focus even more on the business and value delivery view of IT and IT governance. This is reflected in the description of COBIT 2019 as a framework for the enterprise governance of information and technology (EGIT), as compared to the description of COBIT 5 as a framework for the governance of enterprise IT (GEIT). COBIT also no longer talks about information technology (IT), but about information and technology (I&T) to emphasize its wider scope. Additional reasons for releasing a new version of COBIT include the need to keep up with new technologies, in particular agile development and **DevOps**, and the need to revise content in keeping with new versions of other standards referenced in COBIT.

DevOps

approach used to ensure and support close cooperation between development and operations

COBIT is a framework for the governance and management of enterprise information and technology, aimed at the whole enterprise. Enterprise I&T means all the technology and information processing the enterprise puts in place to achieve its goals, regardless of where this happens in the enterprise. In other words, enterprise I&T is not limited to the IT department of an organization, but certainly includes it (ISACA 2019, p. 13).

Because COBIT is designed to be broad and generic, it can be utilized by all types of organizations, from commercial to non-profit to governmental entities. COBIT defines the components that should be used to establish I&T governance and sustain good practices and provides organizations with a collection of guidelines and tools. However, COBIT does not prescribe IT decisions, nor does it describe the entire I&T environment or management of all technologies. Instead, COBIT provides guidance to assist organizations to make optimal decisions based on their mission and business strategies.

COBIT principles

COBIT 5 was based on the following five principles:

- meeting stakeholder needs
- covering the enterprise end-to-end
- applying a single integrated framework
- enabling a holistic approach
- separating governance from management

COBIT 2019 extends these principles and distinguishes between governance system principles and governance framework principles. While the governance system principles are slightly updated versions of the COBIT 5 principles, the governance framework principles describe the idea that COBIT goes beyond being a framework itself and should be now used to set up an enterprise's own governance framework.

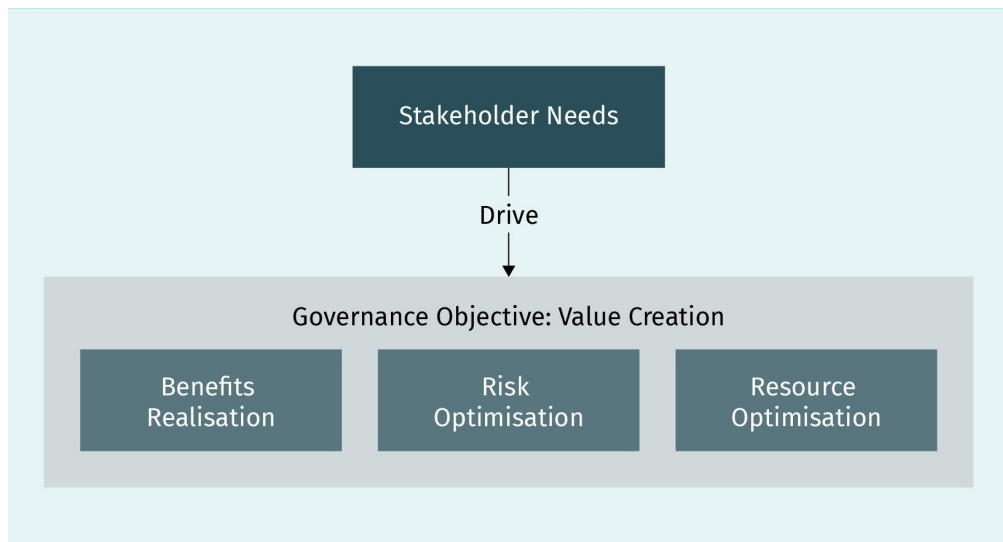
Governance System Principles

Governance system principle 1: Provide stakeholder value

The main reason for an enterprise to exist and therefore COBIT's main governance objective is to support organizations to meet their mission and provide value for their stakeholders. All I&T activities must therefore support the organization's mission through bene-

fit realization, risk optimization, and resource optimization, which COBIT treats as key stakeholders' needs. COBIT makes this principle its first, emphasizing that the first principle of I&T is to support the organizational mission and business value creation.

Figure 5: Main Outcomes from EGIT



Source: Created on behalf of IU (2019).

Value creation means realizing benefits at an optimal resource cost while optimizing risk. Note that COBIT does not discuss minimizing risks but rather optimizing them. Minimizing the risks of I&T in many cases would require eliminating I&T altogether, since any form of I&T involves risk. To access the benefits of I&T, an organization has to accept certain inherent risks; the objective is to find the best balance between accepting risks and achieving the benefits of I&T.

Governance system principle 2: Holistic approach

I&T is an integral part of the overall organization business machinery, and even within I&T, there are many interconnected components. Thus, efficient and effective I&T governance requires a holistic view that takes into account of all the interacting technology and business components.

Governance system principle 3: Dynamic governance system

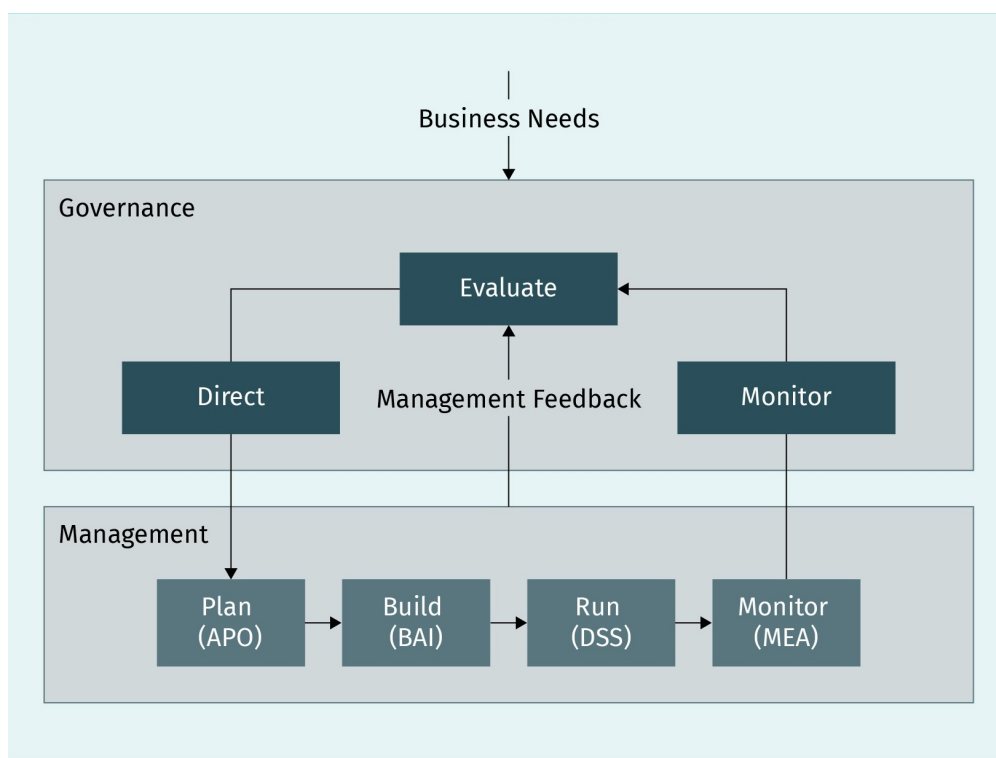
Whenever one of the relevant factors, e.g., design factors, is changed, the governance system should be checked and adapted as necessary.

Governance system principle 4: Governance distinct from management

The COBIT framework makes a clear distinction between I&T governance and I&T management, even though the two are closely linked. The reasons are that governance and management serve different purposes, cover different types of activities, require different

organizational structures, and are executed by different processes, roles, and knowledge. COBIT (2018, p.10) defines governance as ensuring “that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision-making; and monitoring performance and compliance against agreed-on direction and objectives.” COBIT defines management as the organizational structure that “plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives” (2018, p.10). In the following figure, we can see how COBIT recognizes the relationship between governance and management but defines them as separate business structures. COBIT links three key tasks with governance: evaluation, direction, and monitoring, and management with four key tasks: planning, building, running, and monitoring.

Figure 6: COBIT Governance and Management Domains



Source: Created on behalf of IU (2019).

Governance system principle 5: Tailored to enterprise needs

The governance system needs to be **tailored** to the specific needs of the enterprise, rather than strictly following COBIT (or any other reference model). Since each enterprise has its unique mission, it should customize COBIT to match into its own environment. The main tool that facilitates this is the goals cascade, a key concept of COBIT that helps organizations to translate high-level stakeholder drivers and needs into manageable and specific governance and management objectives.

Tailoring
 adapting a general framework to a specific environment or organization

Governance system principle 6: End-to-end governance system

COBIT integrates I&T governance into the enterprise's umbrella governance to cover all functions and processes within the entire enterprise. In other words, COBIT does not focus on I&T governance in isolation but treats information and related technologies as enterprise assets that need to be addressed just like any other enterprise assets that the entire enterprise relies on.

Governance Framework Principles

Governance framework principle 1: Based on conceptual model

An enterprise governance framework should be described in terms of defined entities and their relationship in order to achieve a consistent framework and allow for automation.

Governance framework principle 2: Open and flexible

Once an enterprise has defined its governance framework, it should keep this up to date. In order to update the framework as needed, it must be flexible and open to changes.

Governance framework principle 3: Aligned to major standards

COBIT is an inclusive framework that aligns itself with other major standards and reference models. Other standards and frameworks can be mapped onto key areas of COBIT governance and management activities and used in combination with COBIT, providing additional details on their respective application area.

Governance System Components

A governance system is built from various components such as processes and organizational culture. In combination, these components help to satisfy the principles thus described. COBIT 2019 defines the following set of components, which replace the “enablers” of COBIT 5:

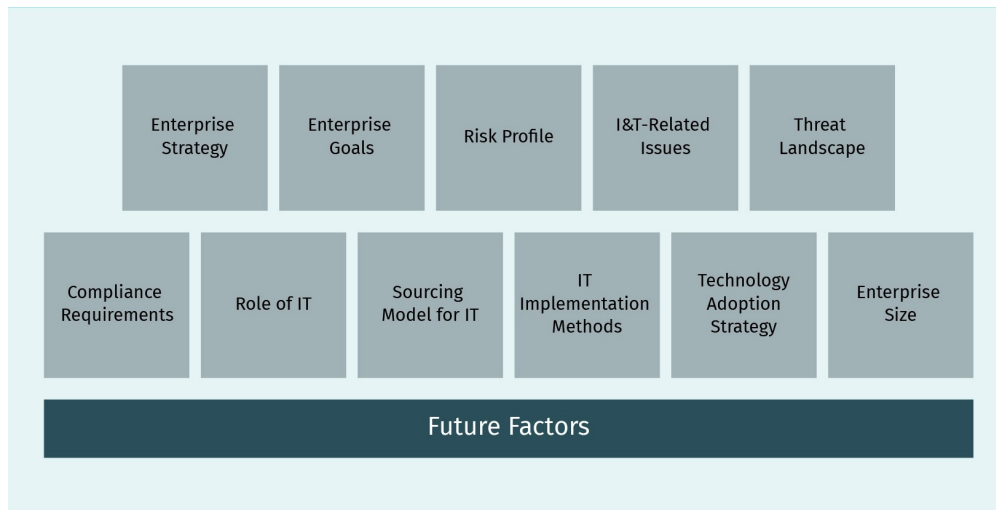
- processes
- organizational structures
- information flows and items
- people, skills, and competencies
- principles, policies and frameworks
- culture, ethics, and behavior
- services, infrastructure, and applications

We can see how the governance system components operate in practice with the following examples. To help provide stakeholder value (governance system principle 1), the enterprise needs to define suitable processes such as including suitable stakeholder feedback loops into the software development process. To establish governance distinct from management (governance system principle 4), a clear distinction between governance and management roles in the organizational structure needs to be created.

Design factors

COBIT 2019 defines a set of design factors that influence the design of an enterprise's governance system, as seen in the following figure.

Figure 7: COBIT 2019 Design Factors



Source: Created on behalf of IU (2019).

When setting up a governance system, an enterprise should analyze these design factors and identify their impact on the governance system. For example, the design factor “enterprise strategy” is concerned with the general strategy the enterprise uses to be successful and its effects on I&T. COBIT 2019 distinguishes the following strategy archetypes:

- growth/acquisition
- innovation/differentiation
- cost leadership
- client service/stability

The strategy selected by an enterprise will of course also affect the expectations on I&T and therefore the focus of the I&T governance system, the purpose of which is to support the enterprise and its strategy.

Focus areas

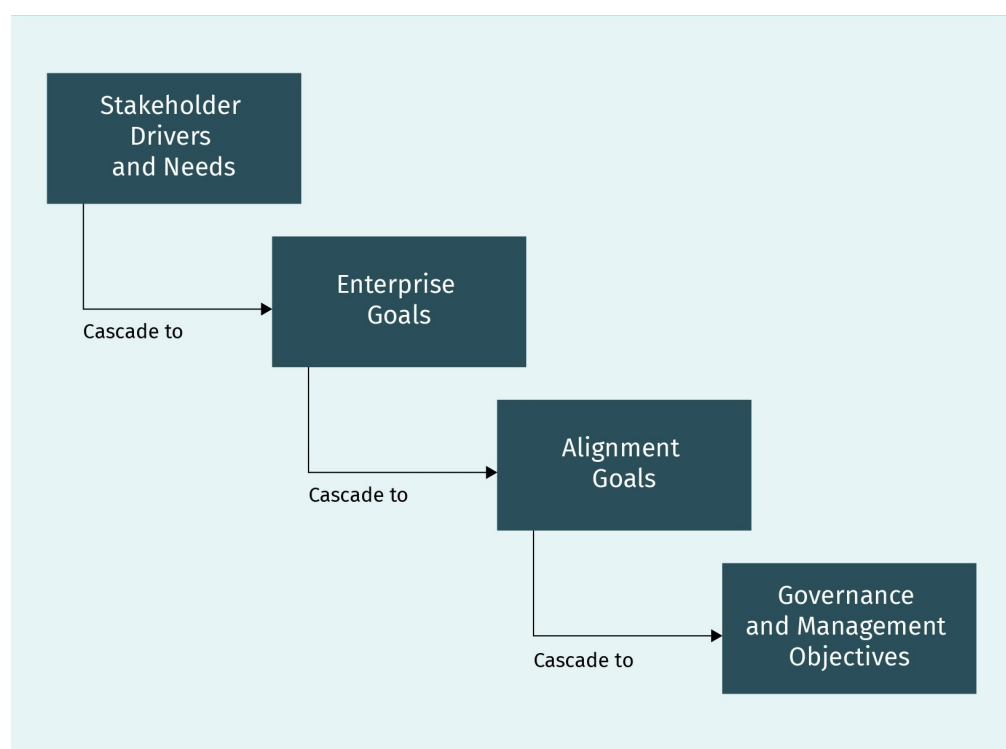
Focus areas are a new concept introduced in COBIT 2019 and describe different topics or domains to be addressed by I&T governance. The model does not contain a predefined set of focus areas but instead provides examples (including small and medium enterprises, cybersecurity, cloud computing, and privacy) and explicitly points out that new focus areas may be added as required.

3.2 The Goals Cascade

One of the key concepts in the COBIT framework of governance is the goals cascade. The goals cascade is a unique logical relationship structure of COBIT which aligns different governance components in a logical pattern. The fundamental concept is to translate stakeholder needs, positioned at the top of the goals cascade, into practical, actionable, specific, and customizable goals within the context of I&T governance and management. Through the cascading process, organizations define goals, stakeholder drivers, and needs at different levels, moving step-by-step down to governance and management objectives. The goals cascade was an existing part of COBIT 5 but the following description refers to the revised goals cascade included in COBIT 2019.

The COBIT goals cascade starts with stakeholder drivers and needs, the core of which is value creation (which in this case means realizing benefits at an optimal resource cost while optimizing risk). These stakeholder drivers and needs can be broken down, which then lead to enterprise goals. These are then further broken down, leading to alignment goals, which are then once again broken down into governance and management objectives. This series of cascading goals is illustrated in the following figure.

Figure 8: COBIT 2019 Goals Cascade



Source: Created on behalf of IU (2019).

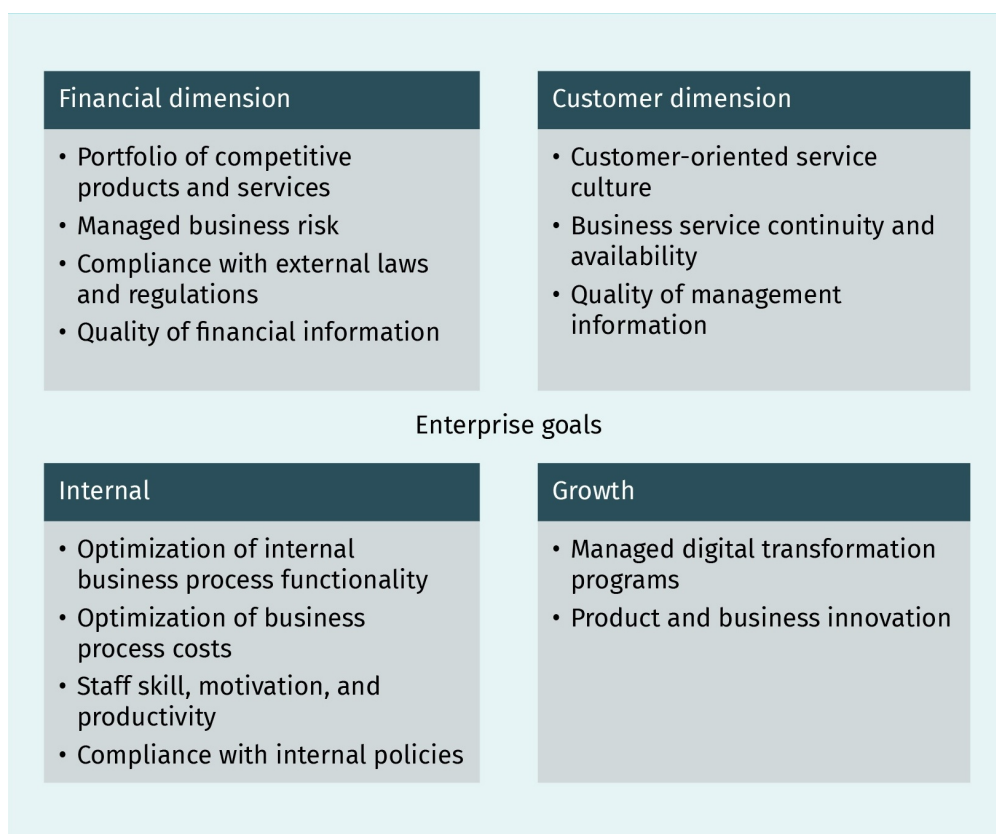
Stakeholder Drivers and Needs

To use the COBIT goals cascade an enterprise needs to first identify its stakeholder drivers and needs. For example, a bank may conclude that its main stakeholders are shareholders, employees, customers, and regulatory bodies. Combining the drivers and needs for these different groups results in the identification of stakeholder drivers and needs such as providing benefit via useful services to customers and optimizing the risk of unpaid loans.

Enterprise Goals

For the next step, COBIT provides a list of 13 predefined enterprise goals seen in the following figure. The task of the enterprise is to interpret and prioritize these enterprise goals, based on the stakeholder drivers and needs. In the following figure, we can see that the enterprise goals have each been assigned to a dimension of the balanced scorecard.

Figure 9: Enterprise Goals



Source: Created on behalf of IU (2019).

Enterprise Goals and Alignment Goals

The enterprise goals (EG) defined in COBIT cascade into alignment goals (AG). This type of goal focuses on the alignment of I&T efforts with the business objectives. As for enterprise goals, a set of metrics is defined for each alignment goal in order to measure the achievement of these goals. The following table lists the enterprise goals and related alignment goals defined in COBIT 2019.

Table 4: Enterprise Goals and Alignment Goals as Defined in COBIT 2019

BSC Dimension	EG Identifier	Enterprise Goal	AG Identifier	Alignment Goal
Financial	EG01	Portfolio of competitive products and services	AG01	I&T compliance and support for business compliance with external laws and regulations
Financial	EG02	Managed business risk	AG02	Managed I&T-related risk
Financial	EG03	Compliance with external laws and regulations	AG03	Realized benefits from I&T-enabled investments and services portfolio
Financial	EG04	Quality of financial information	AG04	Quality of technology-related financial information
Customer	EG05	Customer-oriented service culture	AG05	Delivery of I&T services in line with business requirements
Customer	EG06	Business service continuity and availability	AG06	Agility to turn business requirements into operational solutions
Customer	EG07	Quality of management information	AG07	Security of information, processing infrastructure and applications, and privacy
Internal	EG08	Optimization of internal business process functionality	AG08	Enabling and supporting business processes by integrating applications and technology
Internal	EG09	Optimization of business process costs	AG09	Delivering programs on time, on budget, and meeting requirements and quality standards
Internal	EG10	Staff skills, motivation, and productivity	AG10	Quality of I&T management information
Internal	EG11	Compliance with internal policies	AG11	I&T compliance with internal policies

BSC Dimension	EG Identifier	Enterprise Goal	AG Identifier	Alignment Goal
Growth	EG12	Managed digital transformation programs	AG12	Competent and motivated staff with mutual understanding of technology and business
Growth	EG13	Product and business innovation	AG13	Knowledge, expertise, and initiatives for business innovation

Source: Lane, 2014.

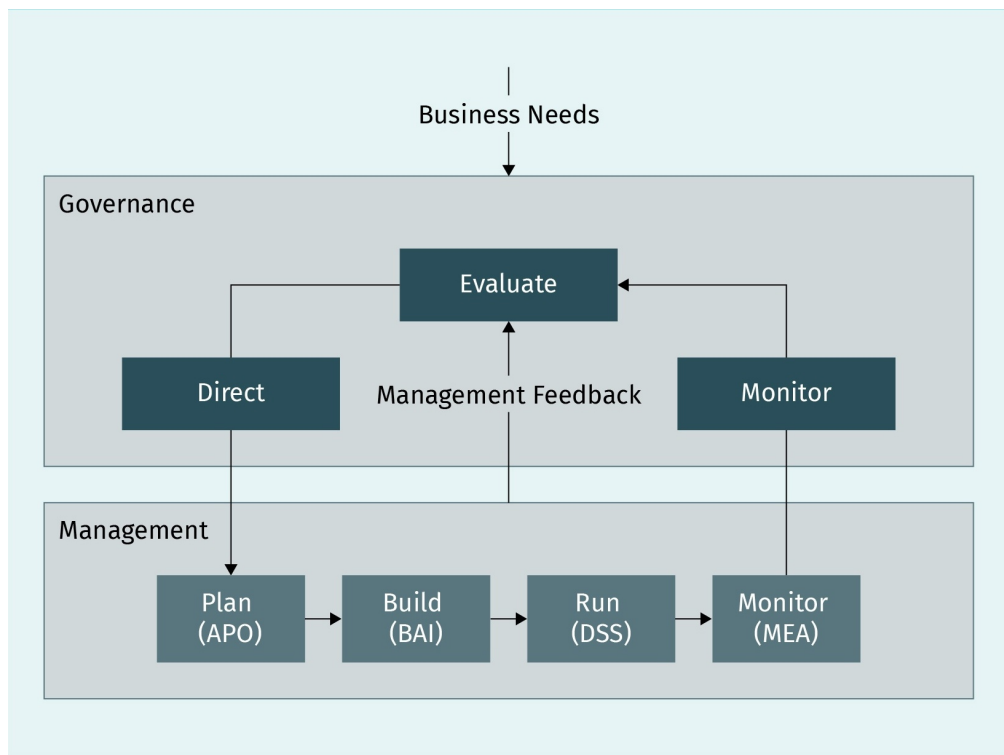
Governance and Management Objectives

The governance and management areas form the lowest level of the goals cascade as defined in COBIT 2019. Objectives are categorized into governance or management domains:

- Evaluate, Direct, and Monitor (EDM) (governance domain)
- Align, Plan, and Organize (APO) (management domain)
- Build, Acquire, and Implement (BAI) (management domain)
- Deliver, Service, and Support (DSS) (management domain)
- Monitor, Evaluate, and Assess (MEA) (management domain)

We can see the relationship between these objectives and domains in the following figure from COBIT, which extends the common IT management structure of plan-build-run to incorporate objectives from the governance domain and links these with business needs and management feedback.

Figure 10: Separation of Governance and Management

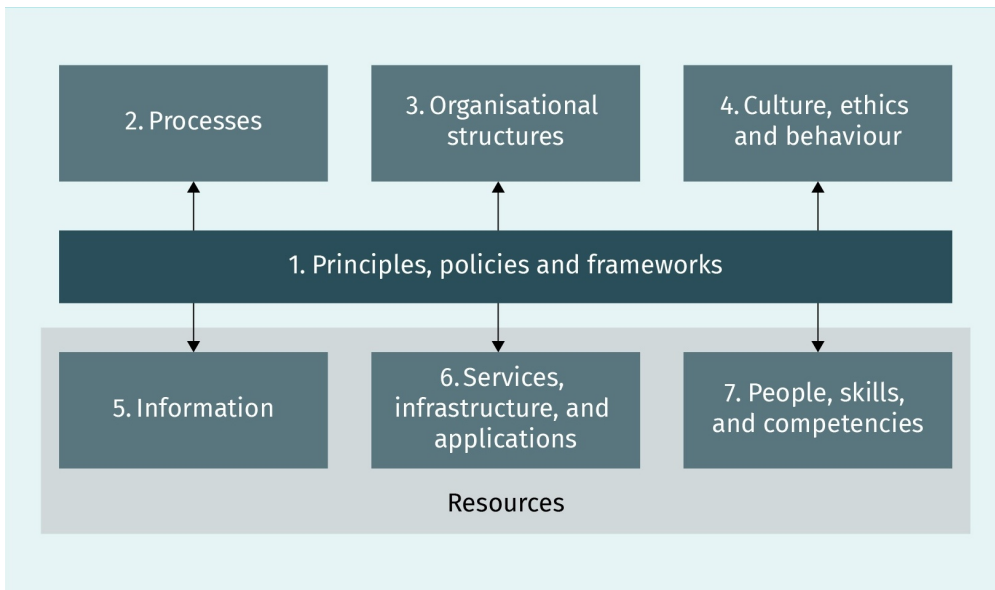


Source: Created on behalf of IU (2019).

Enablers and Processes in the Goals Cascade as Defined by COBIT 5

COBIT 5 is still widely used so an overview of the main concepts used in that model version is warranted. The lowest level of the COBIT 5 goals cascade consisted of so-called enabler goals rather than the COBIT 2019 governance and management objectives. Enablers were defined as the seven components (shown in the following figure) that enable the enterprise to achieve its goals.


Figure 11: COBIT 5 Enablers



Source: Created on behalf of IU (2019).

In practice, processes were the most important of these enablers and are thus structured into the five domains that COBIT 2019 uses to structure governance and management objectives. The processes themselves were revised and rephrased as objectives. For example, the process “APO01 Manage the IT Management Framework” was converted into the objective “APO01 Managed I&T Management Framework.” COBIT 5 included a process reference model which was replaced by the reference model of governance and management objectives thus described which also includes some of the core contents of the other COBIT 5 enablers.

The following table compares the main concepts and terminology of COBIT 5 with its successor COBIT 2019. This is not to suggest that the COBIT 2019 concepts listed here replace in full the relevant COBIT 5 concepts, rather they roughly cover the same topic.

 COBIT 5 AND COBIT 2019 COMPARISON	
COBIT 5 Concept	COBIT 2019 Concept
Governance principle	Governance system principle Governance framework principle
Enabler	Governance component
Process reference model	Core model

COBIT 5 Concept	COBIT 2019 Concept
Process (as part of the process reference model)	Governance and management objective
Goals cascade: <ul style="list-style-type: none"> • Stakeholder needs/mission • Enterprise goals • IT goals • Enabler goals 	Goals cascade: <ul style="list-style-type: none"> • Stakeholder drivers and needs • Enterprise goals • Alignment goals • Governance and management objectives

Applying the COBIT 2019 Goals Cascade

Applying the goals cascade requires a thorough understanding of the enterprise as well as the setup of the cascade itself. The following example is included to illustrate how this process can actually occur in practice. Let's assume that one of the stakeholder needs is: "Become a leader in next generation robotics." This may lead to various enterprise goals, including the COBIT Enterprise Goal EG01 "Portfolio of competitive products and services." This general goal might then be translated into the more specific enterprise goal: "Penetrate three key vertical robotics markets in the next five years". To support the implementation of this enterprise goal, COBIT recommends the use of suitable metrics and lists a set of such metrics for each enterprise goal. In the case of EG01, COBIT includes the metric "time-to-market for new products and services." In the current example, this could be translated into the more specific metric "time-to-market for new robotics products." This specific metric could therefore be set up and monitored regularly.

In the next step, the enterprise goal is cascaded to the COBIT Alignment Goal AG01 "I&T compliance and support for business compliance with external laws and regulations." Again, this general goal should be translated into a more specific alignment goal such as "satisfying I&T legal and other compliance requirements regarding robotics for three key vertical robotics markets". Again, COBIT recommends the use of suitable metrics to monitor progress towards this alignment goal such as the "number of IT-related noncompliance issues reported to the board or causing public comment or embarrassment". In the specific example, it might be helpful to limit this metric to robotics. The next step is to further cascade this alignment goal into governance and management objectives, based on the COBIT core model.

This example demonstrates how the entire COBIT goals cascade can be completed, moving from stakeholder needs to enterprise goals, then alignment goals, and finally to governance and management objectives. This is the main pathway to build up COBIT I&T governance, going from needs to implementation. The key advantage of the COBIT goals cascade is that it allows stakeholder needs to be transformed into practical, actionable, specific, and customizable goals within the context of I&T governance. Using the cascading process, organizations can define relevant and tangible goals at different organiza-

tional levels, from the enterprise level right down to implementation. Because of these cascading stages, organizations can set priorities for implementation and improvement with goals that are explicit and clear to specific levels.

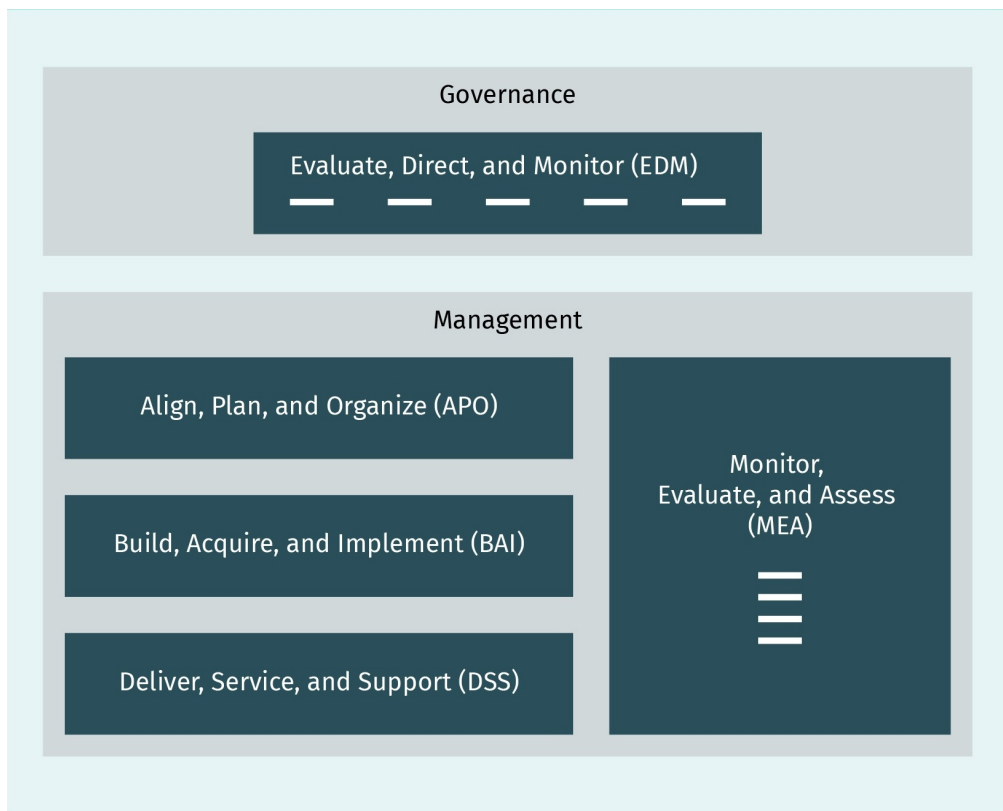
It is important to remember that COBIT is a framework, not a prescription. This means that during the process of adapting the goals cascade for a specific organization, there is no universal map that dictates how this should occur. Organizations must be very careful when comparing and mapping their unique business missions, objectives, and operational environment into various goals and enablers. While COBIT does provide generic metrics for the different levels of goals, these need to be carefully customized to best suit each organization's specific business.

3.3 The COBIT Governance and Management Objectives

The COBIT Core Model

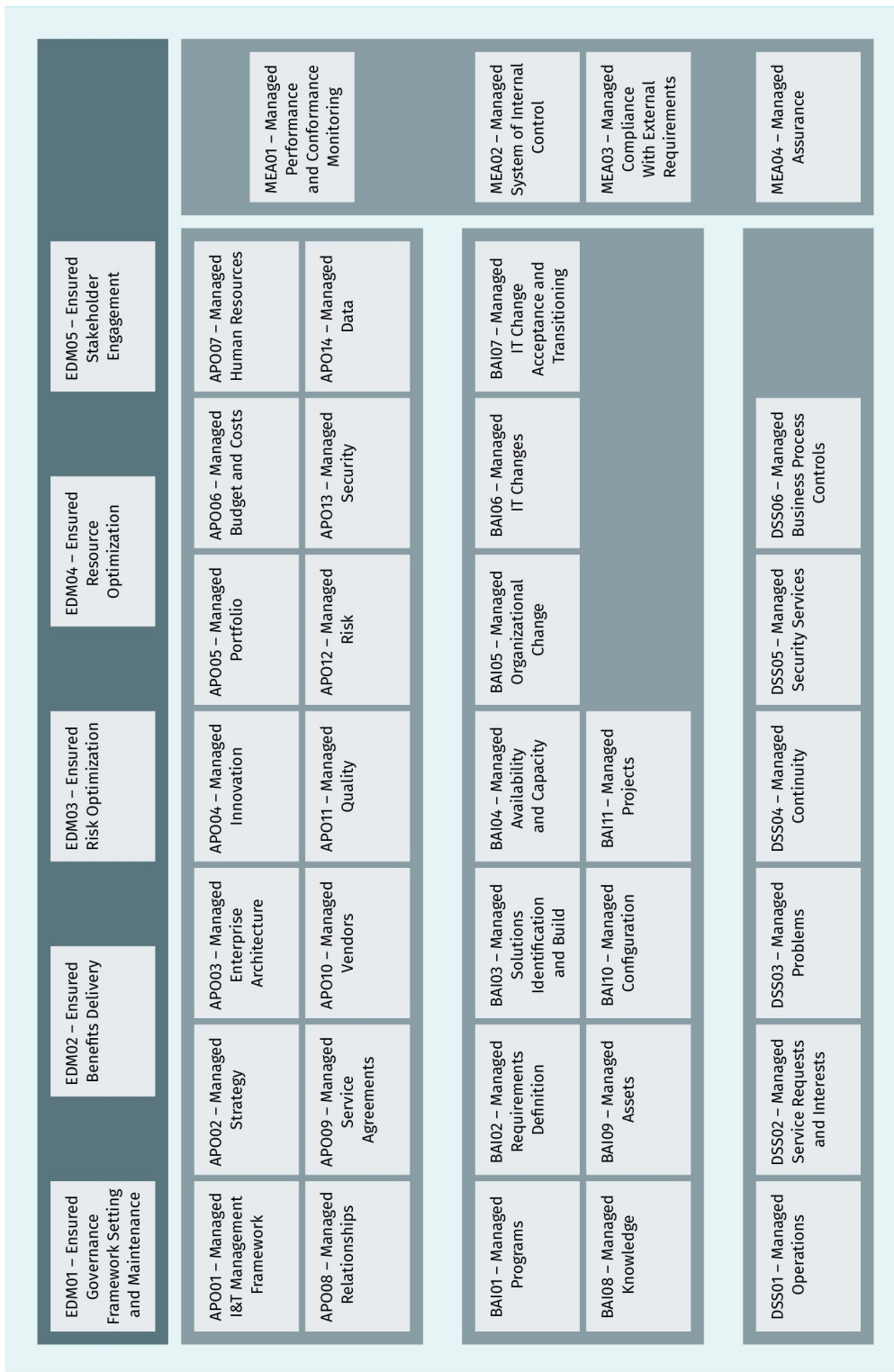
The COBIT core model, also called the “reference model of governance and management objectives”, provides a structure for enterprise and alignment objectives. It is based on the five governance and management domains, each which consist of a set of objectives, as illustrated in the following figure. For example, the first objective in the governance domain “Evaluate, Direct, and Monitor (EDM)” is “EDM01 Ensured Governance Framework Setting and Maintenance” which is concerned with analyzing the requirements on the governance system.

Figure 12: COBIT Core Model I



Source: Created on behalf of IU (2019).

Figure 13: COBIT Core Model II



Source: Created on behalf of IU (2019).

This core model including the governance and management objectives is documented in the ISACA 2019 Objectives document, where each objective is accompanied by the following details: (1) description, (2) purpose, (3) relevant enterprise goals, (4) relevant alignment goals, and (5) governance system components (processes, organizational structures, etc.). This document means that an enterprise that wants to achieve a specific objective has all relevant information available in one place.

The idea behind the COBIT core model is that the model is broad, inclusive, and represents all the I&T work normally found in an enterprise. It is therefore a useful and understandable foundation for operational I&T and business managers. The core model has replaced the process reference model of COBIT 5, which used the same domain structure but only contained the process descriptions of the relevant topics rather than the complete objectives found in COBIT 2019. In this revised version of COBIT, “processes” has been replaced by “objectives”. For example, the process “EDM01 Ensure governance framework setting and maintenance” in COBIT 5 was replaced by the objective “EDM01 Ensured governance framework setting and maintenance” in COBIT 2019.

Governance Domain

Governance objectives deal with the three primary stakeholder objectives: value delivery, risk optimization, and resource optimization. Governance includes activities to evaluate strategic options, provide direction to I&T, and monitor the outcome (Evaluate, Direct, and Monitor (EDM)). EDM includes:

- analyzing the requirements for the governance of enterprise I&T, establishing and maintaining effective enabling structures.
- optimizing the value contribution to the business I&T services and I&T assets resulting from investments made by IT.
- understanding and ensuring enterprise’s risk appetite are identified and managed.
- ensuring that adequate and sufficient IT-related resources and capabilities are available to support enterprise objectives.
- monitoring enterprise I&T performance and conformance measurements are aligned with the goals and metrics.

Management Domains

COBIT management objectives include activities of planning, building, running, and monitoring (PBRM) enterprise I&T.

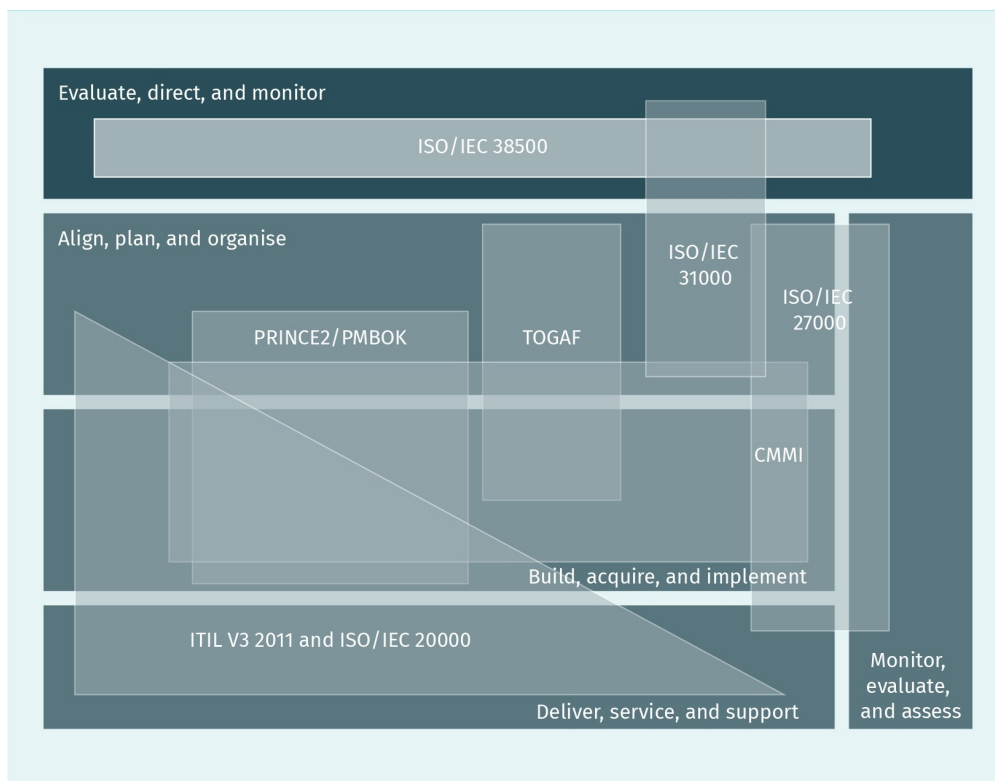
1. Planning: This domain covers aligning, planning, and organizing activities. The main focus is on managing strategy, the management framework, architecture, resources and budget, risk and security, etc.
2. Building: This domain covers building, acquiring, and implementing activities. The main focus is on programs and projects, requirements, solutions, configuration, capacity, assets and knowledge, etc.

3. Running: This domain covers delivering, servicing, and supporting activities. The main focus is on managing operations, service requests, problems, availability, security and process control, etc.
4. Monitoring: This domain covers monitoring, evaluating, and assessing activities within I&T management, and is different from I&T governance “monitoring”. The focus is on performance and conformance, internal control, and compliance.

Alignment with Other Major Standards and Reference Models

An important property of COBIT is that it is an inclusive framework that aligns with other major standards and reference models. As illustrated in the following figure, various other standards and frameworks can be mapped onto the core model. In its conception, special care was taken to ensure that COBIT supports these major standards and reference models rather than conflicts with them. COBIT provides a framework within which to select, use, and combine other models as needed in the specific context of the enterprise.

Figure 14: Other Standards and Frameworks Mapped into COBIT



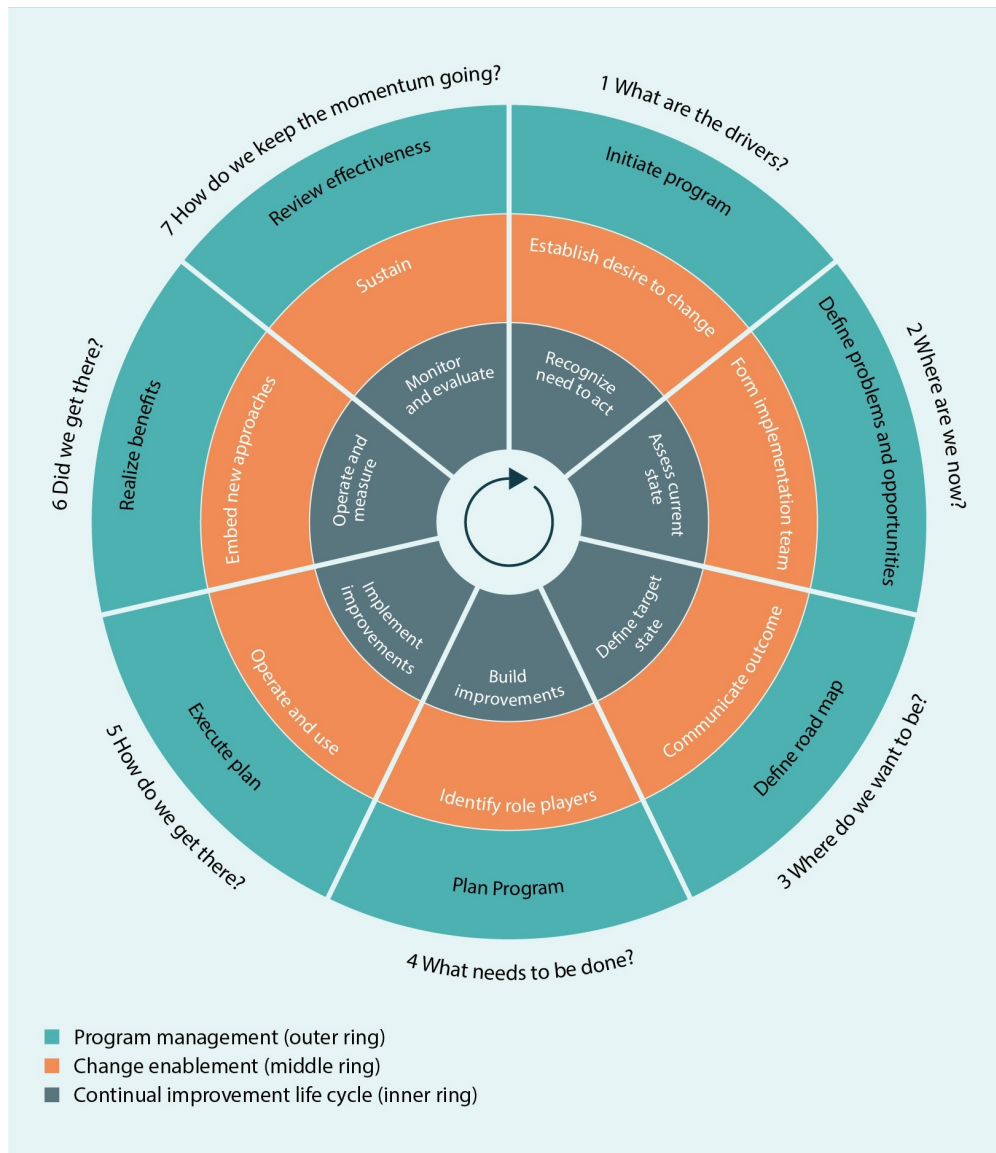
Source: Created on behalf of IU (2019).

3.4 Deploying and Implementing COBIT

To assist with implementation, ISACA has published an implementation guide for COBIT. To begin the implementation process, work has to start at the very top of the enterprise. Since I&T governance is part of enterprise governance, the mandate to establish I&T specific governance mechanisms has to be supported and directed by key stakeholders. Critical steps such as assessment must be followed methodically in order to construct a system of I&T governance that best suits the organization.

The implementation of I&T governance is a complex and challenging process. ISACA recommends utilizing a seven-phase, continual improvement, life cycle approach that provides a method for enterprises to address the complexity and challenges of implementation in an incremental fashion. I&T governance is similar to I&T products and services, in that it is characterized by a continuous life cycle. There are three interrelated components to this life cycle: the core I&T governance life cycle, the enablement of change (addressing the behavioral and cultural aspects of the implementation or improvement), and the management of the program. These three components of the life cycle are illustrated in the following figure.

Figure 15: The COBIT Implementation Roadmap



Source: Thomas, 2019.

This seven-phase roadmap is similar to the **Deming cycle**, also known as the Plan-Do-Check-Act (PDCA) cycle but has more actionable processes at different management levels. The seven phases of the COBIT Implementation Roadmap are now described in detail.

Deming Cycle
a common model for describing continuous or iterative improvement as a cycle with the four phases Plan-Do-Check-Act

Phase 1: What are the drivers?

Phase 1 identifies current change drivers, i.e., an event, condition, or key issue that serves as a stimulus for change. Change drivers are those factors that trigger a desire to change, often at the executive management levels. Usually a business case is generated to solidify the drivers and justify the need for change. This is the most significant step as it requires recognition of the necessity for action. The initial push (i.e., change driver) may come from

a “pain point” such as a significant incident related to an I&T failure. Under these circumstances, the business case for improvement will be related to the experienced failure, which will in turn trigger high-level management actions and increase the chance of management approval.

Phase 2: Where are we now?

Phase 2 identifies the alignment of I&T-related objectives with enterprise strategies and risks. Priorities are established for the most important enterprise goals, I&T-related goals, and enabler processes. Deficiencies and critical processes that need to have sufficient capability are identified via assessment to ensure successful outcomes. The challenges associated with this phase are similar to those of phase 1, including the lack of sustained support from both business and I&T sectors, lack of clear organizational accountability, communications that hamper the alignment effort between different goals, etc. The key to overcoming such challenges is to have management support and structures in place to foster a good working relationship between business and IT.

Phase 3: Where do we want to be?

Phase 3 follows the alignment assessment results from phase 2, and establishes targets for improvements. **Gap analysis** should be performed to identify potential solutions for both the short-term and long-term. Priorities should be determined for the solutions in order to quickly achieve maximum benefits.

Gap Analysis

Comparing the status as-is against the status to-be, to identify the gap that needs to be closed.

Phase 4: What needs to be done?

Phase 4 selects and plans feasible and practical solutions from among the solutions identified and prioritized in phase 3. Here actual projects are defined with the support of business cases. The challenges associated with this phase include any lack of knowledge or skills that hinder the tasks, e.g., a lack of understanding regarding business to I&T alignment, lack of the appreciation of the technological complexity, etc. Training and education about governance and management, and good practice are some of the available means of addressing these challenges.

Phase 5: How do we get there?

Phase 5 establishes the actual implementation of day-to-day activities for proposed solutions. To ensure success, monitoring systems need to be established so that performance can be measured. The challenges associated with this phase are more tactical in nature; they include undertaking problems that are too complicated, not fully understanding the goals and scope, not fully understanding priorities, etc. Effective project and program management help to overcome such problems as they arise.

Phase 6: Did we get there?

Phase 6 focuses on what needs to be done after phase 5 is complete. At this point, the newly improved governance and management practices are being incorporated into normal business operations; performance metrics are used to monitor achievements and

benefits. The main risk associated with phase 6 is the failure to adopt the new solution, which may occur if the solution is too complex to adopt or developed in isolation or is not owned by the process owner. These challenges can sometimes be avoided by modifying a complex solution into smaller, incremental, and ultimately achievable improvements. If this is a management structure-related problem, then communication and structural changes may be possible resolutions.

Phase 7: How do we keep the momentum going?

Phase 7 is the bridge between current cycle and the next. The focus in this phase is on reviewing the overall success of the implementation with regards to business-IT alignment and identifying further governance or management requirements. The main objective of this phase is continual improvement and thus the main challenge associated with it is foster a culture of continuing improvement and maturing the governance. At the completion of implementation, a review and assessment by key stakeholders and implementation committee is necessary to keep the momentum on continuing improvement.



SUMMARY

COBIT has been widely recognized as the IT governance standard by the information technology industry worldwide. Established by ISACA, COBIT has gone through a number of revisions to reflect the evolution of technology, as well as changes in thinking about governance. COBIT provides a comprehensive framework that helps enterprises to achieve their objectives for the governance and management of information and technology assets, and enables I&T to be governed and managed in a holistic manner for the entire enterprise. COBIT defines the components that should be used to establish I&T governance, maintain it, and sustain good practices. COBIT brings together principles that allow the enterprise to build an effective governance and management framework, and optimize the benefits of I&T for stakeholders. In addition, COBIT provides a large collection of guidance and tools.

COBIT is not a prescriptive framework, meaning that it does not define exactly how an organizational I&T environment should be set up, nor does it try to provide detailed information technology management operational tools. Instead, COBIT focuses on the guidance and best practices for organizations to establish, sustain, and improve their I&T governance and I&T management, in order to align with the organization's mission and business strategies. The ultimate objectives for I&T governance, as mandated by COBIT, are benefit realization, risk optimization,

and resource optimization. Organizations must carefully adapt COBIT in order to fully utilize its tool set to fit their own unique mission and business objectives.

UNIT 4

IT GOVERNANCE FRAMEWORKS

STUDY GOALS

On completion of this unit, you will have learned ...

- how the ISO 9000 family relates to IT governance.
- the connection between service and architecture frameworks and IT governance.
- when to apply the correct maturity model.
- the relationship between IT governance and IT security frameworks.

4. IT GOVERNANCE FRAMEWORKS

Introduction

IT governance must include a variety of components in order to bring IT into alignment with an organization's business objectives. The most widely adopted IT governance framework COBIT contains a vast quantity of references to other industry standards and best practices, aggregating knowledge in areas such as quality management, process maturity, service management, enterprise architecture, and information security. Any one of these subjects is informed by vast amounts of knowledge in and of itself; it is not feasible to think that all relevant governance elements will be adequately addressed under the same umbrella. That is why frameworks such as COBIT utilize existing standards and best practices established in respective industries as supporting components.

It is the responsibility of each organization to reference standards, best practices, and guidelines that are most relevant to it when establishing its own IT governance. That said, it is beneficial to have a good understanding of all key components that underpin IT governance, irrespective of their relevance to the specific organization. The following discussion of key components such as quality management and information security is intended to bring such knowledge to the table, so that key individuals involved in establishing governance have a better insight into how this type of related knowledge works in conjunction with IT governance.

4.1 Quality Management as a Foundation

At any level of governance or management, quality is critical to outcomes. Key stakeholders demand quality services from IT investment. Management needs quality information in order to execute business operations. Processes need to achieve goals with intrinsic or contextual quality. There is no doubt that achieving quality is vital for an organization. However, while COBIT has a specific process for quality management, it does not specifically identify exactly what quality management is used for. So what exactly is quality management required for? Simply put, IT governance and management have multiple goals, all processes have outcomes, and all goals and outcomes have services and products associated with them, which require adequate quality management. In this section, we will define quality and quality management and explore the related concepts of quality assurance, quality control, and quality management systems (QMS).

Quality

There are many ways to define quality, depending on the context in which the term "quality" is used. The most widely used definition of quality is from ISO 9000:2015 which defines quality as the "degree to which a set of inherent characteristics of an object fulfils requirements". Quality means that the output, such as a product or a service, from activities, such as a process or a project, complies with specified requirements. For example,

the quality of a specific software product could be determined by the degree to which the product meets the required functionality and possesses important characteristics related to security and maintainability. Aspects of quality can be defined by standards or guidelines, such as ISO/IEC 25010 or COBIT. For example, COBIT process goals have two quality specifications: intrinsic and contextual. The former requires that the outcome from a process is accurate. The latter requires that the result fits the intended purpose. Note that COBIT itself does not specify exactly which standard to apply and how; rather, it includes a process (APO11) that specifies the necessary conditions, as seen in the following table.

Figure 16: COBIT Process on Quality Management

Domain: Align, Plan and Organize Management Objective: APO11 – Managed Quality	Focus Area: COBIT Core Model
Description	
Define and communicate quality requirements in all processes, procedures and related enterprise outcomes. Enable controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts.	
Purpose	
Ensure consistent delivery of technology solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs.	

Source: Created on behalf of IU (2019).

The general attributes of quality can vary considerably, depending on the kind of product, service, or process under consideration. The combination of attributes relevant for a specific type of object (i.e., product, service, or process) is called a quality model. For example, the norm ISO/IEC 25010 defines a quality model for software consisting of functionality, reliability, maintainability, transportability, safety, and security.

In order to understand how quality is measured, controlled, and managed, we will now discuss a number of related concepts. In principle, three levels of activities associated with quality can be distinctively identified and organized. Moving from the top down, these levels are: (a) quality management (QM), (b) quality assurance (QA), and (c) quality control (QC).

Quality Management

Quality management (QM) is the umbrella management of all activities aimed at achieving, sustaining, and improving quality. QM can include establishing quality policies and quality objectives as well as processes to achieve quality objectives through quality planning, quality assurance, quality control, and quality improvement. Good quality management makes organizations more efficient and less wasteful.

The practice of quality management has evolved significantly over the years, from the mere inspection of end-results to the concept of total quality management with its philosophy of building-in quality to final products. This approach is particularly important for the IT industry, as products and services have become far too complex to assure their quality just by testing at the end. Methodologies such as agile development, which merges development and usage in an interactive and fast-moving development environment, allow the realization of quality in the building of products and services.

Quality Assurance

The first level of implementing quality management is quality assurance (QA). The ISO 9000:2015 definition states that quality assurance is the “part of quality management focused on providing confidence that quality requirements will be fulfilled.” The purpose of quality assurance is to support stakeholders who are not in a position to directly oversee operations themselves; quality assurance mechanisms assist them to trust operations and avoid unnecessary interventions.

QA activities do not control quality; they establish the extent to which quality will be, is being, or has been controlled. QA activities are not usually conducted in real-time; they are conducted after the product or the service has been produced. QA is mostly a post-event and off-line action which serves to build confidence in results. In short, QA is verification that quality has been met. For example, a QA activity on database integrity may involve the following steps:

- Confirm that database design documents are complete and compliant with procedures.
- Confirm that database has been implemented according to design.
- Confirm that data tables, views, and fields designs are properly documented.
- Confirm that verification and validation procedures are followed.

There are several steps involved in QA:

1. Obtain the organization documents on plans for achieving quality.
2. Establish a QA plan that defines how an assurance of quality will be obtained.
3. Determine the proposed product or service that will meet the quality specifications.
4. Assess operations, products, and services and determine where and what the quality risks may be.
5. Determine the extent to which the organization quality plans are being adequately implemented.
6. Verify the product or service being produced has met the quality specifications.

Sometimes the planning process is considered a subcategory of QA and given the special designation of “quality planning”.

Quality Control

Quality control (QC) is the next step in quality management. The primary objective of QC is prevention. As defined by ISO 9000:2015, QC is the “part of quality management focused on fulfilling quality requirements”. QC is the part of QM that fulfills the quality requirements, as opposed to QA that simply verifies the outcome. QC activities regulate quality performance.

The basic concept of QC can be simplified into the standard Deming cycle: plan-do-check-act. QC can exercise controls before, during, or after operations. For controls exercised before operations, techniques include establishing competence checks for people and processes and using reliability prediction methods to remove or eliminate potential risks that may affect quality. During operations, constant monitoring of quality parameters provides real-time feedback on the quality of products and services. Inspection or testing after operations is another way to detect deviations in quality and allow corrective actions to take place. For example, a QC activity on database integrity may involve the following steps:

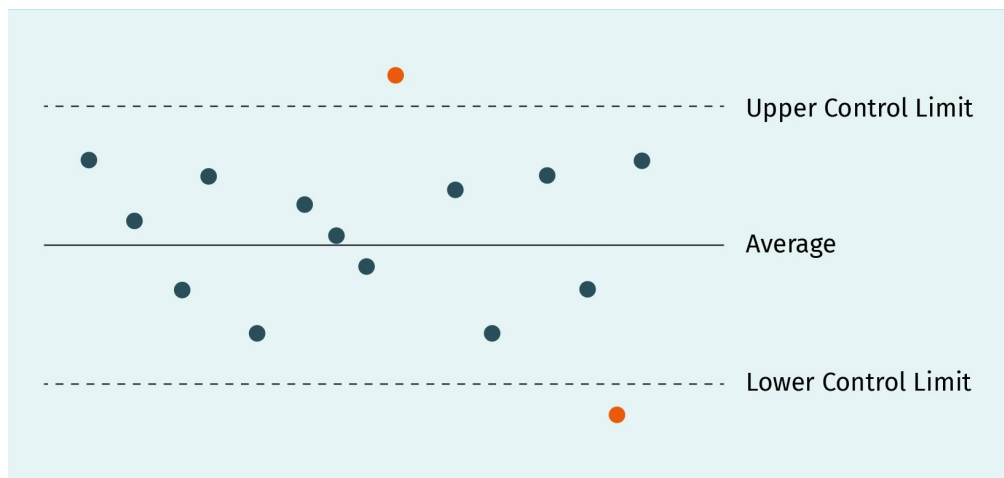
- Confirm database files are free of errors.
- Confirm that all data relationships are correctly represented in the database.
- Confirm that data tables, views, and fields are correctly labeled.
- Confirm table relationships are correct according to design.

There are several actions involved in QC (Hoyle, 2018):

1. Determine quality control parameters and methods for measurement.
2. Establish criticality in order for controls to be inserted before, during, or after operations.
3. Establish a plan that defines how to use controls to detect and to remove variations.
4. Deploy data collection and transmit data for analysis.
5. Verify the results and establish whether the variance is within the quality range.
6. Diagnose the cause of any variance beyond the expected range.
7. Propose remediation and decide on the actions needed.
8. Check that process stability has been restored after remediation.

In practice, QC is used to validate whether a system is operating within a pre-specified range (i.e., within the control limits). For example, statistical process control (SPC) is an industry-standard methodology for measuring and controlling quality during the manufacturing process. The following figure is a simple example of a quality control chart used in SPC to control over time an important quality characteristic of the controlled system.

Figure 17: Quality Control Chart



Source: Created on behalf of IU (2019).

Here the designed value (average) is flanked by an upper control limit and a lower control limit. Any measurements that are within the control limits are considered acceptable (the black dots), whereas any measurements outside the control limits are considered out of acceptable quality range (the red dots). The QC process needs to investigate and to improve the system's operations to eliminate out-of-range results.

Examples of using such QC measurements in the context of IT include controlling the number of bugs found by testing within developed software or the time taken to handle different types of tickets by IT support.

Quality Management System (QMS)

A quality management system (QMS) is an interrelated, coherent collection of policies, procedures, and processes for quality management. A QMS reflects the seven principles for quality management established by ISO 9000 and covers all quality functions and activities as well as business units and external partners and suppliers. Via its QMS, an organization can achieve quality objectives. A QMS supports an organization by ensuring sustained quality management success, increasing customer confidence in the organization's ability to provide quality products and services, optimizing confidence in the organization's supply chain regarding the delivery of quality products and services, and conducting performance conformity assessments against industry standards.

QMS design requirements include

- establishing, implementing, and maintaining the management system.
- instituting the interconnection, interrelation, and sequence of processes.
- establishing measurement processes.

In summary, quality management is a critical part of any organizational governance. For an organization to achieve its mission, the quality of its operations and outcomes must be maintained at a consistent level that meets and exceeds the requirements and expectations of stakeholders. Quality management helps to improve both internal and external products and services, reduce risks, increase efficiencies, and lower costs. It is thus no understatement to say that quality management is a key element of organizational value creation, which is ultimately the primary objective of governance.

4.2 ISO 9000 Family

The ISO 9000 series, also known as the “ISO 9000 family”, was created by the International Organization for Standardization (ISO) as a series of international standards for quality management systems. First published in 1987, the ISO 9000 series is arguably the best-known standard from ISO and deals with the fundamentals and principles of quality management. Its main objective is to help organizations to effectively document, establish, maintain, and improve quality management. The ISO 9000 series is not specific to any one industry but can be applied to all organizations.

The ISO 9000 family refers to the following group of quality management process standards:

- ISO 9000:2015 Quality Management Systems – Fundamentals and Vocabulary: This document specifies the terms and definitions that apply to all quality management and quality management system standards.
- ISO 9001:2015 Quality Management Systems – Requirements: This the core document, which specifies requirements for a quality management system when an organization needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements. This is the one standard in this list that can be used as the basis for **certification** of a quality management system.
- ISO 9004:2018 Quality Management Systems – Managing for the Sustained Success of an Organization: This document provides guidelines for enhancing an organization’s ability to achieve sustained success. This guidance is consistent with the quality management principles outlined in ISO 9000:2015. It also provides a self-assessment tool to review the extent to which the organization has adopted the concepts in this document.
- ISO 19011:2018: Guidelines for Auditing Management Systems: This document provides guidance on auditing management systems, including the principles of auditing, managing an audit program, and conducting management system audits, as well as guidance on the evaluation of competence of individuals involved in the audit process. These activities include the individuals managing the audit program, auditors, and audit teams.

Certification

Third-party confirmation that a product, process, system or person has certain characteristics or satisfies certain requirements.

Together as a collection of guidelines, ISO 9000 provides organizations with the flexibility to implement quality management systems that are most suitable for its business. This freedom allows the ISO 9000 series to be used for almost all organizations, regardless the nature of the business and the size of the organization.

ISO 9000 is built on seven quality management principles (QMP) (ISO 2015):

- QMP 1 – Customer focus
- QMP 2 – Leadership
- QMP 3 – Engagement of people
- QMP 4 – Process approach
- QMP 5 – Improvement
- QMP 6 – Evidence-based decision-making
- QMP 7 – Relationship management

QMP 1 – Customer focus

The objective of QMP 1 is to understand customer needs, meet customer requirements, and exceed customer expectations. Customers are where organizations realize opportunities for value creation. By satisfying customer needs, organizations can retain customers, expand their base for generating value, enhance their reputation, and achieve their mission. Focusing on customers requires recognizing and understanding customer needs, linking those needs with the organization's own objectives, and communicating those needs to the entire organization. Organizations should plan, design, develop, produce, deliver, and support goods and services. This helps them to meet customer needs and expectations, measure and monitor customer satisfaction, and take appropriate actions.

QMP 2 – Leadership

The objective of QMP 2 is to establish unity in the organization's purpose and direction on quality. This means the organization aligns its strategies, policies, processes, and resources to achieve its quality objectives. With good leadership, an organization can be more efficient and effective in meeting its quality objectives and foster an organizational culture that supports quality management initiatives. Leadership must encourage an organization-wide commitment to quality, inspire continuing improvement regarding quality, and recognize the contributions made by everyone within the organization.

QMP 3 – Engagement of people

The objective of QMP 3 is to engage people at all levels throughout the organization with the plan for achieving quality and empower them to enhance the organization's capability to create and deliver value. Organization-wide involvement supports a shared understanding quality management principles and objectives, encourages individuals to take responsibility and embrace quality initiatives, and enhances trust within the organization. Engaging people is important as it is critical that everyone in the organization contributes to quality objectives. In order to support full engagement with quality management, lead-

ership needs to emphasize the importance of individual contributions and facilitate discussions on quality. Other actions undertaken by leaders include sharing knowledge, monitoring job satisfaction, and fostering a culture of trust.

QMP 4 – Process approach

The objective of QMP 4 is to focus on processes that produce consistent and predictable results. This requires a thorough understanding of the activities in each process and the relationship between interrelated processes. Focusing on processes allows the organization to better understand activities and results, improve and optimize key processes, improve process management, and make outcomes more predictable. Establishing a systematic management system for processes is a key step. By clearly defining the processes including objectives, responsibilities, quality criteria, and risks, processes that support quality objectives can be more effective and efficient. A predictable process is the core of quality management.

QMP 5 – Improvement

The objective of QMP 5 is to focus on continuing improvement. To achieve its mission, an organization must consistently improve itself in order to adapt to a changing environment and maintain its performance level over time. Continuing improvement strengthens an organization's reputation among its customers, fosters an internal culture of quality, and encourages learning and innovation. Organizations need to promote continuing improvement through communications, education and training, performance reviews, process improvement systems, and the recognition of improvement when it is implemented.

QMP 6 – Evidence-based decision-making

The objective of QMP 6 is to have decision-making processes that are based on a solid foundation of performance data analysis and evaluation. In an environment where decision-making has become more complex than ever before, it is essential that decisions are based on evidence. While there is always some level of uncertainty and ambiguity surrounding decision-making and the results of data analysis are often subject to interpretation, evidence and data analysis usually lead to a better understanding of the underlying facts and therefore enhance the levels of objectivity and confidence in the decision-making process. Reliable analysis of results requires trustworthy data, meaning that adequate performance monitoring and accurate data collection are essential. A well-founded methodology for analysis that is fully understood by decision makers and conducted by competent analysts is another requirement.

QMP 7 – Relationship management

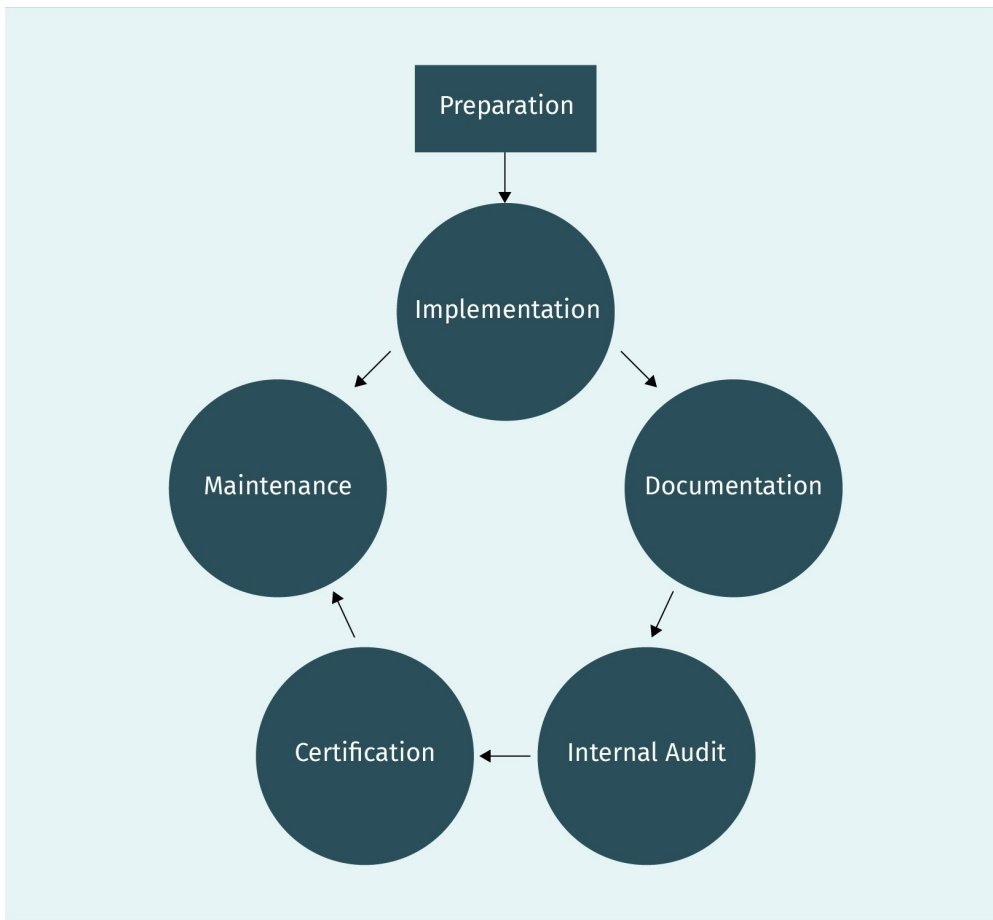
The objective of QMP 7 is to recognize that quality management goes beyond an organization's boundaries. An organization, just like a process, has unique inputs (i.e., upstream suppliers) and the quality of these inputs will naturally affect the quality of outputs (i.e., products and services supplied to downstream customers). Therefore, managing relationships with suppliers and others within an organization's partner networks is critical to overall quality management. Organizations need to identify key partners and establish

trusting and cooperative relationships with them, set up requirements regarding quality standards, share information, and verify and validate quality management and performance with its key partners.

To demonstrate to its customers that it follows ISO 9000 quality standards, many organizations choose to have their QMS certified as ISO 9001-compliant. ISO itself does not provide such certification; it is typically done by independent certification bodies based on results from auditors. There are many advantages of ISO 9001 certification. Externally, it is obvious that being certified can enhance the reputation and credibility of the organization. Internally, certification can also provide benefits such as putting pressure on the organization to actually implement certain improvements and improve decision-making and engage all levels of the organization to advance a culture of quality. While these benefits could also be achieved by implementing a QMS that is not ISO 9001 certified, undertaking the certification process itself will often help an organization to realize such benefits.

Receiving ISO 9001 certification is quite an involved process. There are a number of steps that organizations need to take to receive certification, as illustrated in the following figure:

Figure 18: ISP 9001 Certification Process



Source: Created on behalf of IU (2019).

Preparation

An organization needs to fully understand the ISO 9000 series of standards in order to achieve certification. It needs to have a management team to oversee the entire process. Getting top management support, training key staff, and establishing a project plan are the few preparatory actions to initiate the process.

Implementation

An adequate QMS must be implemented in order for an organization to be certified. The certification is not a “paper certification”; auditors need to validate that quality management is indeed taking place within the organization as specified by ISO 9001. Most if not all employees in the organization will have to change their work routines. Work instructions need to be standardized according to ISO 9001 and adequate training is often necessary.

Documentation

Documentation is an integral part of setting up a QMS and is also a critical step for the successful completion of ISO 9001 certification. The organization needs to document their quality policies, processes, and procedures as well as their quality management system. This may take the form of organizational process descriptions and flowcharts, quality objectives, process and procedure operational instructions. A quality management manual usually provides an overview of the QMS and its main components.

Internal audit

First/second/third party audit

An audit is an independent examination of a process, product or system that can be performed internally (first party), by the customer or supplier (second party) or some other, external entity (third party).

In addition to third-party independent auditing, thorough internal **audits** are necessary to verify that the organization follows its own rules and meets the requirements of ISO 9001. Internal auditing provides verification and gap analysis, providing a basis for improving processes should non-compliance and deficiencies be identified.

Certification

To achieve certification, the organization selects a certification body (registrar) which is an independent entity and authorized (accredited) to issue the ISO 9001 certificate. This certificate is based on the report by an independent, third-party ISO 9001 auditor who visits the organization and performs a site audit. The ISO 9001 certification audit can be conducted as soon as the QMS has been set up as confirmed by internal auditing.

Maintenance

ISO 9001 certification is not a one-time event. Periodical site audits, once or twice a year, are required in order to verify continued ISO 9001 compliance. The auditor may want to see continuing improvement of the implemented ISO 9001 quality management system.

ISO 9001 audit process can be quite extensive and drawn-out, so good preparation is vital. An auditor uses long checklists to validate processes and suppliers, among other aspects. Auditor findings for each audit question fall into one of four categories:

- **Compliant:** This finding indicates that the organization complies with the requirements of the standard and the QMS. The process is implemented and documented and records exist to verify this. Follow-up actions could include continuing to monitor trends and indicators.
- **Opportunity for improvement (OFI):** This finding indicates that there is a low risk issue with the process that offers the organization an opportunity to improve current practice. For example, the process may be overly complex but meets relevant targets and objectives. Follow-up actions include reviewing and implementing actions to improve the process. Unresolved OFIs may degrade over time to become noncompliant.
- **Minor noncompliance:** This finding indicates that there is a minor nonconformance where the main goals of the processes will still be achieved. This is not likely to result in the failure of the management system, nor will the process result in the delivery of non-conforming results. Follow-up actions include investigating root causes and implementing corrective actions by the next reporting period or next scheduled audit.

- Major noncompliance: This finding indicates that this is a high risk, major nonconformance, which directly impacts upon customer requirements or reduces the effectiveness of the QMS. Follow-up actions include implementing immediate containment actions, investigating root causes, and applying corrective actions.

All findings need to be supported by evidence. The following figure is an example of the type of checklist and audit questions used in the ISO 9001 audit process.

Figure 19: ISO 9001

Ref	Audit Question	Audit Findings (Score 1 per box)				Audit Evidence	Comments and Suggestions
		COMPLIANT	OFI	MINOR N/C	MAJOR N/C		
1	Is the process defined and documented?						
2	Is the process owner identified? (process map, procedure or work instruction, etc.)						
Ref	Audit Question	Audit Findings (Score 1 per box)				Audit Evidence	Comments and Suggestions
		COMPLIANT	OFI	MINOR N/C	MAJOR N/C		
	...						

Source: Created on behalf of IU (2019).

To audit a process, the process definition, related resources, execution, monitoring, and improvement are reviewed using the checklists. For other audit areas, e.g., auditing of suppliers, areas such as quality management, continuous improvement, quality planning, training and awareness, and customer documentation are checked for compliance.

In summary, the ISO 9000 series or family is the most adopted among all ISO standards due to the fact that every organization needs to have quality management to meet its mission and strategic objectives. However, the series is a detailed and complex collection of standards and its adoption should not be taken lightly. The successful implementation of these standards will bring a variety of benefits to the organization that will significantly enhance its competitive position.

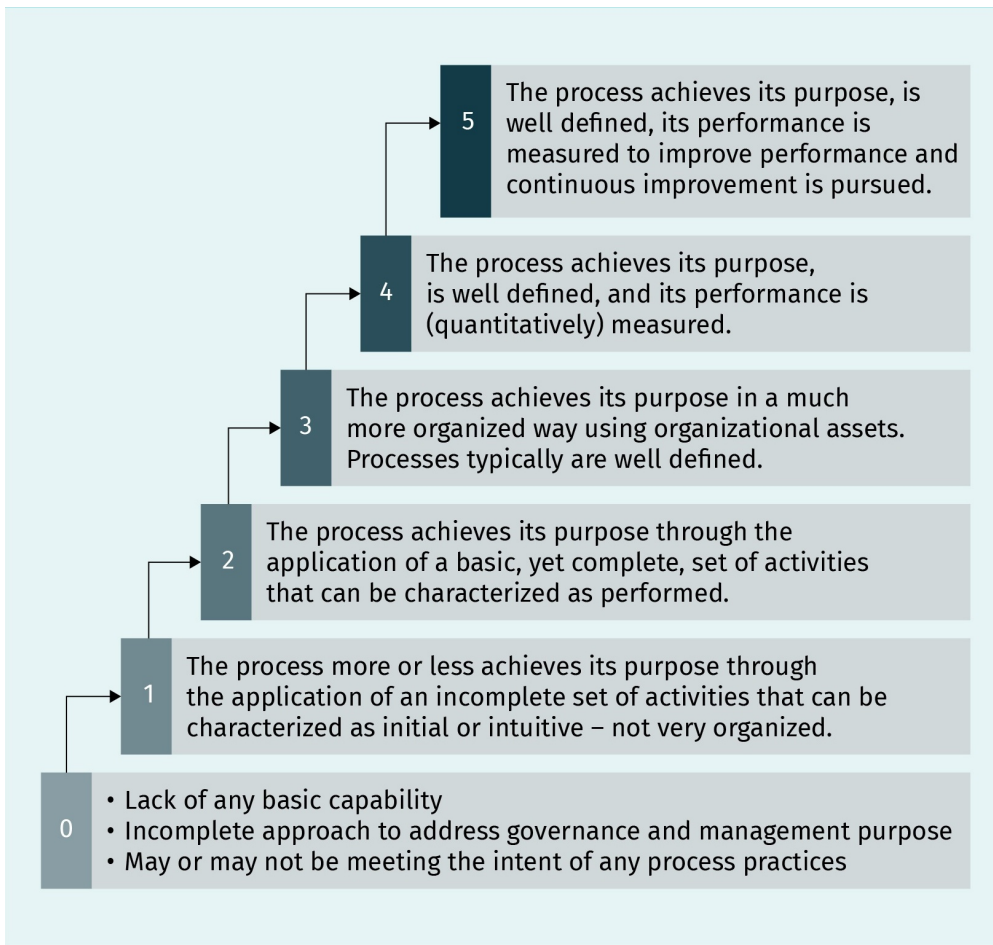
4.3 Maturity Models

One of the core objectives of IT governance is to align an organization's IT strategy with its core mission and strategy. To achieve this, the organization must be sufficiently mature. Organizational maturity is defined as the "extent to which an organization has explicitly and consistently deployed processes that are documented, managed, measured, controlled, and continually improved" (Kock, 2008, p.225). The maturity of an organization can be measured by various assessments which provide organizations with knowledge about the capability and competence of their IT and consequently reveal gaps between desired and current IT performance. Organizations can then make informed decisions regarding governance improvement. There are several commonly adopted performance maturity models that are used by IT communities worldwide. Three of them — COBIT, CMMI, and SPICE — will be discussed here.

COBIT

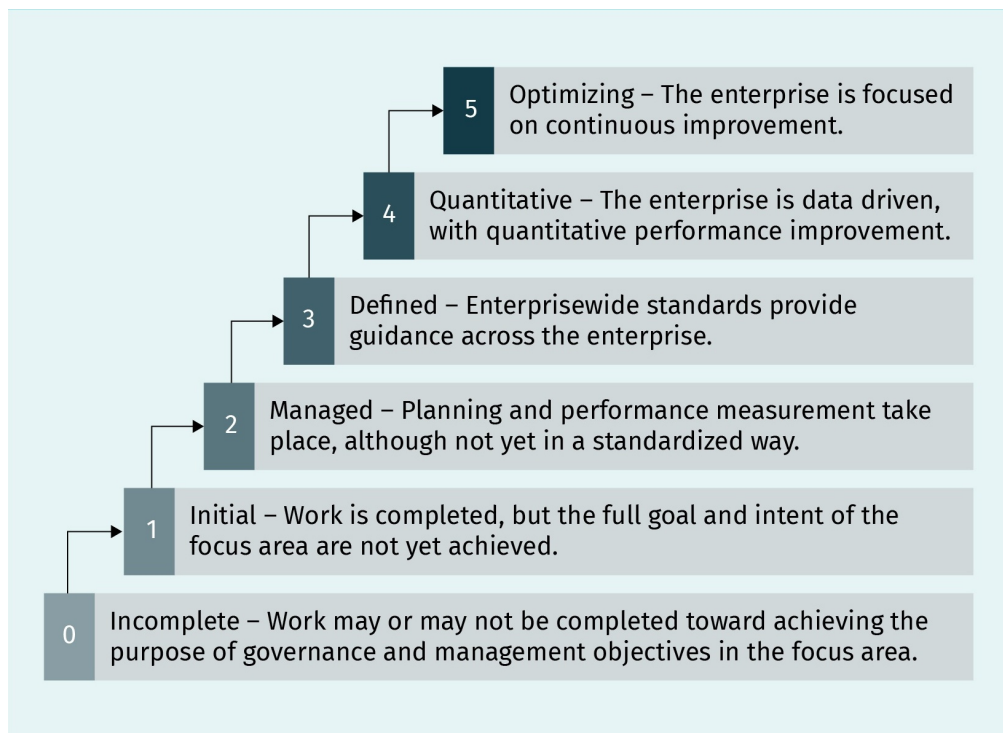
The COBIT process maturity assessment has shifted from an ISO/IEC 33000-based approach (which is the successor to ISO/IEC 15504, better known as SPICE) as used in COBIT 5 to a CMMI 2.0-based approach as used in COBIT 2019. While the general concept of both approaches is the same, the details of the level structure and the maturity evaluation differ considerably. CMMI 2.0 and therefore COBIT 2019 distinguish between the capability level of individual processes and the maturity level of focus areas. The capability levels and maturity levels are seen in the following two figures.

Figure 20: COBIT Capability Levels for Processes



Source: Created on behalf of IU (2019).

Figure 21: COBIT Maturity Levels for Focus Areas



Source: Created on behalf of IU (2019).

Focus area is defined as “a certain governance topic, domain, or issue that can be addressed by a collection of governance and management objectives and their components. Examples of focus areas include small and medium enterprises, cybersecurity, digital transformation, cloud computing, privacy, and DevOps” (ISACA, 2018).

CMMI

Capability Maturity Model Integration (CMMI), successor to the Capability Maturity Model (CMM) developed by Carnegie Mellon University, is an integrated process improvement model currently administered by the CMMI Institute, a subsidiary of ISACA. Originally, CMM was specifically aimed at software development but CMMI is a much broader performance maturity and improvement framework. That said, the focus of CMMI, as with CMM, is still on process.

CMMI 1.3 consists of three models, or “constellations”, that address the following application areas:

- product and service development (CMMI for Development (CMMI-DEV))
- service establishment, management, and delivery (CMMI for Services (CMMI-SVC))
- product and service acquisition (CMMI for Acquisition (CMMI-ACQ))

CMMI 2.0 merges all three models together under one framework with different “customized views”.

The CMMI maturity model consists the following key elements: process areas, goals and practices, and representations. A process area is defined by CMMI as “a cluster of related practices in an area that, when implemented collectively, satisfies a set of goals considered important for making improvement in that area.” Examples of such process areas are “Project Monitoring and Control” (PMC) and “Process and Product Quality Assurance” (PPQA).

CMMI goals describe what is required to be achieved by a process, while practices provide more detail and describe what is expected to be done to satisfy a certain goal. In CMMI 1.3, there are two types of goals and practices: generic and specific, but this distinction has been removed in CMMI 2.0. Essentially the difference is that generic goals and practices are a part of every process area and define how to introduce and manage the different process areas within an organization, while specific goals and practices just relate to one selected process area and define the specific requirements of this process area. A process area is satisfied when organizational processes cover all of the generic and specific goals and practices for that process area. Two examples of generic goals (GG) and practices (GP) are “GG 2 Institutionalize a Managed Process” and “GP 2.2 Plan the Process”. Two examples for specific goals (SG) and practices (SP) are “PPQA.SG 1 Objectively Evaluate Processes and Work Products” and “PPQA.SP 1.1 Objectively Evaluate Processes”.

CMMI supports two improvement paths which correspond to two different types of improvements. A “representation” allows an organization to pursue and achieve a specific type of improvement objective: capability or maturity. Continuous representation uses capability levels to measure improvement; it enables organizations to incrementally improve processes that correspond to an individual process area. Staged representation uses maturity levels to measure improvement; it enables organizations to incrementally improve a set of related processes area such as a focus area. The difference between the two representations is subtle but significant. The staged representation indicates the collective state of the organization’s processes whereas the continuous representation demonstrates the state of an individual process area. The continuous representation allows organizations the flexibility to focus on individual process areas that need to be prioritized for improvement whereas stage representation demonstrates the overall maturity at organization level.

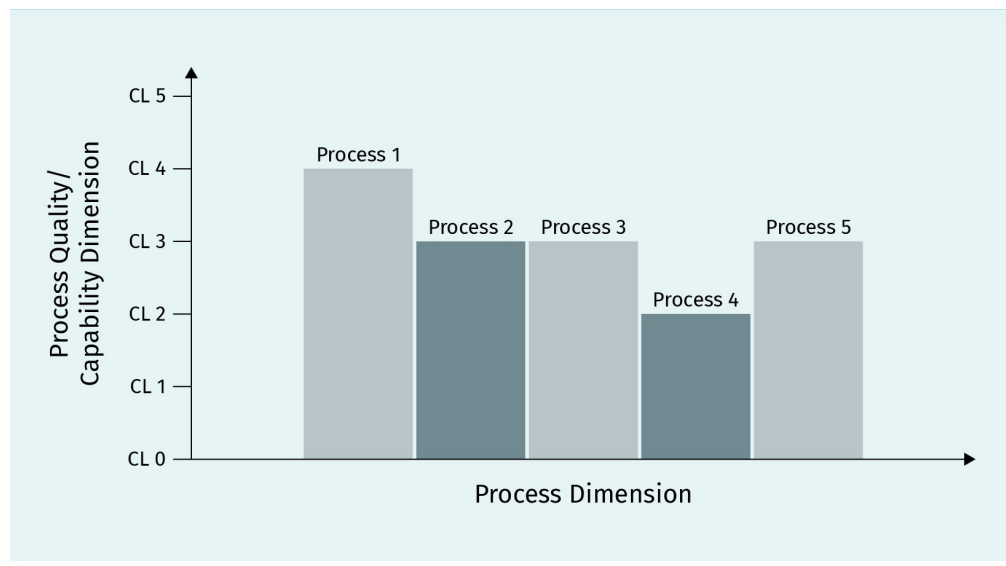
SPICE

Software Process Improvement and Capability Determination (SPICE) was a project that led to the creation of “ISO/IEC 15504 Information Technology—Process Assessment”, a set of technical standards documents used for the assessment of various IT processes. The ISO/IEC 15504 series is currently being replaced by the ISO/IEC 33000 series, so the following discussion is based on ISO/IEC 33000. The ISO/IEC 33000 Process Assessment Standard series is aimed at assessing and understanding the state of organization’s processes and its relationships with upstream suppliers and downstream customers. ISO/IEC 33000 series is a very large “family”, with standard documents covering: core elements; guidance; measurement frameworks; documented assessment processes; process reference models; process assessment models; and organizational maturity models.

ISO/IEC 33000 provides a framework for assessing the maturity of an organization and its processes which can be adapted to differing application areas based on the concepts of a “process reference model” and “process assessment model”. A process reference model (PRM) consists of process definitions in a life cycle with purpose and outcomes and is performed within the architecture of the entire organization processes. A process assessment model (PAM) builds on the PRM and provides the criteria to measure the capabilities of the PRM processes, assigning a capability from 0 to 5 based on assessment results. Specific PRMs and PAMs have been created for software development, systems development, and IT service management.

Just like the results of an assessment based on the continuous representation of CMMI, the results of a SPICE-based assessment are reported as a “capability profile” with two dimensions, as shown in the following figure.

Figure 22: Sample Capability Profile



Source: Created on behalf of IU (2019).

Measuring IT governance maturity can reveal the degree of alignment between an organization’s IT and its mission and strategy. More mature governance has many benefits to an organization such as improved confidence and enhanced reputation. In order to specify the level of maturity, a designated methodology that is widely accepted and recognized need to be implemented, and verification and validation processes need to be in place for objective analysis and maturity certification to occur.

4.4 Relationship to Service and Architecture Frameworks

IT governance and IT strategy are implemented through various IT processes which work together to accomplish results that satisfy governance and strategy objectives. Frameworks such as COBIT establish what needs to be done via processes but do not prescribe exactly how the process should be incorporated into an organization's business structure, nor do they describe exactly how these processes should be connected and organized to support high-quality IT operations. In order to implement IT governance based on a framework such as COBIT, additional procedures are needed to exercise governance principles in a real environment. In this section, two such procedures, IT service management (ITSM) and IT enterprise architecture (EA), are discussed in detail.

IT Service Management

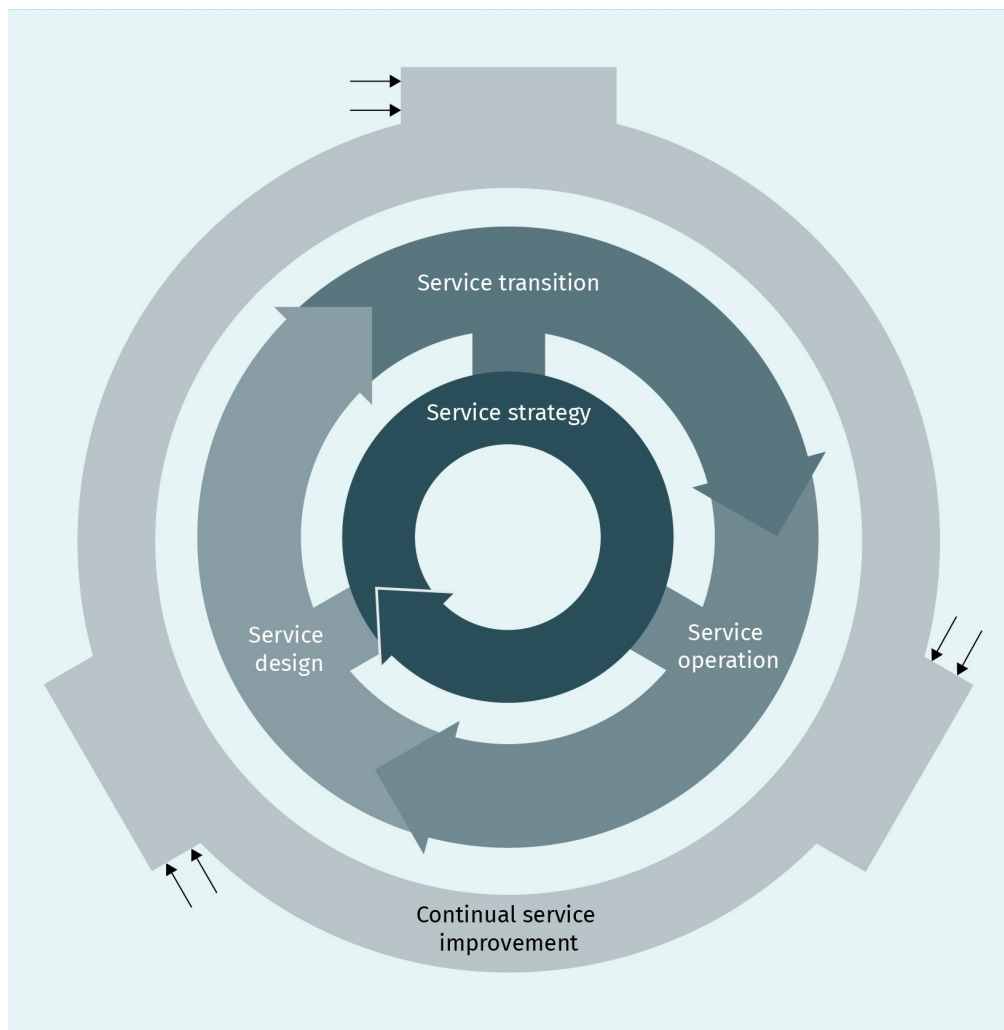
IT service management (ITSM) is where IT operational actions take place. ITSM refers to all the activities involved in planning, designing, delivering, supporting, managing, and improving IT services based on service strategy. ITSM represents how IT services interact with an organization's business activities. Effective ITSM provides several benefits to an organization: lower costs for IT operations; reduced IT operational risks; improved change management; and improved efficiency of IT operations.

A typical IT service cycle starts with a service request, which can be either an incident or a request for a new service. Depending upon the nature of the service request, a series of different actions will take place, from incident management to new service design, transition, and support. Regardless of the type of action taken, change management is typically involved. With all ITSM processes, best practice requires that performance metrics are identified and measured in order to continuously improve and mature. Hence a framework of ITSM can greatly assist an organization to manage its IT operations.

There are several ITSM frameworks available to the IT industry, but by far the best known and most widely adopted framework is the Information Technology Infrastructure Library (ITIL), a collection of ITSM best practices originally developed by the British government and currently managed by AXELOS, a joint venture between the British government and the business consortium Capita. ITIL describes processes, procedures, tasks, and checklists which can be applied by any organization for integrating IT services with an organization's strategy, thereby delivering value and maintaining a minimum level of competency. ITIL is a non-prescriptive framework that provides best or good practice guidelines.

ITIL is focused on service, which is defined as "a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks" (McCulloch, 2018). This value proposition is the key principle of ITIL, which is an ideal fit for IT governance's objective of creating value for the organization. ITIL is structured around the core concept of service life cycle management, which consists of the elements service strategy, service design, service transition, service operation, and continual service improvement, as illustrated in the following figure.

Figure 23: ITIL Service Life Cycle



Source: Pink Elephant, n.d.

Adhering to its own life cycle management principle, ITIL is constantly improving itself. The current version (v3) was published in 2007 and updated as edition ITIL 2011. In early 2019, initial documents of version 4 were published which expand v3 to include quality management, DevOps, Agile, and Lean methodologies.

ITIL service building blocks are functions and processes. A process is a structured set of activities designed to accomplish a specific objective. For example, the change management process establishes a series of activities to facilitate the enacting of specified changes. A function can be viewed as a group of people with tools and resources carrying out activities as prescribed by processes. For example, a helpdesk function consists of helpdesk personnel who utilize various helpdesk tools and follow various processes to assist users throughout the organization.

ITIL processes have the following characteristics:

- They are closed-loop systems that provide change and transformation towards a goal and use feedback for self-reinforcing and self-corrective actions.
- They are performance-driven with measurable parameters including cost, quality, and other variables such as duration and productivity.
- They have specific results that are individually identifiable and countable.
- They deliver primary results to internal or external stakeholders and must meet their expectations.
- They respond to a specific event, albeit that event may be ongoing or iterative.

ITIL functions have the following characteristics:

- They are units of organizations specialized to perform certain types of work and responsible for specific outcomes.
- They are self-contained with capabilities and resources necessary for their performance and outcomes.
- Their capabilities include work methods internal to the functions.
- They have their own body of knowledge which accumulates from experience.
- They provide structure and stability to organizations.

The major ITIL stages—strategy, design, transition, operation, and improvement, traditionally called the “books” of ITIL—are all built upon processes and functions, as summarized in the following figure.

Figure 24: ITIL Processes and Functions

Continual Service Improvement			
Service Improvement	Service Measurement	Service Reporting	
Service Strategy	Service Design	Service Transition	Service Operation
Financial Management	Service Level Management	Change Management	Incident Management
Service Portfolio Management	Availability Management	Configuration Management	Problem Management
Demand Management	Capacity Management	Release Management	Request Fulfillment
Strategy Generation	Service Continuity Management	Transition Planning and Support	Access Management
	Service Catalogue Management	Validation and Testing	Event Management
	Security Management	Evaluation	Technical Management (Function)
	Supplier Management	Knowledge Management	Operation Management (Function)
			Applications Management (Function)
			Service Desk (Function)

Source: Created on behalf of IU (2019).

ITIL Service Strategy provides guidance on service management as a strategic asset. Service strategy guides service management policies, guidelines, processes, and functions across the ITIL service life cycle. Associated activities include strategic assessment and the development of IT capabilities. Service strategy uses demand management and financial management to process service requests to establish a service portfolio and catalogue.

ITIL Service Design provides guidance for the design and development of IT services and service management practices. The main purpose of the design of IT services is to meet the requirements of customers. The overall design aspects include service functions and capabilities, service management systems and tools, service technology architectures, processes to transit into production, and performance methods and metrics.

ITIL Service Transition provides guidance on transitioning new services into the production environment. Essentially, service transition deals with what has been planned and built and tries to ensure that this will actually achieve the expected objectives of the service request. Service transition deals with planning and managing resources and capacities required to build, test, and deploy new services. Change management based on rigorous methodologies that address service functionality, integrity, risk, security, and serviceability is critical to success.

ITIL Service Operation provides guidance on the day-to-day production, delivery, and support of IT services. In the end, governance and strategic objectives are ultimately realized via service operations, delivering desired IT values to stakeholders efficiently and effectively. Service operation covers a large range of activities, including service functions (i.e., units in organizations that perform specific tasks and are responsible for specific outcomes). ITIL service operation functions include service desk, technical management, operations management, and applications management. Together, these functions provide a contact point for technical and daily operational support and software management. Service operations are supported with a set of processes that aims to provide an effective IT support structure. Core processes include incident management (i.e., managing incidents which negatively affect the provision of services), problem management (i.e., identifying and resolving the causes of incidents), and request fulfillment (i.e., focusing on fulfilling service requests).

ITIL Continual Service Improvement provides guidance on monitoring, evaluating, and improving the quality of services and the maturity of the ITSM life cycle, along with its underlying functions and processes. In addition to providing feedback on ITSM health, capabilities, and maturity, continual service improvement also enables the organization to measure and advance the IT-business alignment, as IT values manifest throughout the entire service management life cycle.

An organization's IT service is the most direct interface between its IT governance and its stakeholders. Effective and efficient IT service management can reduce risks, enhance positive relationships, build confidence, and ultimately contribute towards achieving IT governance objectives.

IT Enterprise Architecture

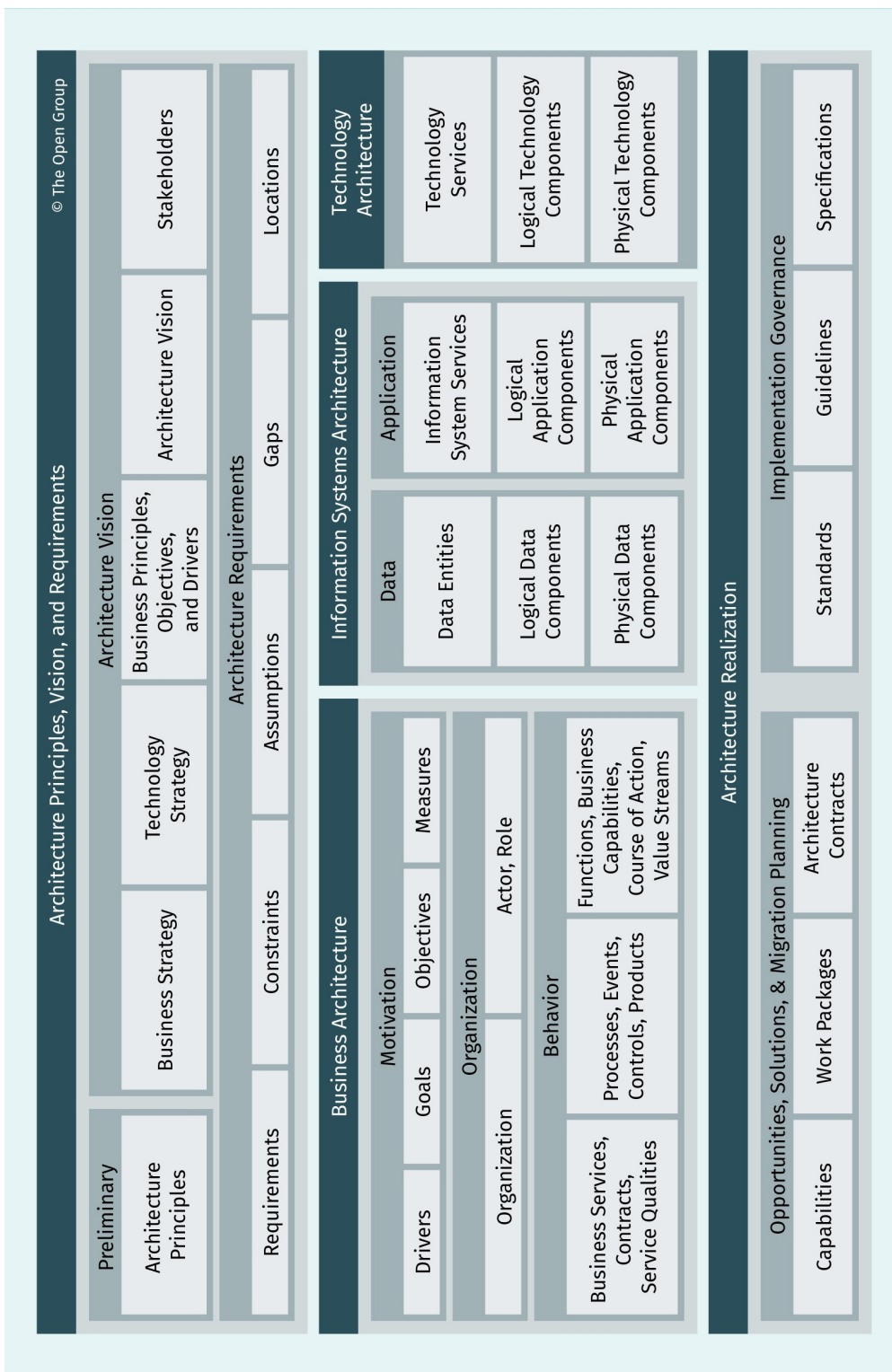
Enterprise architecture (EA) defines, standardizes, and optimizes the structure of an organization. The objective of enterprise architecture is to determine how an organization can efficiently and effectively achieve its mission and business objectives and build it accordingly. EA involves analysis, design, planning, and implementation for the successful development and execution of an organization's business strategy. EA applies architecture principles and practices to guide organizations through the design and deployment of business, information, process, and technology changes. The idea behind EA is to create an environment that promotes shared interests and goals within the entire organization, and ultimately build a unified business infrastructure that can fulfill the needs of everyone.

Within IT governance, e.g., under the COBIT framework, EA can play a significant role in planning and building IT infrastructure that enables the entire organization to operate in a unified, standardized, and optimized environment. Advantages of such architecture is that it can be less wasteful, easier to manage and update, and provides better ROI on IT investment.

EA has been gaining greater recognition as IT governance has been gaining momentum. Several frameworks that provide EA guidance include: The Open Group Architectural Framework (TOGAF); the Federal Enterprise Architecture Framework (FEAF); the Gartner Methodology; and the Zachman Framework for Enterprise Architectures. Among them, TOGAF is the most widely adopted EA framework.

TOGAF was developed and is maintained by The Open Group, an industry consortium with the mission to “enable the achievement of business objectives” (n.d.). The Open Group provides the following definition for TOGAF: “The TOGAF standard is an architecture framework. It provides the methods and tools for assisting in the acceptance, production, use, and maintenance of an Enterprise Architecture. It is based on an iterative process model supported by best practices and a re-usable set of existing architecture assets” (2018). TOGAF contains several key architectural building blocks, as seen in the following figure.

Figure 25: TOGAF Architecture Metamodel



Source: Created on behalf of IU (2019).

The main architectural framework of TOGAF is based on four interrelated subsets of EA known as architecture domains:

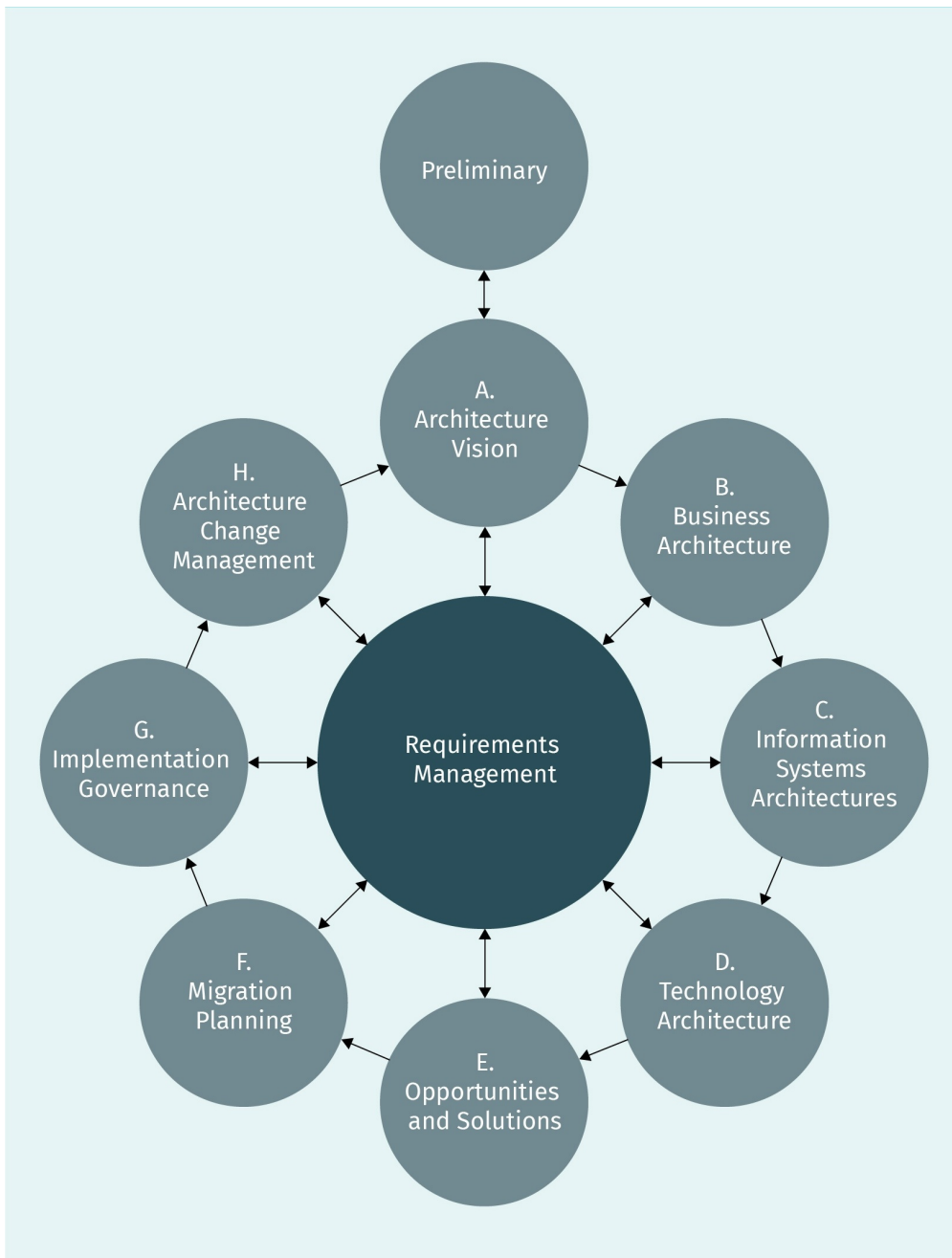
- Business architecture defines the business strategy, governance, organization, and key business processes of the organization.
- Data architecture describes the structure of an organization's logical and physical data assets and associated data management resources.
- Applications architecture provides a blueprint for individual applications to be deployed and identifies their interactions between and relationships to the core business processes of the organization.
- Technology architecture describes the logical software and hardware capabilities that are required to support the deployment of business, data, and application services. This includes IT infrastructure, middleware, networks, communications, processing, and standards.

The core TOGAF documents provide an abundance of practical information and guidelines and include the following documents:

- Architecture Development Method (ADM) and ADM Guidelines and Techniques, which provide methodologies for delivering IT architecture and a TOGAF library
- Architecture Content Framework, which describes the TOGAF content framework and includes a structured metamodel for architectural artifacts and an overview of typical architecture
- Enterprise Continuum and Tools, which discusses classifications and tools to categorize and store the outputs of architecture activity within an enterprise
- Architecture Capability Framework, which discusses the organization, processes, skills, roles, and responsibilities required to establish and operate an architecture function within an enterprise

The TOGAF ADM provides very detailed, step-by-step, practical guidelines for an organization to implement their own EA. The ADM uses a continuous, cyclical, and iterative process for gradually building up the architecture. The phases described by ADM are illustrated in the following figure.

Figure 26: Architecture Development Cycle



Source: Created on behalf of IU (2019).

These phases are further expanded into steps. The ADM utilizes an “architecture repository” to deposit and reuse components that have been developed. The ADM defines a recommended sequence for the various phases and steps involved in developing the necessary architecture, based on the scope determined by the organization. As the architecture develops, the depth and breadth of the deliverables increases and finished components are added to the organization’s architecture repository.

TOGAF should be treated as a part of IT governance, as the enterprise architecture it establishes will need to be a part of IT strategy. The TOGAF framework fits well with the objective of IT governance as a holistic IT architectural tool set.

In summary, building an organization's IT infrastructure and providing services to stakeholders are some of the actual IT strategic objectives that have a direct impact upon an organization's business. It is therefore important to have certain proven methodologies and guidelines such as the ITSM and EA to assist the fulfillment of these IT objectives when establishing the overall organization's IT governance. Frameworks like ITIL and TOGAF can provide benefits including faster and simpler IT service establishment due to standardization, better utilizations of IT assets, reduced risks, improved ROIs, and more. They reflect exactly the key elements of IT governance and value creation: benefit realization, risk optimization, and resource optimization.

4.5 Relationship to IT Security Frameworks

As society becomes more information-driven, information security is critical for every IT function for one main reason: information without security is not only useless, but dangerous. Without exception, any form of IT governance must contain a security component.

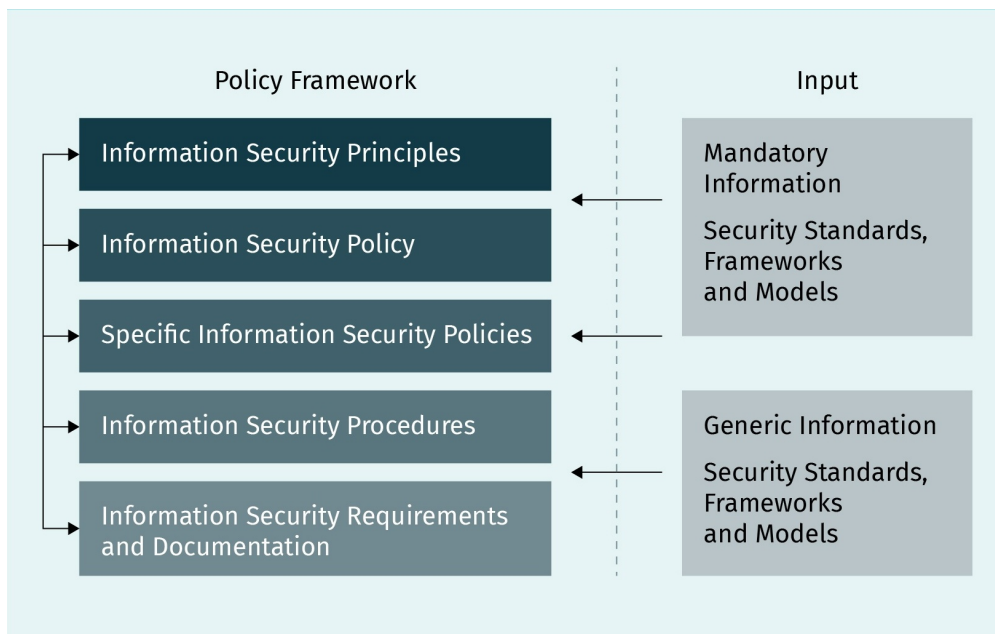
IT security is a broad umbrella. It encompasses governance strategies, management policies, governance frameworks, industry best practices, and technologies. The fundamental aim of IT security is to prevent unauthorized access and modification to information assets in operation, in transit, and at rest, and to assure information availability. IT security is always a significant challenge for organizations because it is a "moving target"; technology is evolving in an ever-increasing pace and threats are becoming increasingly sophisticated. This means that IT security must be a primary concern for any organization.

There are various laws and regulations related to IT governance and almost all of them address IT security. All current IT governance frameworks used in the industry have some component on information security. For example, COBIT has a specific information security framework that addresses four specific areas:

1. Guidance on enterprise business drivers and benefits related to information security
2. Principles from an information security perspective
3. Enablers used by information security to support enterprise governance and management
4. Alignment with other information security standards

The following figure illustrates the key elements and inputs that constitute COBIT's security policy framework.

Figure 27: COBIT Security Policy Framework



Source: ISACA, n.d.

COBIT further establishes 12 security principles, as seen in the following table. (Note: COBIT does not specify exactly how to implement security management. It relies on other specific information security standards to fill in the details.)

Figure 28: COBIT Information Security Principles

A. Support the business	A 1 Focus on the business
	A 2 Deliver quality and value to stakeholders
	A 3 Comply with relevant legal and regulatory requirements
	A 4 Provide timely and accurate information on security performance
	A 5 Evaluate current and future information threats
	A 6 Promote continuous improvement in information security
B. Defend the business	B 1 Adopt a risk-based approach
	B 2 Protect classified information
	B 3 Concentrate on critical business applications
	B 4 Develop systems securely
C. Promote responsible security behavior	C 1 Act in a professional and ethical manner
	C 2 Foster a security-positive culture

Source: Created on behalf of IU (2019).

Within the industry, several standards address components of IT security but the ISO/IEC 27000 series specifically tackles this issue. The objective of the ISO/IEC 27000 family of standards is to help organizations to keep their information assets secure. The ISO/IEC 27000 series is, like many other ISO/IEC standards, a big “family”. Among the standards, the first three are of most interest:

- ISO/IEC 27000: Information security management systems—Overview and vocabulary
- ISO/IEC 27001: Information security management systems—Requirements
- ISO/IEC 27002: Code of practice for information security controls

C-I-A Triad
IT security addresses the three aspects of Confidentiality, Integrity and Availability of data and systems

The ISO/IEC 27000 concept of security is based on the **C-I-A triad** of security principles: confidentiality, integrity, and availability. Confidentiality is the security principle that controls access to information. It is designed to ensure that information is accessible only to intended users. Integrity is the security principle that assures that information is trustworthy and accurate and not altered by unauthorized users. Availability is the security principle that guarantees that information is available to authorized users and the information system is designed to assure high availability.

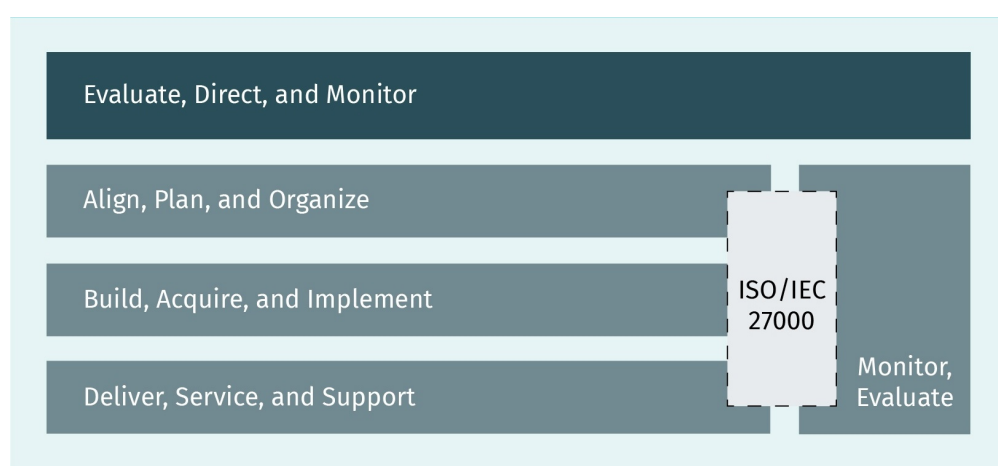
An information security management system (ISMS) is a framework that seeks to keep an organization’s information secure. It contains a set of policies and procedures as well as logical and physical controls to protect the information based on the C-I-A triad. The ISMS is the system through which the organization identifies, analyzes, and controls its information risks.

An ISMS can be certified via the ISO/IEC 27001 standard. The ISO/IEC 27001 standard is a technology-agnostic and vendor-independent ISMS standard. It is a collection of information security guidelines that are intended to help an organization implement, maintain, and improve its ISMS. It offers specifications and a prescriptive description of the features of an effective ISMS. There is a certification process associated with ISO/IEC 27001 that states what is expected of an ISMS to achieve conformity. In order to receive certification or to pass an audit, the ISMS must satisfy these requirements. The second document within the ISO/IEC 27002 series provides code of conduct guidance and recommended best practices that can be used to enforce the ISO/IEC 27001 specifications.

ISO/IEC 27002 recommends implementing information security controls that address objectives arising from risks to the C-I-A triad. An organization that adopts the ISO/IEC 27002 standard must clarify its control objectives and apply suitable controls-based risk assessments. The standard is structured logically around groups of related security controls. Many controls are relevant across various sections; however, they are each assigned to a single section and cross-referenced where necessary. There are a total of 35 control objectives and over 100 controls.

While the ISO/IEC 27000 series is specifically focused on information security, it needs to be properly integrated into the overall IT governance. In general, IT governance is a high-level framework that consists of governance objectives but does not address the precise method required to achieve them. For example, COBIT covers a broad range of governance issues including security but leaves other standards such as ISO/IEC 27000 to provide the detail regarding how to achieve specific objectives. The relationship between COBIT and ISO/IEC 27000 is illustrated in the following figure.

Figure 29: Relationship Between COBIT and ISO/IEC 27000



Source: Created on behalf of IU (2019).

As seen in the preceding figure, to properly incorporate ISO/IEC 27000 into COBIT, it must be clearly mapped into all COBIT management areas, specifically APO, BAI, DSS, and MEA. The following table provides an example of how the ISO/IEC 27001 standard control objectives can be mapped to COBIT processes.

Table 5: ISO/IEC 27001 Standard Control Objectives Mapped to COBIT Processes

COBIT Process References	ISO/IEC27001 Control Objectives
APO01 Manage IT management framework	<ul style="list-style-type: none"> • Management commitment • Organization of information security
APO02 Manage strategy	<ul style="list-style-type: none"> • Establish the ISMS

Source: Created on behalf of IU (2019).

 **SUMMARY**

Although IT governance is a part of the general organization's governance, it also contains various interrelated components. These components cover different aspects of organization IT resources and operations, and together they form the foundation of the organization's IT governance and management. In this section, several key components were discussed, including quality management, process maturity, service management, enterprise architecture, and information security, with the focus on their relationships with IT governance.

The individual governance framework components must not be viewed in isolation. They are closely linked together to form the governance foundation. For example, no governance can be effective without quality management, as all the products and services that are under the governance's control must have the management processes associated with quality. Process is the fundamental building block of activities that deliver designed outputs, and must be constantly monitored for its performance and improvement. IT service management is the front-facing interface for users, and it must be managed based on IT governance core principles. Effective and efficient IT management cannot be established without a holistically planned, designed, and built IT infrastructure, covering the enterprise end-to-end. That is the main focus for enterprise architecture framework. Lastly, IT security plays an important role in any IT governance, and every organization must make it a top priority.

A broad and high-level understanding of various key components within IT governance can provide important insights with respect to the governance itself. This knowledge should greatly enhance understanding, planning, establishing, and improving IT governance.

UNIT 5

DATA PROTECTION AND IT SECURITY

STUDY GOALS

On completion of this unit, you will have learned ...

- to identify IT security threats.
- to apply countermeasures such as firewalls and spread security awareness.
- basic data protection concepts.

5. DATA PROTECTION AND IT SECURITY

Introduction

As the world has become more and more dependent upon information, the security and protection of information has been elevated in its importance within organizations. Information security is one of the top IT governance components, especially in light of some large-scale security breaches by major corporations reported in recent times. While IT governance lays the foundation for an organization to align their IT investment and resource allocation with their mission, information security provides the necessary framework for IT governance to fulfill its core objectives: to maximize value creation, maximize resource utilization, and minimize risks.

Data protection and information security covers a broad range of topics, from legislation, compliance, policy, procedures, risk management, and various technology-related matters to human behavior. It is a challenge for any organization to have advanced knowledge in just one of these areas, let alone have expertise in all these areas. However, in order for IT governance to be effective, each of these topics that relate to information security must nevertheless be well understood.

In the following sections, some of these key data protection and information security components will be discussed, including principle concepts, standards, threats, and countermeasures, along with certain technologies that are associated with security. This discussion will of course be conducted from the perspective of IT governance.

5.1 Data Protection

The main objective of data protection is to ensure that private data are protected against unauthorized access and modification. Specifically, data protection ensures the right to privacy of individuals and that any private data is used appropriately by organizations that collect it.

Data protection is related to IT security and to some extent uses the same methods and tools. Nevertheless, the two concepts start from very different perspectives: data protection is concerned with protecting individuals (customers, employees, etc.) against misuse of their personal data, including misuse by the company under consideration. An important part of data protection therefore is the protection against the company itself, which is why most countries have introduced appropriate legislation to enforce that this is implemented. IT security, on the other hand, is mainly concerned with protecting the company's IT assets against external threats such as hackers, viruses, and also accidental damage such as fire or floods. There are several industry standards and legal frameworks that specifically address data privacy and data protection-related topics and issues. Some well-known data privacy protection standards include ISO/IEC 29100 and the Payment Card Industry Data Security standard (PCI DSS) while some of the most significant privacy pro-

tection legislature includes the European Union’s General Data Protection Regulation (GDPR) and the United States Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Acts (FERPA). The following discussion focuses on two of these: the ISO/IEC 29100 and GDPR.

ISO/IEC 29100

The specific requirements that data protection needs to accomplish are centered on privacy. ISO/IEC 29100 (ISO 2011) is the international standard that provides “a high-level framework for the protection of **personally identifiable information (PII)** within information and communication technology (ICT) systems”. ISO/IEC 29100 establishes a privacy framework by specifying common privacy terminology, defining roles and responsibilities, describing privacy requirements, and referencing privacy principles. Roles, interactions, safeguard requirements, policies, and controls are considered by ISO/IEC 29100 as basic elements of the privacy framework.

The main objective of ISO/IEC 29100 is “to meet legal and regulatory requirements, practice corporate responsibility, and enhance consumer trust” (ISO 2011). It establishes the privacy protection framework between the PII data provider and the PII receiver. Just like other information components, PII has its own life cycle that moves through the stages of collection, storage, usage, transfer, and finally destruction. At each stage of the PII life cycle, ISO/IEC 29100 uses privacy principles to establish privacy controls that are specific to the requirements of that stage.

ISO/IEC 29100 refers to the following eleven principles of data privacy:

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention, and disclosure limitation
6. Accuracy and quality
7. Openness, transparency, and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

These principles can be used, along with other framework elements, to assist the design, development, and implementation of privacy policies and controls as well as the monitoring and auditing of data privacy management.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a major piece of legislation that addresses data privacy protection within the European Union (EU) and the European Economic Area (EEA). It replaces the earlier Data Protection Directive of 1995. The purpose of

Personally Identifiable Information (PII)

Any information that might be linked to an individual. The linking may be direct (e.g. by giving the name or social security number) or indirect (by including other attributes that are sufficient to identify the person).

the GDPR is to provide a set of standardized data protection laws across all the member countries in order to protect the “fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data” (2016).

Instead of personally identifiable information, GDPR uses the term personal data which it defines as “any information relating to an identified or identifiable natural person (data subject)” (2016). The GDPR provides further clarification of the concept of a data subject: “an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (2016). The GDPR clearly defines the ways in which the privacy rights of every EU citizen must be protected and how and under what controls that individual’s personal data can and cannot be used through its key principles.

In term of roles and responsibilities, the GDPR defines a “data controller” as an entity who “determines the purposes and means of the processing” and a “data processor” as an entity who consistently acts only “on behalf of the data controller”. The GDPR places responsibility on both the data controller and data processor to comply with the legislation and demonstrate compliance, and it carries significant penalties for those who do not comply.

The GDPR sets out seven key principles, which are similar to the data privacy principles described by ISO/IEC 29100:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

These principles are the core of the GDPR and provide the foundation for the rest of the legislation. They don’t provide specific rules, rather, they are principles designed to guide general data protection. However, these principles can be used as to guide compliance and can be used as a compliance checklist. For example, transparency requires that the subject must be informed of what data processing will be done, fairness means that the data processed must match with how it has been described, and lawfulness means that the processing must meet the tests described in the GDPR.

Compliance with GDPR requires the full attention of an organization’s top leadership as it has the potential to fundamentally change the existing data usage culture in the organization as well as its data protection policies and procedures. GDPR compliance thus requires collaboration between people, processes, and technology.

With modern society becoming increasingly dependent upon data, protecting it (particularly individuals' private data) has become a high priority. Failure to safeguard private data can have devastating consequences. In recent years, several major international organizations have suffered from data protection failures including Sony (77 million PlayStation accounts impacted), Yahoo (3 billion accounts impacted), Marriott International (500 million accounts impacted), Equifax (143 million accounts impacted, many of which included credit card data), and JP Morgan Chase (over 80 million accounts impacted). Since private data is valuable on the black market, this type of cyberattack will undoubtedly continue and intensify in the future. Recognizing the importance of data privacy and the need to provide safeguards to protect data is the first step towards establishing an organization's data protection governance and framework. Industry standards and governmental regulations and compliances are essential foundations for such governance.

5.2 IT Security Management

The goal of IT security management (ISM), as defined by ITIL (AXELOS) is "to align IT security with business security and ensure that information security is effectively managed in all service and service management activities". ISM is part of the overall IT management and is therefore considered to be under the same umbrella of IT governance. Specifically, ISM is governed by a set of "security governance", as in the COBIT framework. Like other areas of IT governance, security governance is driven by business requirements. ISM needs to fully understand business security environment, including business security policies, operational security requirements, current and future security needs, regulatory compliances, and risk management requirements.

IT Security Management Establishment

The actual establishment of an organization's security management requires a series of actions to take place that use best practices documented in the ISO/IEC 27000 series and ITIL as a guide. The process to establish an information security management system (ISMS) begins with security governance, followed by objectives, scope, information asset analysis, information risk analysis, security controls, and finally the system itself. Each of these steps is now explained in greater detail.

Information security governance

Information security governance establishes the framework for security management, including formal policies, procedures, and other processes. The COBIT framework can be used for IT security management, providing a practical roadmap from governance processes to management processes. In order to properly set up IT security governance, an organization needs to review legal and compliance requirements; identify business needs; determine the risk management framework to be used; and align IT security with business objectives. The results of these actions will allow the organization to begin its planning phase for IT security management.

Information security management objectives

An organization can establish its information security objectives and requirements by examining the organization's overall business mission, strategy, and objectives. This process allows the organization to establish critical business infrastructure and operations, identify vulnerabilities and risks, and determine a risk management policy. Information security management initiatives must align with business objectives as dictated by IT governance.

Information security management scope

In line with ISO/IEC 27001, which provides well-defined general security measures and requirements, organizations should choose the specific and relevant components from the standards to create its security management system scope. This then becomes the basis for subsequent implementation processes. When determining the scope of information security management, it is important to systematically examine an organization's structure, people, processes, products, services, and business relations to determine what should be included and what should be considered beyond the scope of the system.

Information asset analysis

The next step is to evaluate information assets included in the security management scope. This requires an organization to conduct a systematic review and create an inventory to identify and record the information assets covered. Some asset categories are:

- hardware, including computers, servers, and data storage
- software, including business applications, database applications, and office products
- networks, including routers, switches, firewalls, and cable infrastructure
- communications, including telephony infrastructure and any call centers
- data, including both internal and customer information

Note that there are other asset categories which organization may need to customize as well.

Information security risk analysis

Following the information asset analysis, a risk analysis is carried out to identify the risks associated with each category. The IT risk assessment requirements must consider a number of factors, such as legal and regulatory requirements, business requirements, IT resources, and various IT operation processes, procedures, and staff.

Security Controls

Following risk assessment and analysis, the next step in establishing IT security management is to set up security controls. This is the stage where actual information security management is established. Security controls can include policies, procedures, processes,

guidelines, standards, and specific technology. One of the key success factors for IT security management is to have a well-constructed security policy with clearly defined objectives that are closely aligned with the organization's business objectives.

Security controls form the foundation of IT security management. The goal of IT security management is to effectively manage these controls to meet the IT security governance. Some of the key aspects of security controls and management processes include

IT security management at an organization level

IT security management starts at the organizational level. Security must be a top-down process, meaning that there must be a strong commitment from executive management to drive the security policy establishment and enforcement. Additionally, there need to be clear security management responsibilities and authority.

Physical and environmental security

Physical security controls aim to prevent unauthorized physical access into secure areas while environmental security controls focus mainly on protecting against fire, flood, and other forms of environmental destruction.

Information system security

Information system security is a core part of the technological and procedural security controls of ISMS. This is a rather broad control structure, covering a wide range of technology and operations. First there is the information system hardware and software-related security. This involves all computer system hardware, system software, applications, storage, networking, messaging systems, and telephony systems. All these information system elements can pose vulnerabilities and thus require proper maintenance, patching, upgrading, backup, etc., in order to provide the system confidentiality, integrity, and availability necessary for operations.

Administrative and operational procedures are also critical ISMS components. Administrative procedures provide policy-based instructions for operational areas such as access management, data classification, data life cycle management, system life cycle management, and other policies that govern operations. Another major process to address is information security incident management. Incident response is a critical process; many organizations have a dedicated Incident Response Team (IRT) to act as the first responders to any detected security incidents. The IRT provides security alerts, tracks and reports incidents, and coordinates activities according to a set of incident response procedures.

IT security management has its own life cycle and requires continuous improvement. As a result, there needs to be a performance evaluation process to monitor the entire system and measure performance against specific metrics, just like any other IT systems. An internal auditing process should be established and audits should be conducted regularly. As previously discussed, information security is a moving target; as technologies constantly evolve, so too do potential vulnerabilities and risks.

Overall, IT security management encompasses a number of elements, from governance to management, from policies, procedures, processes, standards, and best practices, to auditing and compliance. The best resources to guide the establishment of ISMS are COBIT, ITIL, and the ISO/IEC 27000 series. Organizations need to pay close attention to their IT security management establishment, operations, and improvement, as the security management is one of the most critical components of IT infrastructure for organizations.

5.3 IT Security Threats and Attack Scenarios

One of the key IT security management processes is assessing vulnerabilities and risk. It is very important to identify, categorize, and analyze any potential IT security threats; only then can responses and countermeasures be taken. This process, sometimes referred as “attack surface analysis”, involves recognizing all points where vulnerabilities are located and identifying which types of threats could exploit these vulnerabilities. The types of attack surfaces include physical, network, and software. The first step of attack surface analysis is to identify and map out the surfaces, which we will now discuss in detail.

IT Security Threats

Information security threats and attacks are numerous in origin, with various targets, and are conducted for different reasons. Motives behind the attacks are as varied as the types of attackers. The “basic user” (e.g., script kiddie, hobbyist) is an unskilled individual who uses already established and potentially automated techniques for attacking and who has access to common hardware, software, and Internet connectivity. This type of attacker often randomly attacks websites or organizational infrastructure simply for the thrill (and perhaps bragging rights amongst peers).

The “insider” has various access privileges within the organization. Such attackers specifically target their own organizations, typically for revenge as disgruntled employees or to obtain information for personal gain. A “hacktivist” (a portmanteau of “hacker” and “activist”) uses technology and hacking abilities to promote political or social agendas. This type of attacker does not seek personal or financial gain, but instead seeks to disrupt services and bring attention to specific political or social causes. Hacktivists typically target large corporations and governments.

“Terrorists” (or cyberterrorists) have premeditated political motivations to attack information and systems, which results in violence against non-combatant targets, causing severe disruptions or widespread fear in communities. They tend to target less resilient civilian IT infrastructures such as utilities, mass transit, and governments. Meanwhile, “cybercriminals” (or “**black-hats**”) possess advanced security knowledge and skills and take advantage of known vulnerabilities or find new vulnerabilities. They are typically motivated by financial gain, seeking to steal information to sell on the black market, blackmail an individual or an organization, or engage in espionage.

The “nation-state” attacker is sponsored by a governmental entity and typically runs sophisticated operations with highly-trained and highly-skilled IT professionals. Targets are usually governmental and military intelligence, public infrastructure systems such as mass transit, power or water systems, and advanced commercial intelligence. The term “cyber warfare” is often used to describe these types of hacking activities.

The detailed mechanisms of information security threats vary, but all can be analyzed based on the information security triad: confidentiality, integrity, and availability. Cyberattacks can be directed at a single aspect or all three of these aspects. The types of actual threats and the ways that the threats are delivered are innumerable. Essentially any information technology component can be attacked or used to launch attacks on other information components. For a basic understanding of information security threats, a few of the most common types of attacks will now be discussed.

Malware

Malware is a generic term for any software developed for the sole purpose of creating a threat to the security triad. There are many forms of malware and the ways they are delivered to their target are varied. Some common ones include viruses, Trojans, logic bombs, worms, spyware, and ransomware.

- **Viruses:** This is the oldest and most common type of malware. A virus is a type of malicious code written to harmfully change the way that a computer operates. It has the ability to replicate itself and is designed to spread from one system to another. There are many types of viruses:
 - A macro virus is designed to infect applications such as Microsoft Word. It attaches to the application’s initialization sequence, so that when the application is opened, the virus executes its instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.
 - A file infector is designed to attach to an executable file (.exe) or masquerade itself as the legitimate .exe file. In either case, when the file is opened, the virus code is executed.
 - A system or boot-record infector is similar to a file infector but it attaches to the master boot record on hard disks. When the system is started, it will look at the boot sector and thus load the virus into memory.
 - A polymorphic virus will conceal itself through varying cycles of encryption and decryption to avoid common antivirus checks.
 - A stealth virus will take over system functions to conceal itself and compromise malware detection software.
- **Trojans:** This term refers to malicious code that hides within an application. A major difference between viruses and Trojans is that Trojans do not self-replicate.
- **Logic bombs:** A logic bomb is a malicious code appended to an application and triggered by a specific occurrence, such as a logical condition or a specific date and time.
- **Worms:** A worm is self-contained malicious code that propagates across networks and computers. It differs from a virus in that it does not attach to a host file. Worms are commonly spread through email attachments whereupon opening the attachment activates the worm program.

Black-hat vs. white-hat crackers

Black-hat refers to crackers that attack IT systems for malicious reasons (blackmail, espionage etc.). White-hat refers to crackers that attack IT systems on behalf of the owner of the system, identifying weaknesses and thus helping to protect against black-hat crackers.

- **Spyware:** This term refers to malicious code designed to monitor user activities and pilfer user data, such as a key logger. It usually invades computers through software downloads and peer-to-peer file sharing. Another version of spyware is adware which monitors a user's Internet traffic.
- **Ransomware:** This is a special type of malware that blocks access to the victim's data and demands a ransom to be paid in exchanging for unblocking the data.

Malware is constantly being created and thus represents a challenging and moving target. New malware that has not been identified by antimalware applications are commonly referred as "zero-day threats".

Denial-of-service

A denial-of-service (DoS) attack overwhelms a system's resources by flooding it with traffic to exhaust available resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can use multiple compromised devices to simultaneously launch an attack on a specific target, which is known as a distributed-denial-of-service (DDoS) attack. Unlike other types of attacks, DoS/DDoS attacks do not provide direct benefits to the attackers and are a pure attack on availability. DoS/DDoS attacks use enormous volumes of unclosed network connections, irregular data packets, and spoofing, or simply ping the host in order to eventually use up all available system resources. A technique called a Botnet is often used to accomplish DDoS attacks. Botnets are the thousands or millions of systems infected with malware under the hacker's control to launch simultaneous DDoS attacks.

Social engineering

Social engineering is a technique attackers use to deceive users into making security mistakes such as giving away sensitive information. It covers a broad range of malicious activities, accomplished through human interaction by means of psychological manipulation. Examples include emails and phone calls from attackers masquerading as trusted sources, e.g., management, hospital emergency rooms. Strictly speaking, social engineering is not technology-related; it is especially dangerous as it relies on human error, rather than technological vulnerabilities to achieve the attack. Mistakes made by humans are much less preventable, making them harder to identify than typical malware-based threats. Two common types of social engineering are phishing and spear phishing. Phishing is one of the most popular types of social engineering attacks. It is the practice of sending false communications, e.g., e-mails that appear to come from a trusted source. "Vishing" is a term used to describe phishing with voice calls. Spear phishing is a more targeted version of phishing. The attacker chooses specific individuals or organizations, and tailors messages to the characteristics of the individual or organization to include details such as job positions and contacts known to the victim to make the deception less conspicuous.

Man-in-the-middle

Man-in-the-middle (MITM) attacks, also known as eavesdropping attacks, occur when an attacker inserts themselves between a client and a server communicating with one another. Once the attacker interrupts the traffic, they can eavesdrop, filter, alter, and steal data.

SQL injection

A structured query language (SQL) injection attack inserts malicious code into a server that uses SQL, such as a database, in order to execute SQL commands that are not authorized. SQL injection has become a common issue with database-driven websites.

Cross-site scripting

A cross-site scripting (XSS) attack uses web resources to run scripts in the victim's web browser. The attacker injects a malicious code into a website, the code is then picked up by the victim's browser and executes on the victim's computer.

Information security threats exist within all forms of information technology-related infrastructure. Given the variety of attackers and the wide range of possible attacks, protecting information security is extremely challenging. As the FBI director Robert Mueller is famously quoted as saying: "There are two types of companies: those that have been hacked, and those who don't yet know they have been hacked" (2012). In recent times, the security attack surface is growing even larger and more and more big organizations have suffered major security breaches.

Over the years, many incidents of large-scale data loss have occurred, many of which were caused by hackers exploiting known system vulnerabilities and others by phishing techniques. But threats and attacks are not just limited to attacks on confidentiality; integrity and availability have also been the targets of many well-publicized attacks. For example, the use of Facebook to spread misinformation via hijacked or fake accounts causing major social upheaval is a classic breach of information integrity. A large scale DDoS attack in 2016 on DynDNS, a DNS service provider, causing major disruptions to major companies such as Twitter, Netflix, PayPal, and Pinterest, is emblematic of the type of attacks that target information availability.

All of these security threats and examples of distressing data breaches present a very serious reality for organizations operating in the information age. Organizations and IT professionals must remain ever-cognizant of the fact that information security is one of the most critical IT governance and management elements, deserving the highest priority in this information-driven age.

5.4 Countermeasures

Once information security governance has been established and policies are in place, one of the next actions should be to establish administrative and technical processes and procedures to bring information security into all IT practices. Prerequisites for creating and implementing security processes and procedures should already be in place, including the identification and classification of information assets, risk assessment and treatment plans, and a defined information security management system scope.

Security processes and procedures should follow the line of identified vulnerabilities and risks, and appropriate security controls to counter the threats should be associated with them. There are two major categories of countermeasures typically found in security policies: administrative countermeasures and technical countermeasures.

Administrative Countermeasures

Administrative countermeasures cover security controls that are for the most part non-technology-related; they focus on areas such as general organization culture, business operations, and human behavior.

- **Policies and procedures:** Policies provide structural security directives that executive management put in place for the entire organization. They address legal and regulatory compliance demands, business security objectives, and the general high-level security management framework. Procedures are derived from policies. They relate more to operational processes including business operations and IT operations.
- **Organizational structure:** Organizations need to establish a management chain-of-command that administers general risk management including information security management. This is important to facilitate clear responsibility and quicker response times in the event of a security incident. Organizations should consider whether to create an incident response team (IRT) and how to manage relevant aspects of performance, audits, etc.
- **Plan and review:** Security planning and reviews should be conducted on a periodical basis. Disaster recovery planning and business continuity planning (DRP/BCP) should include regular testing and updating as necessary.
- **Human resources:** A critical preventative security control is to have a comprehensive personnel management process and procedure on security concerns. Personnel controls should include job function-related security classifications and responsibilities, documented expected employee behaviors, new-hire orientations, penalties for violations, and employee separation or termination processes in the case of major breaches.
- **Awareness training:** Security policies and procedures need to be properly disseminated throughout the entire organization. For example, regular communication via an organization's intranet can be used to remind and update employees on security policies and procedures. Awareness training can be conducted in various formats, e.g., classroom training, lunch-and-learn sessions, and one-on-one coaching.

Administrative security countermeasures are usually preventative rather than reactive, but care needs to be taken to update procedures to correct outdated information or add new relevant information. Administrative security controls will form a major part of any compliance audit.

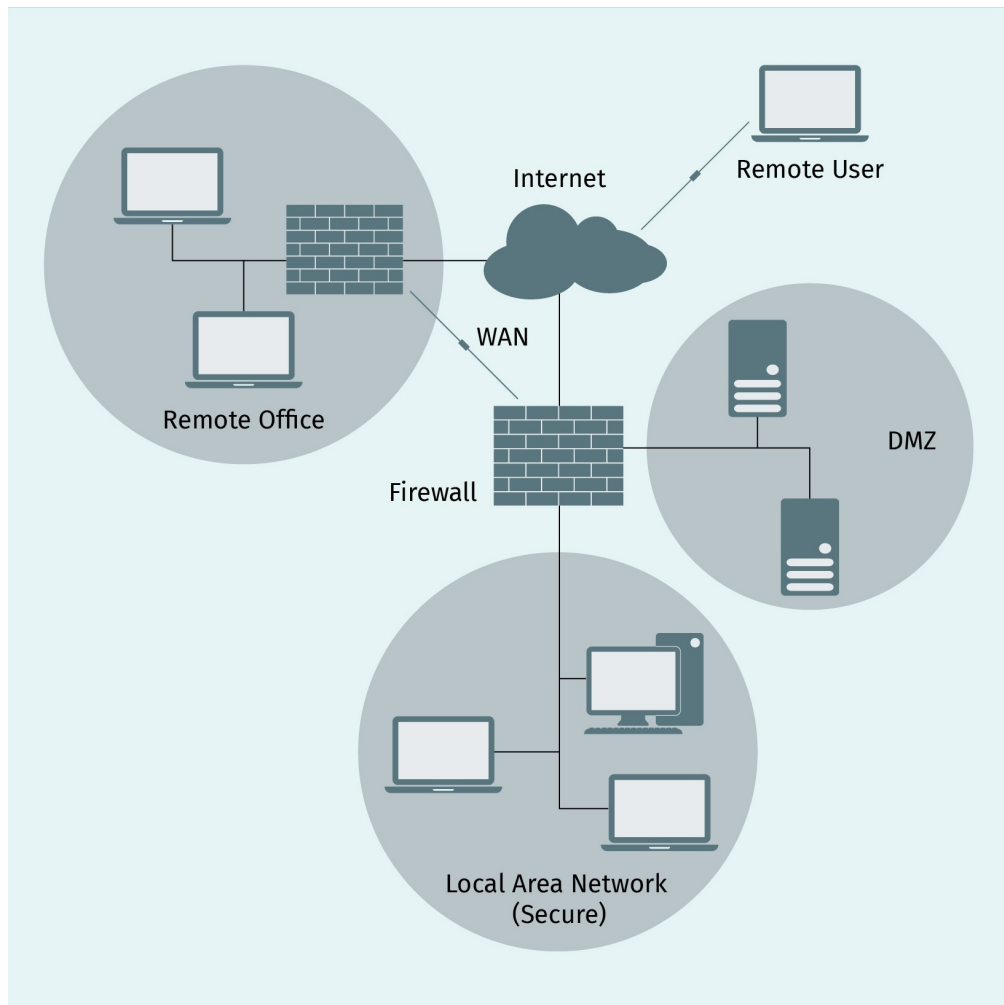
Technical Countermeasures

Every part of information system infrastructure has some level of vulnerability, from software to networks to communication. Therefore, technical security countermeasures are necessary to address a wide spectrum of threats and risks. The following discussion focuses on some of the key elements of technological measures that directly address security controls.

Networks

A typical organization's network infrastructure consists of four major components: (a) an internal network (Local Area Network, or LAN) for organization users, (b) a demilitarized zone (DMZ) for an organization's publicly accessible resources such as its website, (c) a connection with the general Internet, and (d) a connection to an organization's remote sites (Wide Area Network, or WAN) and remote users.

Figure 30: Common Organizational Network Schematic



Source: Created on behalf of IU (2019).

There are a number of security-specific countermeasures that can be implemented in the network environment.

Firewall and network segmentation

A firewall is a network device that controls network traffic based on security rules. A firewall separates network segments such as the LAN, DMZ, and Internet in a standard three-branch configuration. The LAN is the most private segment of an organization's network environment which only its own employees are allowed to access. The DMZ is semi-private network segment, where controlled and limited public access is permitted, such as the front-end of the organization's website and email system. The Internet segment is the open, non-private network. Should organization have other remote campuses, a WAN segment is necessary, which is connected via dedicated links or via a virtual private network. Perimeter (border) firewall controls the ingress and egress traffic, forwarding or denying

the network packets to their destinations based on established rules. There are often internal firewalls that segregate the private LAN further, e.g., at the junction between the LAN and datacenter.

Intrusion detection/intrusion prevention systems

An intrusion detection system (IDS) and intrusion prevention system (IPS) are both internal network monitoring devices that observe traffic and detect anomalies based on rules, network packet signatures, or baseline traffic patterns. Should anomalies be detected, the IDS will alert the network monitoring system and the IPS will alert and stop the suspicious traffic. Besides the network IDS/IPS, host-based IDS/IPSs are also available to protect individual computer systems. IDS/IPSs are critical countermeasures that protect private networks against malware such as viruses, worms, botnets, and other types of attacks that reside or originate within the private network.

Virtual private network

A virtual private network (VPN) protects traffic passing through unprotected network environments against eavesdropping or man-in-the-middle attacks in order to ensure confidentiality and integrity. A VPN uses encryption to establish a private network “tunnel” between two communication destinations. Network-to-network VPNs link two network segments together and host-to-host VPNs link two computers together.

Wireless networks (WLAN) face the same types of threats as wired networks, but they are also more susceptible to DoS and MITM attacks. The key countermeasure for a WLAN is to fortify wireless secure access points (APs) by a deploying stronger WPA (Wi-Fi protected access) protocol which utilizes more sophisticated data encryption and better user authentication than that of a WEP (Wired Equivalent Privacy) protocol. It can also be useful to deploy a rogue AP detection to shun unauthorized WLAN extensions.

Monitoring from all angles is a critical security operation that is not just limited to networks; it also covers individual systems, applications, and telecommunications. Monitoring provides baselines for detecting anomalies as well as for capacity planning. It assists in protecting against attacks on confidentiality, integrity, and availability.

Software

It is rather difficult to establish threat countermeasures for software applications from the end-user perspective, as the internal workings of applications are usually only known to the software developers. At the end-user level, two effective countermeasures are: (a) patching software library and (b) validating configurations. Attacks directly on software mostly involve in exploiting code vulnerabilities such as memory overflow, data reuse, code corruption, and information leaks. Countermeasures are applicable at development and testing stages.

Software countermeasures against the exploitation of application vulnerabilities include “stack canaries” which place an unpredictable value into a memory stack to detect possible buffer overflow attacks, “data execution prevention” (DEP) which mark the code seg-

ment non-writable and the data segment non-executable to avoid malicious code injection, and “address space layout randomization” (ASLR) which introduces artificial randomness into the memory, making harder for malicious code to be injected.

Data center

Data centers are highly sensitive facilities that require both physical and logical protection. Physical protections include access control, motion detection, surveillance, and power, fire, and flood protections. Logical protections are similar to both network and computer controls.

Telecommunications

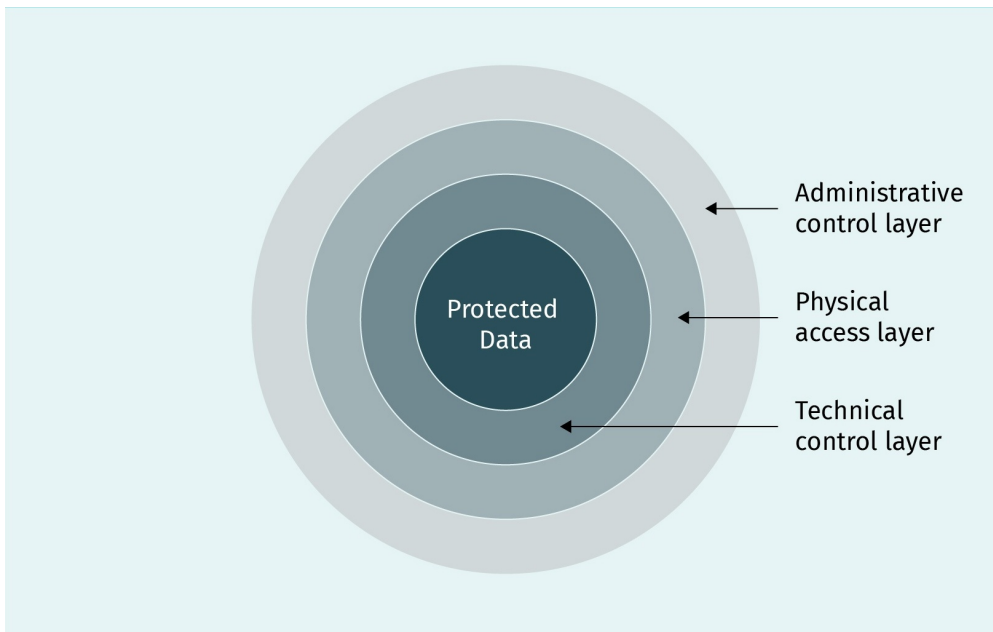
Telecommunications have unique attack surfaces, especially in the case of traditional nonVoIP lines which are vulnerable to wiretapping. For Centrex lines (on-premise private branch exchange (PBX) and key systems) physical access to equipment needs to be tightly controlled. For VoIP-based systems, including digital call-centers and converged messaging system such as voicemail, email, contact, presence, and video conferencing capabilities, threat countermeasures are similar to those of network controls and computer controls.

Mobile devices

Mobile devices present some of the toughest challenges for security controls, as they are often personally owned and can connect to organization’s network via cellular networks and WLAN. Optimizing security requires both administrative and technical controls. Security for mobile devices starts with a strong BYOD (“bring your own device”) policy that requires personal devices be patched, separating personal and organizational email accounts, using VPNs to connect from off premise, not allowing hot-spotting while connected to organization networks, using encryption on organization data, etc. Personal mobile devices need to be certified before joining organizational networks and automated posture assessments need to be utilized to verify that the devices meet an organization’s requirements.

As information security threats are constantly evolving, so too must countermeasures. None of the countermeasures discussed here are static; they must constantly monitored, reviewed, and updated. Threat countermeasures must be viewed in their entirety, with all parts working together in conjunction. The fundamental strategy for protecting against security threats is in-depth defense with layered protections, as illustrated in the following figure.

Figure 31: Information Security Defense



Source: Created on behalf of IU (2019).

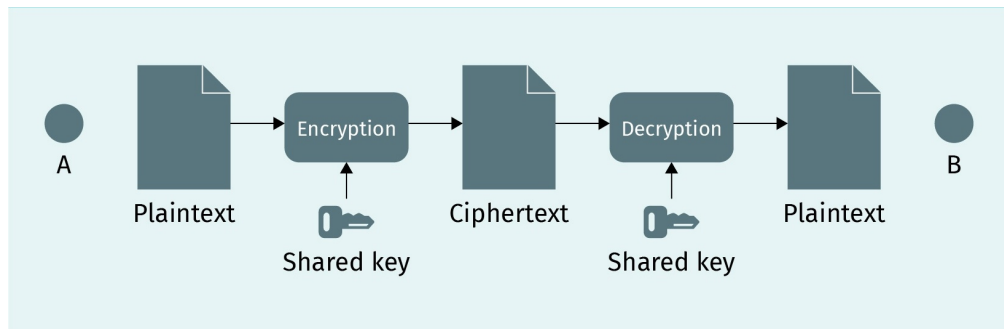
Organizations cannot guarantee 100 percent security, but with layered and redundant information security controls, the attack surface can be significantly reduced and the information security risk minimized, as required by IT governance.

5.5 Cryptography

One of the key technologies associated with information security is cryptography. Cryptography has a long history; it can be traced all the way back to ancient Egyptian and Roman times and was revived as a powerful military communication tool in the 20th century, e.g., in WWII with Germany's "Enigma machine". The fundamental and original goal of cryptography is confidentiality. Cryptography is a method of writing messages such that only intended receivers can understand the contents. Modern cryptography technologies have extended the protection afforded by cryptography to integrity as well as other information assurance features for data in transit (communications) and data at rest (storage).

The foundation of cryptography is encryption and its reverse: decryption. Encryption involves converting normal text (plaintext) into non-readable text (ciphertext) via an encryption algorithm (cipher) with the help of a special and unique variable or key (cryptovariable). Decryption is exactly the opposite, reversing ciphertext into original plaintext. The general process of encryption and decryption is illustrated in the following figure.

Figure 32: Encryption and Decryption



Source: Created on behalf of IU (2019).

Here is an example of how a simple encryption and decryption process works.

1. Plaintext: “meet me at 123 main street”
2. Algorithm: alpha-numeric circular right shift (shift cipher)
3. Key: 2. The combination of an alpha-numeric circular right shift with the key value of 2, makes a→c, b→d, ..., y→a, z→b; 1→3, 2→4, ...,9→1, 0→2. So the encryption results in ciphertext are: “oggv og cv 345 ockp uvtggv”
4. Decryption: alpha-numeric circular right shift with a key value of -2

The intended receiver needs to know both the algorithm and the key, in order to reverse (decrypt) the message. Anyone else can read the encrypted message but cannot understand the real contents.

The example provided is a symmetric encryption algorithm, meaning that the encryption and decryption key is the same. There are two pieces of knowledge revealed by this simple example. First, the algorithm must be known to both communication parties; the first principle of cryptography is that the algorithm is not a secret. All current cryptography algorithms are available to everyone. Second, the key must be known to both communicating parties and only to them. Otherwise, everyone can decrypt the ciphertext. The second principle of cryptography is that the key is a secret; the combination of these two principles is known as Kerckhoffs’s principle.

Combining cryptography algorithms and secret keys, along with necessary software and operational protocols, a complete cryptosystem comes to existence.

Symmetric Cryptography

There are two categories of encryption: symmetric and asymmetric. Symmetric encryption uses a single key to encrypt and decrypt the message, whereas asymmetric encryption uses one key to encrypt and another to decrypt. In symmetric encryption, the sender not only needs to send ciphertext but also the secret key which is usually sent via different means. Symmetric encryption has the advantage of simplicity, making it much easier and faster to deploy.

Symmetric cryptographic algorithms have two major encrypting techniques: stream and block ciphers. Stream cipher converts one symbol of plaintext directly into a symbol of ciphertext. Block cipher encrypts a group of plaintext symbols as one block. For example, simple substitution is an example of a stream cipher whereas the transposition of one row of data in a single step is a block cipher.

Symmetric cryptography has one major hurdle to overcome: how to securely share the secret key between two communicating parties. This problem was addressed by the Diffie-Hellman-Merkle (DHM) key exchange algorithm. DHM is a multiple-step exchange process that allows two parties that have no prior knowledge of each other to exchange a secret key over public communication media. The algorithm uses the modular calculation, which is easy to calculate but extremely difficult to reverse. This allows the two parties to begin with a non-secret pair of related prime numbers (modulo) and then each party chooses its own secret to modularly calculate and exchange the intermediate results until a common secret is reached.

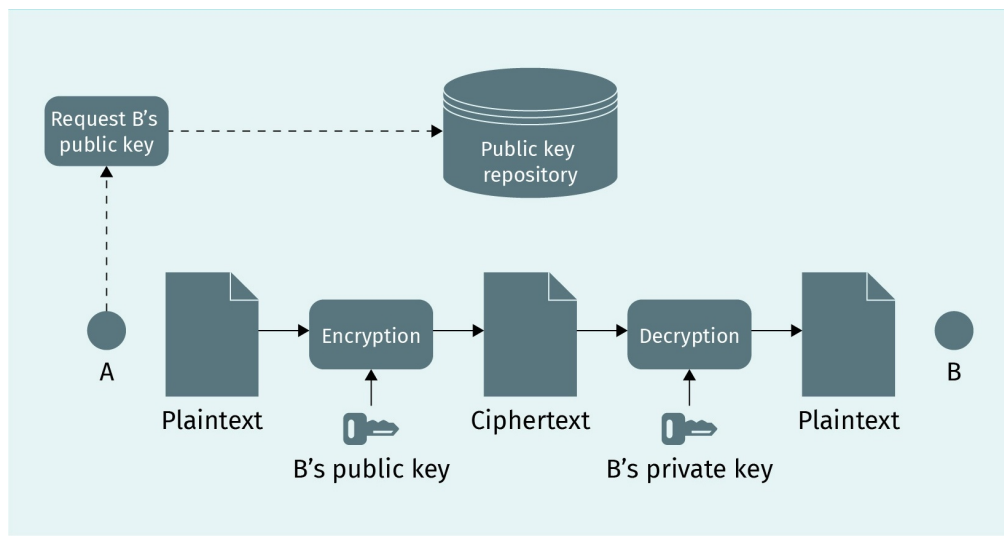
The main disadvantage of the symmetric cryptography remains key management. When a large number of senders and receivers are involved, the task of constantly managing and updating keys becomes extraordinarily difficult, as each communication pair needs to have a unique key which is different from other pairs.

Asymmetric Cryptography

To address the difficulties of symmetric encryption, asymmetric encryption-based cryptography was developed to solve the issue of key management, making cryptography much more practical and secure. Asymmetric cryptography, also known as public key cryptography, uses a pair of related keys: a public key and a private key to encrypt and decrypt data. The public key is often deposited in a trusted repository and thus can be made available to general public while the private key is kept by the sender. The cryptography system based on public key cryptography is called public key infrastructure (PKI), which contains certificate authority (CA), and other elements that binds the public keys to their rightful identities, e.g., organizations.

In an asymmetric encryption algorithm, a pair of different yet related keys is generated. The asymmetric nature of the pair means that messages that are encrypted by one of the key pair can only be decrypted by its counterpart. Thus messages encrypted by the public key can only be decrypted by the corresponding private key, and messages encrypted by the private key can only be decrypted by the corresponding public key. Obviously the latter is not meant for encrypting messages per se, but it is used to verify authenticity. Because of this asymmetric character, not only confidentiality, but also integrity, authenticity, and non-repudiation can be provided by this type of cryptography. Confidentiality through asymmetric encryption is illustrated in the following figure.

Figure 33: Asymmetric Encryption



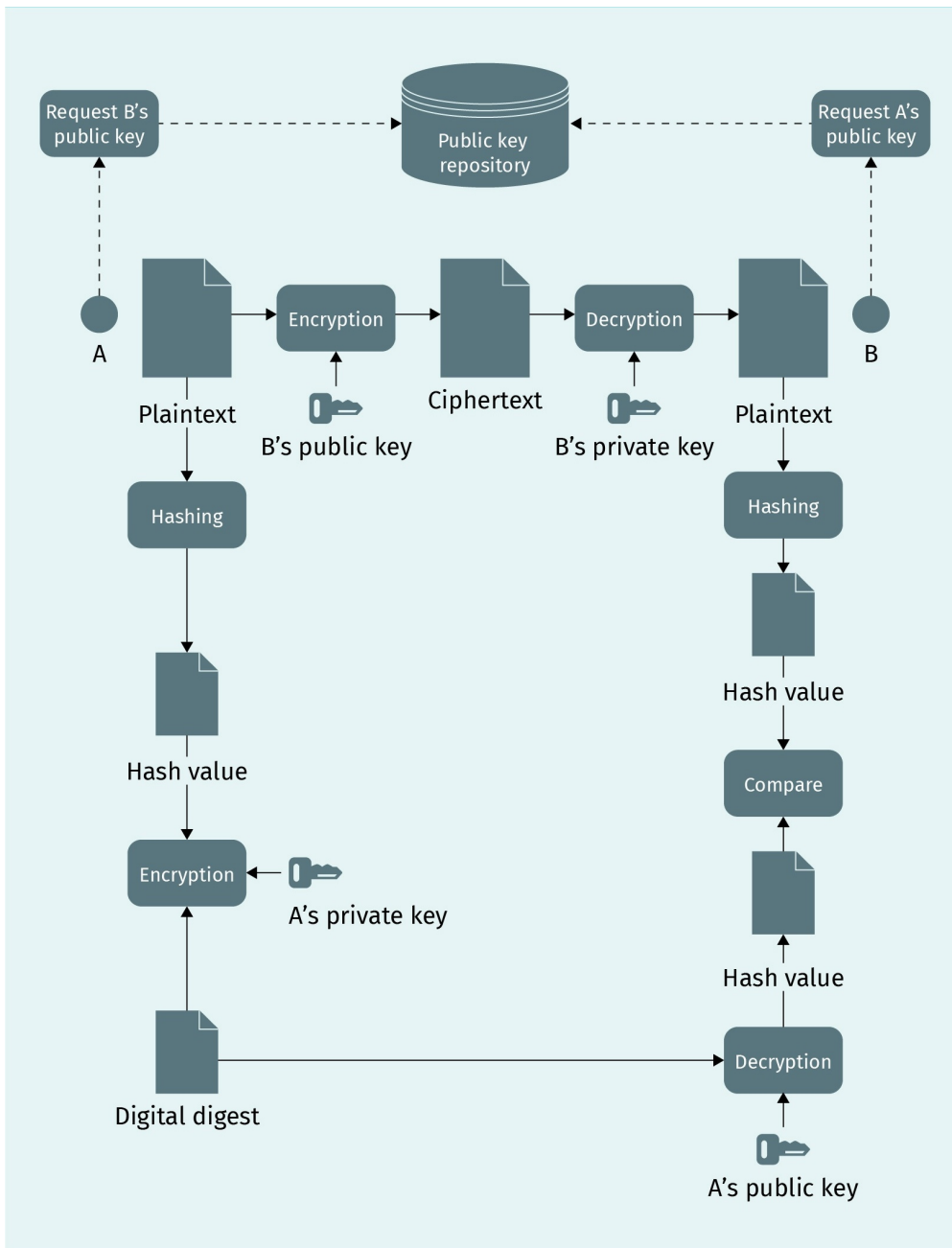
Source: Created on behalf of IU (2019).

We can see in this figure that the sender, A, first requests a copy of B's public key through a CA, then it encrypts the message with B's public key. After receiving the ciphertext from A, B then uses its private key to decrypt the message. Since B is the only one who has the private key, no one else can decrypt the ciphertext that A sent to B. With a public-private key pair, anyone who wants to send and receive confidential data needs only to maintain a single pair, regardless how many different parties it needs to communicate with.

Before other features of asymmetric encryption can be discussed, another important concept requires an introduction: hashing. Hashing uses mathematical functions (hash function) to transform any arbitrary size of data to a fixed size value called a hash value (hashes or digits). Hashing is very sensitive, so much so that any small change in the original data, e.g., a bit flip, will result in different hash values. Hashing is also irreversible, meaning hash values cannot be used to find the original data. In encryption algorithms, hashing plays a key role in integrity, authenticity, and non-repudiation. Hashing can be incorporated into cryptography.

The entire asymmetric cryptography process with hashing is illustrated in a very simplified process flow diagram.

Figure 34: Simplified Asymmetric Cryptographic Process Flow



Source: Created on behalf of IU (2019).

We can see in the figure that the top flow ensures that B receives a confidential message from A. But how can B be assured that: (1) the message has not been tampered with along the transmission, (2) the message is indeed from A, and (3) A cannot later deny the sending of the message? The second flow is added to address these three concerns. First, A hashes the original message into a hash value, which is then encrypted with its own private key. A then sends this extra piece of information (digital digest or digital signature)

along with the original ciphertext to B. B then carries out two additional operations. The first is to decrypt A's digital digest with A's public key, which results in the original hash value that A created from the original message. The second operation is to hash the received and decrypted original message to create another hash value. B then compares the two hash values. If the two hash values are an exact match, then B can draw the following three conclusions simultaneously:

1. The message has not been altered along the transmission. If it had been tempered with, the hashing is so sensitive and consequently the resulted hash value would be different from what A has created from the original message (thus confirming integrity).
2. The message is authentic as A is the only one who has A's private key. Otherwise, B would not have been able to decrypt the digital digest with A's public key (thus confirming authenticity).
3. Because A is the only one who can use A's private key, A cannot claim that someone else sent the original message (thus ensuring non-repudiation).

Confidentiality, integrity, authenticity, and non-repudiation can be verified through asymmetric cryptography, as demonstrated by this simplified example of an asymmetric cryptographic transaction. In practice, the encryption and decryption are carried out in much more complex exchanges, and there are different hashing mechanisms involved. In addition, asymmetric cryptography and symmetric cryptography methods are very often used together (hybrid cryptosystem) through various applications and protocols to take advantage of both types of cryptography. For example, asymmetric encryption can be used to deliver symmetric keys that are used to encrypt the original message, thus adding more complexity to the process while solving the key sharing problem associated with symmetric cryptography.

There are various types of cryptography and hashing algorithms. A brief description of several of the most commonly deployed ones now follows.

- Symmetric cryptography
 - DES (Data Encryption Standard) is a block cipher that uses a 56bit key. Its successor, Triple DES (3DES), uses three such keys in certain sequences. There are also older symmetric algorithms that are largely being phased out. 3DES is still used in hardware encryption solutions.
 - AES (Advanced Encryption Standard) is a block cipher that uses 128-, 192-, and 256-bit-length keys with multiple rounds of encryption to add greater strength.
 - DES is no longer secure and therefore rarely used today, while 3DES is still used in hardware encryption solutions.
- Asymmetric cryptography
 - RSA (Rivest–Shamir–Adleman) is one of the first, and a widely-used PKI asymmetric cryptographic algorithm. The most complex part of RSA is its public and private key generation algorithm. Two large prime numbers are generated using the Rabin-Miller primality test algorithm, then modular operations are used to generate public and private key pairs. The security of RSA depends on the fact that while it is quite easy to

multiply to large prime numbers, it is in practice impossible to factor the result, i.e. to derive the prime numbers given their product, assuming that the prime numbers are sufficiently large.

- DSA (digital signature algorithm) refers to a standard for digital signatures. It uses a different algorithm for signing and encryption to RSA. Along with RSA, DSA is one of the most preferred digital signature algorithms currently in use.
- ECC (elliptic-curve cryptography) is the latest encryption method. Its key generation and algorithm are based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography, and is therefore ideal for mobile communication devices.
- Hashing
 - The MD5 (message digest) algorithm is a widely used hash function producing a 128bit hash value. With known vulnerabilities, MD5 is not widely used in cryptography nowadays.
 - SHA (secure hash algorithm) is a family of hashing algorithms with significantly different core methods. The two operational versions, SHA-2 and SHA-3, each has a variety of final digest value (e.g., 224-, 256-, 384-, or 512-bit-length), and different rounds to calculations.

Cryptography Applications

In actual communication applications, cryptography is embedded in various types of communication protocols. Some of the common protocols include the following:

- Internet protocol security (IPSec): IPSec works at the Internet layer, one of the communication layers within the open systems interconnection (OSI) model, using a combination of asymmetric and symmetric encryptions. IPSec provides encryption and authentication. Common applications include virtual private networks (VPNs).
- Secure socket layer/transport layer security (SSL/TLS): SSL/TLS works at the transport layer within the OSI model using a combination of asymmetric and symmetric encryptions. Popular applications include secure web browsing (“https://”) and VoIP.
- Pretty good privacy (PGP) and OpenPGP: PGP/OpenPGP is an open-source encryption protocol, using a combination of asymmetric and symmetric encryptions. PGP/OpenPGP is commonly used for signing, encrypting, and decrypting texts, e-mails, files, and hard drives.
- Secure/multipurpose Internet mail extensions (S/MIME): S/MIME is designed to provide confidentiality, integrity, authenticity, and nonrepudiation for emails. S/MIME uses a combination of asymmetric and symmetric encryptions.
- Secure shell (SSH): SSH uses a combination of asymmetric and symmetric encryptions, mostly for secure remote access. SSH is another commonly-used VPN technology.

The main objective of cryptography is to keep secrets secret, i.e., to maintain information confidentiality. This objective has been extended to several other key information assurance aspects, including integrity, authenticity, and non-repudiation. As information security has become a top priority in IT governance, the technologies that support security management require increasing attention from IT management. Among these technologies, cryptography is a key player. Technologies involved in cryptography are rather com-

plex. However, with a high-level overview, organizations should be able to understand the principles, applicable uses, and general process for implementing this important security tool.



SUMMARY

IT security and data protection are becoming more vital every year. In order for an organization to fulfill its core objectives, it must allocate enough resources to this area, lest it become the latest professional example in a string of high-profile data breaches. IT security and data protection encompass many seemingly disparate areas, which must be properly understood and implemented according to the organization's needs. These include legislation, compliance, policy, procedures, risk management, and some human-related factors. IT security threats can come in many forms, including malware, denial-of-service, and even social engineering. Thus, it is not enough to only prepare for traditional infiltration pathways; an organization must constantly reevaluate its countermeasures. A basic requirement for success is an understanding of cryptography, and the updating of technology on an ongoing basis.

BACKMATTER

LIST OF REFERENCES

- Asgarkhani, M., Cater-Steel, A., Toleman, M., & Ally, M. (2018). A conceptual model to evaluate the effectiveness of information technology governance. In V. Ribiere (Ed.), *ICMLG 2018 Proceedings of the 6th International Conference on Management Leadership and Governance* (pp. 41–50). Sonning Common: Academic Conferences and Publishing.
- ASL BSL Foundation. (2012). *ASL2: A framework for application management*. Hertogenbosch: Van Haren Publishing.
- Buckby, S., Best, P. J., & Stewart, J. D. (2008). The current state of information technology governance literature. In A. Cater-Steel (Ed.), *Information technology governance and service management frameworks and adaptations* (pp. 1–43). Hershey, PA: Information Science Reference (IGI Global).
- Carr, N. G. (2003). IT doesn't matter. *Harvard Business Review*, 81(5), 41–49.
- CMMI Institute. (2019). CMMI Institute homepage [website]. Retrieved from <https://cmmiinstitute.com/>
- Coca Cola. (2013). Mission, vision and values [website]. Retrieved from <https://www.coca-cola.co.uk/about-us/mission-vision-and-values>
- Darweesh, M. S. (2015). Correlations between corporate governance, financial performance, and market value (Unpublished doctoral dissertation). Walden University, Minneapolis, Minnesota.
- De Haes, S., & Van Grembergen, W. (2015). *Enterprise governance of information technology: Achieving alignment and value*. New York, NY: Springer.
- Deutsche Bank. (2019). Corporate governance at Deutsche Bank [website]. Retrieved from <https://www.db.com/ir/en/corporate-governance-at-deutsche-bank.htm>
- Encyclopedia Britannica. (2019). Utility and value [entry]. Retrieved from <https://www.britannica.com/topic/utility-economics#ref189355>
- Eur-lex. (2016, May 4). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [document]. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504>
- Federal Election Committee. (2018). FY 2018-2022 Strategic plan [report]. Retrieved from https://www.fec.gov/resources/cms-content/documents/FEC_Strategic_Plan_FY_2018-2022.pdf

- Fowler, F. J. (1995). *Applied Social Research Methods Series* (Vol. 38). Thousand Oaks, CA: Sage Publications.
- Hoyle, D. (2018). *ISO 9000 quality systems handbook-updated for the ISO 9001: 2015 standard: Increasing the quality of an organization's outputs* (7th ed.). Abingdon-on-Thames: Routledge Publishing.
- Gartner. (2019). IT governance (ITG) [entry]. Retrieved from <https://www.gartner.com/it-glossary/it-governance/>
- Google. (2014). About [website]. Retrieved from <https://about.google/>
- GreyCampus. (n.d.). IT service continuity management [guide]. Retrieved from <https://www.greycampus.com/opencampus/itil-foundation/it-service-continuity-management-it-scm-goals-and-objectives>
- International Organization for Standards (ISO). (2011). *Information technology: Security techniques: Privacy framework* (Standard no. 21900). Retrieved from <https://www.iso.org/standard/45123.html>
- International Organization for Standards (ISO). (2013). *Information security management systems* (Standard no. 27000). Retrieved from <https://www.iso.org/isoiec-27001-information-security.html>
- International Organization for Standards (ISO). (2015). *Quality management systems: Fundamentals and vocabulary* (Standard no. 9000). Retrieved from <https://www.iso.org/standard/45481.html>
- International Organization for Standards (ISO). (2015). *Quality management systems: Requirements* (Standard no. 9001). Retrieved from <https://www.iso.org/standard/62085.html>
- International Organization for Standards (ISO). (2015). *Quality management principles* (2nd ed.). Retrieved from <https://www.iso.org/publication/PUB100080.html>
- International Organization for Standards (ISO). (2017). *Guidance on Social Responsibility* (Standard no. 26000). Retrieved from <https://www.iso.org/standard/42546.html>
- International Organization for Standards (ISO). (2017). *Systems and software engineering: Vocabulary* (Standard no. 24765). Retrieved from <https://www.iso.org/standard/71952.html>
- International Organization for Standards (ISO). (2018). *ISO 31000:2018. Risk assessment* (Standard no. 31000). Retrieved from <https://www.iso.org/iso-31000-risk-management.html>
- Information Systems Audit and Control Association. (n.d.). Audit [entry]. Retrieved from <https://www.isaca.org/Pages/Glossary.aspx?tid=1095&char=A>

- Information Systems Audit and Control Association (2012). *A business framework for the governance and management of enterprise IT* [website]. Retrieved from <http://www.isaca.org/COBIT/Pages/COBIT-5.aspx>
- Information Systems Audit and Control Association Germany Chapter (2017). *Implementation guideline ISO/IEC 27001:2013*. Berlin: dpunkt.verlag. Retrieved from https://www.isaca.de/sites/default/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf
- Information Systems Audit and Control Association. (2018). *COBIT 2019 framework: Introduction and methodology*. Schaumburg, IL: ISACA.
- Information Systems Audit and Control Association. (2018). *COBIT 2019 framework: Governance and management objectives*. Schaumburg, IL: ISACA.
- Information Systems Audit and Control Association. (n.d.). COBIT 5 for information security [website]. Retrieved from <http://www.isaca.org/cobit/pages/info-sec.aspx>
- IT Governance Institute. (2003). *Board briefing on IT governance* (2nd ed.). Rolling Meadows, IL: IT Governance Institute.
- Kaplan, R., & Norton, D. (1992). The balanced scorecard: Measures that drive performance. *Harvard Business Review*, 70(1), 71–79.
- Kneuper, R. (2018). *Software processes and lifecycle models*. Cham: Springer.
- Kock, N. (2008). *Encyclopedia of e-collaboration*. Hershey, PA: IGI Global.
- Lane, M. (2014, October 3). COBIT 5 and the balanced scorecard [blog]. Retrieved from <http://www.orbussoftware.com/blog/cobit-5-and-the-balanced-scorecard/>
- McCulloch, A. (2018, February 7). How and why to focus on value for customers in service management [article]. Retrieved from <https://www.axelos.com/news/blogs/february-2018/how-why-focus-value-customers-service-management>
- Merriam Webster. (2019). Value [entry]. Retrieved from <https://www.merriam-webster.com/dictionary/value>
- Pink Elephant. (n.d.). ITIL service lifecycle [website]. Retrieved from <https://pinkelephant.co.uk/it-service-management-2/service-lifecycle/>
- Sciforma. (n.d.). For IT teams [website]. Retrieved from <https://www.sciforma.com/customers/teams/it-project-management#tab2>
- Smits, D., & van Hillegersberg, J. (2018). The continuing mismatch between IT governance maturity theory and practice: A new approach. *Procedia Computer Science* 138, 549–560.

Stanford University. (2017). Strategic goals [website]. Retrieved from <https://businessaffairs.stanford.edu/strategic-goals>

The Federal Bureau of Investigation. (2012, March 1). Speeches [transcript]. Retrieved from <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>

The Open Group. (2018, November 1). Core concepts [guide]. Retrieved from <http://www.togaf.com/togaf9/chap02.html>

Thomas, M. (2019, January 1). Finally! A guide for tailoring a governance system for information and technology [guide]. Retrieved from <https://www.escoute.com/finally-a-guide-for-tailoring-a-governance-system-for-information-and-technology/>

Vodafone. (2013). Vision and approach [website]. Retrieved from <https://www.vodafone.com/content/sustainabilityreport/2015/index/vision-and-approach.html>

Zuhdi, A. F. (2018, September 28). COBIT [article]. Retrieved from <https://medium.com/@afawwazz/cobit-bc5b8d88ceae>

LIST OF TABLES AND FIGURES

Figure 1: IT Governance Implementation Life Cycle	28
Figure 2: General Assessment Process Flow	30
Table 1: Comparisons Between Strategic and Tactical Plans	37
Figure 3: Strategy, Tactics, and Operations	40
Figure 4: Incident Escalation Process	42
Table 2: Monitoring IT Services	46
Table 3: COBIT BSC for Enterprise Goals	48
Figure 5: Main Outcomes from EGIT	54
Figure 6: COBIT Governance and Management Domains	55
Figure 7: COBIT 2019 Design Factors	57
Figure 8: COBIT 2019 Goals Cascade	58
Figure 9: Enterprise Goals	59
Table 4: Enterprise Goals and Alignment Goals as Defined in COBIT 2019	60
Figure 10: Separation of Governance and Management	62
Figure 11: COBIT 5 Enablers	63
Figure 12: COBIT Core Model I	66
Figure 13: COBIT Core Model II	67
Figure 14: Other Standards and Frameworks Mapped into COBIT	69
Figure 15: The COBIT Implementation Roadmap	71
Figure 16: COBIT Process on Quality Management	77

Figure 17: Quality Control Chart	80
Figure 18: ISP 9001 Certification Process	85
Figure 19: ISO 9001	87
Figure 20: COBIT Capability Levels for Processes	89
Figure 21: COBIT Maturity Levels for Focus Areas	90
Figure 22: Sample Capability Profile	92
Figure 23: ITIL Service Life Cycle	94
Figure 24: ITIL Processes and Functions	96
Figure 25: TOGAF Architecture Metamodel	99
Figure 26: Architecture Development Cycle	101
Figure 27: COBIT Security Policy Framework	103
Figure 28: COBIT Information Security Principles	104
Figure 29: Relationship Between COBIT and ISO/IEC 27000	105
Table 5: ISO/IEC 27001 Standard Control Objectives Mapped to COBIT Processes	106
Figure 30: Common Organizational Network Schematic	120
Figure 31: Information Security Defense	123
Figure 32: Encryption and Decryption	124
Figure 33: Asymmetric Encryption	126
Figure 34: Simplified Asymmetric Cryptographic Process Flow	127



IU Internationale Hochschule GmbH
IU International University of Applied Sciences
Juri-Gagarin-Ring 152
D-99084 Erfurt



Mailing Address
Albert-Proeller-Straße 15-19
D-86675 Buchdorf



media@iu.org
www.iu.org



Help & Contacts (FAQ)
On myCampus you can always find answers
to questions concerning your studies.