PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

ABOU BEKR BELKAID UNIVERSITY – TLEMCEN
FACULTY OF ECONOMIC SCIENCE AND MANAGEMENT

Specialty: Management

Option: Enterprise Information System

TITLE: COBIT 5 AS A MECHANISM FOR IT GOVERNANCE

A CASE STUDY OF STATOIL COMPANY

Dissertation submitted in partial fulfillment of the requirements for the degree of Magister in management

Presented by:
Azzaoui Abdelbasset

Board of examiners:

Pr. Benbouziane Mohammed (President)	(University Of Tlemcen)
Pr: Bendiabdellah Abdessalam (Supervisor)	(University Of Tlemcen)
Mme. Dahou Khadra (Internal Examiner)	(University Of Tlemcen)
Mr: Hacini Ishak (External Examiner)	(University of Mascara)
Dr: Djennass Mostapha (Internal Examiner)	(University Of Tlemcen)

Academic Year: 2013 – 2014

Aknowledgments

In the name of Allah the most Compassionate, the most Merciful

I would first of all to thank my thesis supervisors Pr. Bendiabdellah and Mme Dahou for the continual support and guidance that helped to give this study a breadth.

Besides, I also owe a debt of gratitude to Pr. Benbouziane and my uncle Pr. Abderrahmane.

My appreciation and thanks are extended to the members of my thesis committee who will hopefully correct, evaluate and advice. Thank you for giving me some of your experience and thank you for sharing my own experience.

I wish to acknowledge all the staff of Statoil Company and In Salah Gas Join -venture.

Dedication

This work is dedicated to all whom I know with a special emphasize on: My parents who supported me during all the stages of my life from the date of birth up to now.

My brothers

My friends

My relatives.

SUMMARY:

CHAPTER 02: COBIT 5 AND ITS USE IN IT GOVERNANCE

INTRODUCTION

I. COBIT 5: A Conceptual Background

1-1-Historical evolution of COBIT

1-2-Mapping of COBIT 5 with the Most Relevant Related Standards and Frameworks

1-3- Principles of COBIT 5

II. COBIT 5 Fundamental Structures and Processes

2-1- COBIT 5 Goals Cascade

2-2- COBIT 5 Enablers

2-3- Process Reference Model

2-4- COBIT 5 Process Capability Model

III. Implementing IT Governance using COBIT 5

3-1- Primary Steps towards IT Governance

3-2- Implementation Life cycle Tasks, Roles and Responsibilities

3-3- Impact of COBIT 5 on IT Governance

CHAPTER 03: Case Study of Statoil Company

INTRODUCTION

3-1-Methodology

3-2-Statoil Management System

3-3- Corporate Governance

3-4-Data Analysis

3-5-Discussions and conclusions.

GENRAL CONCLUSION.

GENERAL INTRODUCTION

General Introduction:

"Information Technology (IT) has become pervasive in current dynamic and often turbulent business environments. While in the past, business executives could delegate, ignore or avoid IT decisions, this is now impossible in most sectors and industries" (**Peterson, 2003**).

Today Information Technology (IT) has become one of the most main parts of an enterprise; it has made managers aware of its fundamental role in enterprise success, and it has become a main component for most of great corporations. That's why; IT subject has influenced different management researchers. IT was submitted for a long time as a crucial resource allocated and managed by the company for the purpose of achieving its managerial goals. Currently, most enterprises have moved from management to governance. This latest is about two principles; **conformance** that serves the institutional dimension making the corporation more legislative, and the **performance** that improves efficiency and effectiveness, meeting the different stakeholders' goals. The governance necessitates a set of changes such as IT and business alignment, delivering value from IT, managing the associated risks, managing available resources and measuring the performance frequently. This has led to seek new large concept that combines governance with IT.

IT governance aims at assuring that IT is used effectively for company growth, costs' reducing, raising business flexibility level and the wise assets allocation (**Jukka Perko, 2008**). Thus, it makes insure that IT delivers more value from IT investments and enforcing IT role as a business enabler. IT Governance focuses on five domains: Strategic Alignment, Value Delivery, Resource Management, Risk Management and Performance Measurement.

Problem Statement and Questions:

IT Governance cannot be successful without an effective model, which makes it possible and effective. Many researches has been accomplished in the IT Governance enablers' area since its emerging until now, seeking the best way to enhance planning, organizing, implementing and assessing IT Governance. Thus, many frameworks and models had been appeared and they had showed different levels of impact on IT Governance. COBIT 5 (Control Objectives for Information and related Technology) is considered as the latest framework. COBIT 5 is a model of five domains; Evaluate, Direct and Monitor (EDM); Align, Plan and Organise (APO); Build, Acquire & Implement (BAI); Deliver, Service & Support (DSS); and Monitor, Evaluate and Assure (MEA). Each domain is a panel of many processes.

Statoil is the largest Norwegian company and it has its own IT Department which, among other activities, works with development and maintenance of software systems used in the oil and gas industry all around the world. To be competitive in the oil and gas market, Statoil continuously explores and takes advantage of new technologies and updates strategies and governance policies.

This project is written in cooperation with In Salah Gas Group (SONATRACH – British Petroleum-Statoil). This study aims to help Statoil map its use of COBIT 5, and IT Governance, and the connection between these two concepts. COBIT (the previous versions) and IT Governance as concepts have existed in Statoil for some time, but have newly been re-developed. COBIT 5 is a fairly new version in Statoil. This hopefully makes this study a useful analysis tool for Statoil. The study will compare Statoil's perception and implementation of the concepts; COBIT 5 and IT Governance, to perceptions and methodologies defined from literature.

As a consequence, the study problematic is summarized in the following question; "**Can COBIT 5 be determined as an adequate mechanism for effective IT Governance?**". This includes testing the study's model on Statoil, investigating the impact of COBIT 5 on IT Governance components and effectiveness, by responding the following research's questions:

Can COBIT 5 enhance the IT Governance stages?

- Can COBIT 5 enhance Strategic Alignment?
- Can COBIT 5 enhance Value Delivery?
- Can COBIT 5 enhance Resource Management?
- Can COBIT 5 enhance Risk Management?
- Can COBIT 5 enhance Performance Measurement?

Can IT Governance stages influence IT Governance effectiveness?

- Can Strategic Alignment influence IT Governance effectiveness?
- Can Value Delivery influence IT Governance effectiveness?
- Can Resource Management influence IT Governance effectiveness?
- Can Risk Management influence IT Governance effectiveness?
- Can Performance Measurement influence IT Governance effectiveness?

Importance of the study:

This study provides the searcher with theoretical and practical information and knowledge about the IT governance, highlighting the processes that aim to successfully and effectively planning, operating and evaluating IT governance project. So, it ensures formidable transition from theoretical approach to implementation, reflecting the organizational impact of COBIT 5 framework on IT governance effectiveness. It also kills ambiguities concerning the best IT Governance enhancer model that is applicable by great companies. This study may play a role in killing general lack of accountability and not enough shared ownership and clarity of responsibilities for IT services and projects. It may treat the problem concerning the potentially widening gap between what IT departments think the business requires and what the business thinks the IT department is able to deliver. It may discover critical success factors and weaknesses for some IT Governance adopter companies. It sets the light on the adequate organisational characteristics for IT Governance. It

investigates practically the level of dependency between IT Governance and COBIT 5. Because of its organisational characteristics, the use of Statoil Company as a model for empirical investigation may give more interest for the study.

Objectives of the study:

Through this thesis the searcher shall study and evaluate how COBIT 5 and IT Governance are related in Statoil. So, the goals derived in cooperation with In Salah Gas Group (SONATRACH-BP-Statoil) for this study is as follows:

1. Contributing to academic works about IT Governance and its mechanisms based on a literature review and updated documents;
2. Define and structure Statoil implementation of IT Governance using COBIT 5, and important relating concepts, governance mechanisms or infrastructures;
3. Discuss Statoil implementation of IT Governance using COBIT 5 with focus on use of frameworks and interaction between the concepts;
4. Discover Statoil IT Governance critical success factors;
5. Discuss possible weaknesses and inconsistencies Statoil implementation of the relevant concepts might reflect, and suggest improvements.
6. Contribute to the benchmarking periodic projects applied by SONATRACH and its partners.

Initial Literature review:

Most of the available studies tried to define IT Governance and its adequate mechanisms and frameworks, COBIT 5 has been chosen as the best mechanism for implementing IT Governance.

● IT Governance:

Luftman (1996) defined IT Governance as the **"Degree to which the authority for making IT decisions is defined and shared among management, and the processes managers in both IT and business organizations apply in setting IT priorities and the allocation of IT resources"**. So, he referred to IT decision making and the processes concerning IT resources allocation. **BearingPoint (2003)** established the IT alignment dimension that aims to achieve a new strategic goal, which is IT risk management. This led him to set the following definition for IT Governance; **"Structures and processes that ensure that IT supports the organization's mission. The purpose is to align IT with the enterprise, maximize the benefits of IT, use IT resources responsibly and manage IT risks"**. **IT Governance Institute (ITGI) (2003)** clarified the entities that are charged to apply and control ITG enjoying the board of directors and the executives. It defines ITG as **"Responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives"**.

Van Grembergen and De Haes (2003) tried to combine the second definition with the third one forming a global conception. From their viewpoint, ITG is "**Organizational capacity exercised by the Board, executive management, and IT management to control the formulation and implementation of IT strategy and in this way, ensure the fusion of business and IT"**. **Schwarz and Hirscheim (2003)** treated the ITG in an environmental context considering the external imperatives. They defines ITG as "**IT-related structures or architectures (and associated authority patterns), implemented to successfully accomplish (IT-imperative) activities in response to an enterprise's environment and strategic imperatives"**. **Simonsson and Johnson (2005)** defined IT Governance as; **"IT decision-making: The preparation for, making of and implementation of decisions regarding goals, processes, people and technology on a tactical and strategic level"**. So, they discussed the IT decision-making linking it with IT Governance features; they referred to the synergic linkage of processes, people and technology for the purpose of meeting strategic and tactical goals.

A new definition had been appeared in **2006** and adopted by **Weill and Ross**. Their study showed that IT Governance means **"Specifying the decision rights and accountability frameworks to encourage desirable behavior in using IT. IT governance reflects broad corporate governance principles, while focusing on the management and use of IT to achieve corporate governance goals"**. This latest trend reconsiders wise method enjoyed by the board of directors to deploy the IT seeming to achieve the governance goals. **Webb, Pollardand Ridley (2006)** integrated strategic alignment with control, accountability, performance management and risk management adopting a new approach that defines ITG as **"Strategic alignment of IT with the business such that maximum business value is achieved through the development and maintenance of effective IT control and accountability, performance management and risk management"**.

Each of the previous definitions focuses on one or some of the dimensions or domains of IT Governance. The latest studies benefitting from the past ones setting a conventional combination of five fundamental domains, like **Steven Hunt & Michael Nelson (2012)**, who summarized IT Governance domains (stages) as follows:

Strategic Alignment: Focuses on ensuring the linkage of business and IT plans; on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations.

Value Delivery: Is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.

Resource Management: Is about the optimal investment in, and the proper management of, critical IT resources: people, applications, information, and infrastructure. Key issues relate to the optimization of knowledge and infrastructure.

Risk Management: Requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organization.

Performance Measurement: Tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

Schwarz and Hirschheim (2003) and **Willcocks et al. (2002)** determined five indicators to measure IT Governance performance effectiveness; cost effective use of IT, effective use of IT for growth, effective use of IT for asset utilization, effective use of IT for business flexibility and compliance with legal and regulatory requirements.

Cobit (Control Objectives for Information and related Technology):

Koen Brand & Harry Boonen (2006) defined the Cobit as a **"model for control of the IT environment. It supports IT governance by providing a comprehensive description of the control objectives for IT processes and by offering the possibility of examining the maturity of these processes"**.

IT Governance Institute (2012) stated that **"COBIT 5 is an operational model and a common language for all parts of the business involved in IT activities. It also provides a framework for measuring and monitoring IT performance, integrating best management practices, governance and communicating with stakeholders"**.

ISACA (2012) stated that COBIT 5 supports the Governance of IT by providing a framework to ensure that:

- IT is aligned with the business (Strategic Alignment);
- IT enables the business and maximizes benefits (Value Delivery);
- IT resources are used responsibly (Resource Management);
- IT risks are managed appropriately (Risk Management);
- IT services are measured (Performance Measurement).

Previous Studies:

In his doctoral thesis, **Mårten Simonsson (2008)** studied the correlation between IT governance maturity and IT governance performance, using 35 cases; he tested his hypotheses for Cobit-based IT Governance. He said that improved activities, documentation, and monitoring would pay off in terms of business stakeholder satisfaction while improvements of the problem management process would not provide as high performance. He also stated that COBIT's representation of project and program management could be improved based on the analysis of reasons behind the weak correlation to IT governance performance.

Mathew Nicho (2008) tried to find the key-success tools to realize systems alignment and effectiveness measures in his doctoral thesis. He found that the most important factors are: establishing a Comprehensive Model for IT Governance, accomplishing the Benchmarking in Information Systems (IS) in the corporate industry, Software Engineering and establishing Control Standards/ Framework.

Based on what the researcher presents in this proposal, the study subject will be modeled as follow:

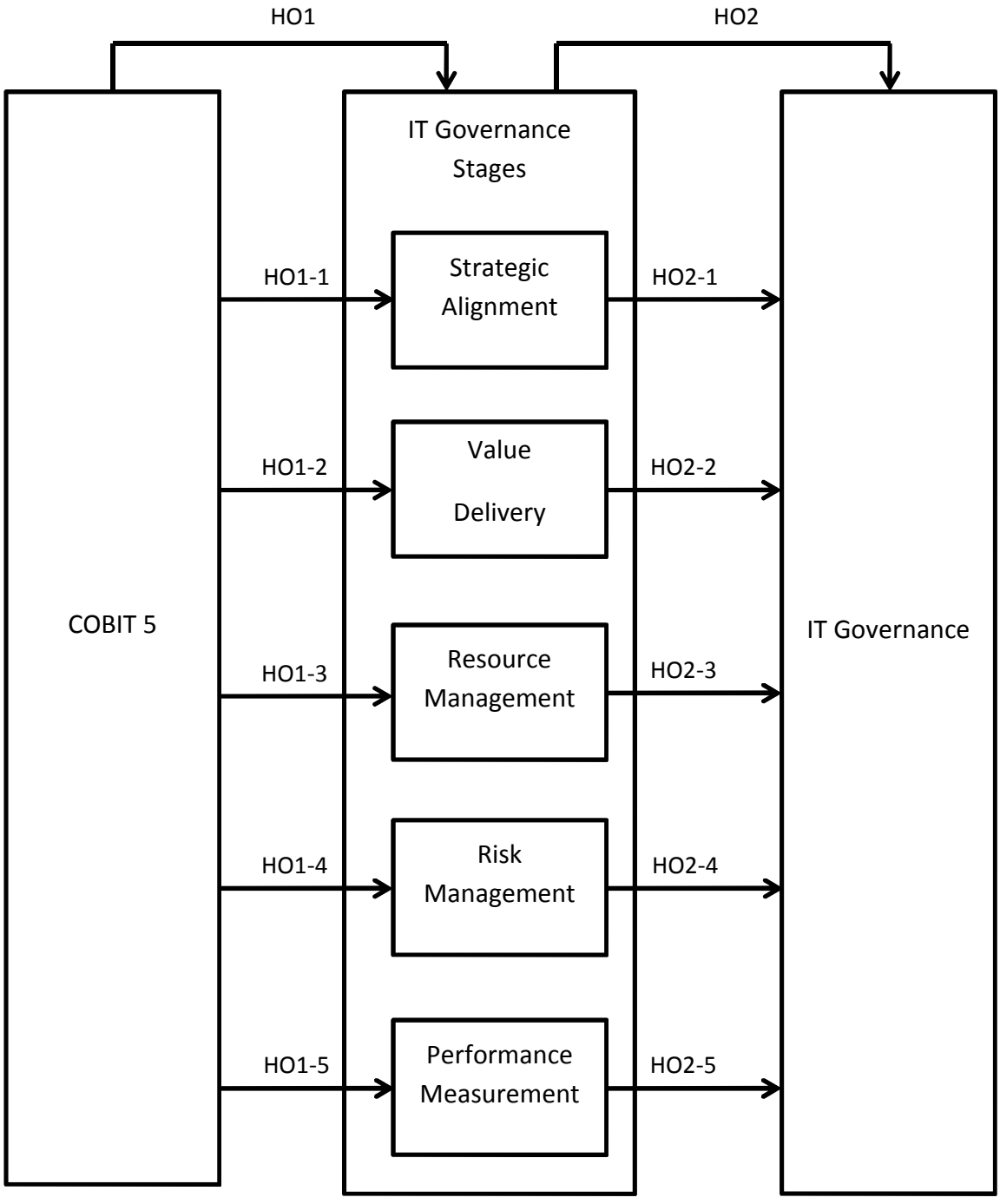


Figure 1: Study model

Research Hypotheses:

In Order to test the previous analysis model, the study proposes the following hypothesizes:

H01: COBIT 5 enables IT Governance stages;

- H01-1: COBIT 5 enables Strategic Alignment;
- H01-2**:** COBIT 5 enables Value Delivery;
- H01-3: COBIT 5 enables Resource Management;
- H01-4: COBIT 5 enables Risk Management;
- H01-5: COBIT 5 enables Performance Measurement.

H02: IT Governance Stages impact positively IT Governance effectiveness;

- H02-1: Strategic Alignment impacts positively IT Governance effectiveness;
- H02-2: Value Delivery impacts positively IT Governance effectiveness;
- H02-3: Resource Management impacts positively IT Governance effectiveness;
- H02-4: Risk Management impacts positively IT Governance effectiveness;
- H02-5: Performance Measurement impacts positively IT Governance effectiveness.

Operational Definitions of variables:

●Independent Variable:

COBIT 5: It is an integrated model for support IT governance and improves its effectiveness by providing a comprehensive control objectives, applicable management guidelines and maturity assessment tools.

●Moderate Variables:

Strategic Alignment: Provide for strategic direction of IT and the alignment of IT and the business with respect to services and projects.

Value Delivery: Confirm that the IT/Business organisation is designed to drive maximum business value from IT. Oversee the delivery of value by IT to the business.

Resource Management: Provide high-level direction for sourcing and use of IT resources. Oversee the aggregate funding of IT at enterprise level. Ensure there is an adequate IT capability and infrastructure to support current and expected future business requirements.

Risk Management: Ascertain that processes are in place to ensure that risks have been adequately managed. Include assessment of the risk aspects of IT investments.

Performance Measurement: Verify strategic compliance, i.e. achievement of strategic IT objectives. Review the measurement of IT performance and the contribution of IT to the business (i.e. delivery of promised business value).

Dependent Variable:

IT Governance: Organizational capacity exercised by the Board, executive management, and IT management to control the formulation and implementation of IT strategy that aims to ensure cost effective use of IT, effective use of IT for growth, effective use of IT for asset utilization, effective use of IT for business flexibility and compliance with legal and regulatory requirements.

CHAPTER 01

IT GOVERNANCE

A THEORETICAL BACKGROUND

CHAPTER 01: IT GOVERNANCE A THEORETICAL BACKGROUND

Introduction:

The purpose of this chapter is to make a clear understanding for IT Governance, it has been divided into three parts. The first part is about **Information Tchnology** fundamental concepts, it begins with the study hub which is known as "**information"** clarifying necessary characteristics, which make it adequate for wise decisions. Additionally, this part includes **Information Technology (IT) Infrastructure** that covers **hardware**, **software**, **databases systems**, **networks and telecommunications**. It contains lastly the **IT** functional form; which is called as **information systems.**

The second part attempts to clarify the IT Governance essence, that's why it refers to its original **sources** in a historical approach giving an account for the transition from **IT Management** to **IT Governance**. Furthermore, there has been little discussion about the Interaction between **Corporate Governance** and **IT Governance**, and this helps to evaluate IT Governance **importance**. In addition, this part highlights entities concerned by IT Governance concern. Finally, it explores an important tool for organising all IT Governance decisions, that is scientifically known as the **Governance Arrangement Matrix.**

The third part is about **IT Governance Focus Areas (stages),** which explains its domains. It starts with method to align IT with business, this is called as **Strategic Alignment**. The second domain is **Value Delivery**; it deals with how to optimize expenses and provides the value of IT. Thirdly, it is important to know the adequate way for Addressing the safeguarding of IT assets, this latest is the **Risk Management** mainfocus**.** Fourthly, the third part doesn't forget **Resource Management,** because it is submitted as a guide for optimizing knowledge and IT infrastructure. Finally, it involves the **Performance Measurement** which hundles the manner to which project delivery and IT services'effectiveness may be trucked.

I. Generalities about Information Technologies (IT):

1-1-Definition of Information Technology:

[Information technology (IT) is a general term that describes any technology that helps to produce, manipulate, store, communicate, and/or disseminate information][1]. [An organization's defined set of IT hardware, software, databases'systems and networks & telecommunications is called its **IT infrastructure**. This latest must be integrated with employees and procedures to build, operate, and support **information systems]**[2]**.** So, what is the IT infrastructure? And what does it mean an information system ?

1-2-Data and information:

1-2-1-The difference between data and information:

It is important to distinguish between data and information. [Data is a raw fact and can take the form of a number or statement such as a date or a measurement][3]. Another definition says: [Information in raw or unorganized form (such as alphabets, numbers, or symbols) that refer to, or represent, conditions, ideas, or objects. Data is limitless and present everywhere in the universe. See also information and knowledge][4]. It is necessary for businesses to put in place procedures to ensure data are recorded. For example, to ensure a call center operator includes the postcode of every customer this can be written into their script and a validation check performed to check these data have been entered into the system.

A common definition of information is that it is [Data that has been verified to be accurate and timely, is specific and organized for a purpose, is presented within a context that gives it meaning and relevance, and that can lead to an increase in understanding and decrease in uncertainty][5]. In other [words Information is data placed in a meaningful and useful context][6]. Some examples of information include a sales forecast or a financial statement.

---

[1] BRIAN K. WILLIAMS & STACEY C. SAWYER, 2011, USING INFORMATION TECHNOLOGY: A PRACTICAL INTRODUCTION TO COMPUTERS & COMMUNICATION: COMPLETE VERSION, 9 th edition, Page : 04.

[2] George W. Reynolds, 2010, Information Technology for Managers, CORSE TECHNOLOGY CENGAGE Learning, Page: 05.

[3] Elizabeth Hardcastle, 2011, Business Information Systems, Palgrave Macmillan, Basingstoke, Page: 07.

[4] http://www.businessdictionary.com

[5] http://www.businessdictionary.com

[6] James A. O'Brien & George M. Marakas, 2007, Enterprise Information Systems, McGraw-HILL Irwin, 13th edition, Page : 511.

1-2-2-Caracteristics of information:

Information can be characterized in a number of ways; some kinds of information are more suitable for decision making than others. The time frame for information can be historical or predictive. **Historical** information can be used to design alternative solutions and to monitor performance. Information may be expected or it may be unanticipated. Some information systems experts feel that information is worthless unless it is a surprise to the recipient. However, information that confirms something also reduces uncertainty. **Surprise** information often alerts us to the existence of a problem; it is also important in developing and evaluating different alternatives. Information may come from sources **internal** to the organization or from external sources, such as government agencies. Information may be presented in summary form or in detail and vary in **accuracy**. **Summary** information is often sufficient for problem finding, but summary and detailed information may be needed for other uses. Information can be frequently updated, relatively old, loosely organized, or highly **structured**. An example of highly structured information is a report with clear categories to classify all the information it contains. Loosely organized information might be a report composed of different forms of information from multiple sources. Because operational control decisions involve day-to-day operations of the firm, information often must correspond closely to **real time**. This information is often highly structured and precise[7].

Information for strategic decisions, on the other hand, is more predictive and long range in nature. Strategic planning may uncover many surprises. Often, external data on the economy, the competition, and so forth are involved in strategic decision making. Summary information on a periodic basis is adequate; there is usually no need for highly detailed or extremely precise information. Strategic planning decisions are usually characterized by loosely structured information. The requirements for managerial control decisions fall between operational control and strategic planning[8].

Table 1-1: INFORMATION CHARACTERISTICS VERSUS DECISION TYPES

	Decision Type		
Characteristics	**Operational control**	**Managerial control**	**Strategic planning**
Time frame	Historical	→	Predictive
Expectation	Anticipated	→	Surprise
Source	Largely internal	→	Largely external
Scope	Detailed	→	Summary
Frequency	Real time	→	Periodic
Organization	Highly structured	→	Loosely structured
Precision	Highly precise	→	Not overly precise

Source: Henry C. Lucas, Jr., 2009, Information Technology for Management, Jacobs Foundation, 1st edition, Zurich, Switzerla

[7] Henry C. Lucas, Jr., 2009, Information Technology for Management, Jacobs Foundation, 1st edition, Zurich, Switzerland, Page: 30

[8] Henry C. Lucas, Jr., The previous reference, Page: 31

1-3-Information Technology Infrastructure :

1-3-1-Hardware:

[Hardware describes the physical components of a computer system which can be categorized as **input devices**, a **central processing unit**, **the memory (storage)** and **output devices**][9].

●***Input and Output Devices:***

The studies show that human beings interact with computer systems largely through input and output devices. Input devices gather data and convert them into electronic form for use by the computer, whereas output devices display data after they have been processed.

The principal input devices consist of keyboards, pointing devices (such as the computer mouse and touch screens), and source data automation technologies (optical and magnetic ink character recognition, pen-based input, digital scanners, audio input, and sensors), which capture data in computer-readable form at the time and place they are created. They also include **radio-frequency identification (RFID)** devices that use tiny tags with embedded **microchips**[10] containing data about an item and its location to transmit radio signals over a short distance to special RFID readers. The RFID readers then pass the data over a network to a computer for processing. RFID is especially useful for tracking the locations of items as they move through the supply chain. The principal output devices are cathode ray tube terminals (CRTs), sometimes called video display terminals (VDTs), printers, and audio output. **Table 1-2** and **Table 1-3** describe in detail the principal input and output devices.

[9] Elizabeth Hardcastle, the previous reference, Page: 10

[10] A microchip (sometimes just called a "chip") is a unit of packaged computer circuitry (usually called an integrated circuit) that is manufactured from a material such as silicon at a very small scale. Microchips are made for program logic (logic or microprocessor chips) and for computer memory (memory or RAM chips). Microchips are also made that include both logic and memory and for special purposes such as analog-to-digital conversion, bit slicing, and gateways. **The source:** http://searchcio-midmarket.techtarget.com/definition/microchip.

Table 1-2 : Input devices

Input device	Description
Keyboard	Principal method of data entry for text and numerical data.
Computer mouse	Handheld device with point-and-click capabilities that is usually connected to the computer by a cable. The computer user can move the mouse around on a desktop to control the cursor's position on a computer display screen, pushing a button to select a command. Trackballs and touch pads often are used in place of the mouse as pointing devices on laptop PCs.
Touch screen	Device that allows users to enter limited amounts of data by touching the surface of a sensitized video display monitor with a finger or a pointer. Often found in information kiosks in retail stores, restaurants, and shopping malls.
Optical character recognition	Device that can translate specially designed marks, characters, and codes into digital form. The most widely used optical code is the *bar code*, which is used in point-of-sale systems in supermarkets and retail stores. The codes can include time, date, and location data in addition to identification data.
Magnetic ink character recognition (MICR)	Technology used primarily in check processing for the banking industry. Characters on the bottom of a check identify the bank, checking account, and check number and are preprinted using special magnetic ink. A MICR reader translates these characters into digital form for the computer.
Pen-based input	Handwriting-recognition devices, such as pen-based tablets, notebooks, and notepads, that convert the motion made by an electronic stylus pressing on a touch-sensitive tablet screen into digital form.
Digital scanner	Device that translates images, such as pictures or documents, into digital form; essential component of image-processing systems.
Audio input	Voice input devices that convert spoken words into digital form for processing by the computer. Microphones and tape cassette players can serve as input devices for music and other sounds.
Sensors	Devices that collect data directly from the environment for input into a computer system. For instance, today's farmers can use sensors to monitor the moisture of the soil in their fields to help them with irrigation.
Radio-frequency identification (RFID)	Devices that use tags with microchips to transmit information about items and their locations to special RFID readers. Useful for tracking items as they move through the supply chain.

Source : Kenneth C. Laudon and Jane P. Laudon, 2011, Essentials of MIS, Prentice Hall, 9th edition.

Table 1-3 : output devices

Output device	Description
Cathode ray tube (CRT)	Electronic gun that shoots a beam of electrons illuminating tiny points on a display screen. Laptop computers use flat panel displays, which are less bulky than CRT monitors.
Printers	Devices that produce a printed hard copy of information output. They include impact printers (such as dot matrix printers) and nonimpact printers (such as laser, inkjet, and thermal transfer printers).
Audio output	Voice output devices that convert digital output data back into intelligible speech. Other audio output, such as music, can be delivered by speakers connected to the computer.

Source : Kenneth C. Laudon and Jane P. Laudon, 2011, Essentials of MIS, Prentice Hall, 9th edition

●***Central Processing Unit (CPU) :***

[The unit of a computer that includes the circuits that control the interpretation and execution of instructions. In many computer systems, the CPU includes the **arithmetic-logic unit**, the **control unit**][11].

Arithmetic-Logic Unit (ALU) : [An arithmetic-logic unit (ALU) is the part of a computer processor (CPU) that carries out arithmetic and logic operations on the operands in computer instruction words. In some processors, the ALU is divided into two units, an arithmetic unit (AU) and a logic unit (LU). Some processors contain more than one AU][12].

Control Unit : [The control unit deciphers each instruction stored in the CPU and then carries out the instruction][13]. So, it directs the movement of electronic signals between main memory and the arithmetic/logic unit. It also directs these electronic signals between main memory and the input and output devices.

[11] James A. O'Brien & George M. Marakas, the previous reference, Page : 504.
[12] http://searchcio-midmarket.techtarget.com/definition/arithmetic-logic-unit.
[13] BRIAN K. WILLIAMS & STACEY C. SAWYER, the previous reference, Page : 212.

●***Storage (Memory) :***[Pertaining into a device in which data can be entered, in which can be held, and from which they can be retrieved at a later time][14]. There are two kinds of storage ; **primary storage** and **secondary storage**.

Primary Memory :

[The memory in which programs and data are stored and from which they are generally executed; main storage][15]. The main primary storage devices are: **Semi-Conductor Memory, Random Access Memory (RAM), Read Only Memory (ROM), Bubble Memory, Flash Memory** and **Video RAM.**

Semi-Conductor Memory : [The number of transistors are integrated or combined together on a thin silicon wafer to form a complete set of circuits that can hold data][16].

Random Access Memory (RAM) : [It is used for temporary storage of data and programs during processing. Each memory position can be directly sensed (read) or changed (written) in the same length of time, regardless of its location on the storage medium][17].

Read Only Memory: [Perform the basic control and supervisory operation of the computer. Three types of ROM are - **PROM**, **EPROM**, and **EEPROM]**[18].

PROM (Programmable read-only memory): [is read-only memory (ROM) that can be modified once by a user][19].

EPROM (erasable programmable read-only memory): [is programmable read-only memory (programmable ROM) that can be erased and re-used][20].

EEPROM (electrically erasable programmable read-only memory): [is user-modifiable read-only memory (ROM) that can be erased and reprogrammed (written to) repeatedly through the application of higher than normal electrical voltage][21].

---

[14] James A. O'Brien & George M. Marakas, the previous reference, Page : 518.
[15] Henry C. Lucas, Jr, 2009, Information Technology for Management, 7 th edition, CREATIVE COMMONS (available in the following website: www.creativecommons.org), Page: 708.
[16] THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA – Board of studies, 2011, Information Technology VOL2, The revised edition accomplished in January 2011 (available in www.icai.org), Page : 08.
[17] James A. O'Brien & George M. Marakas, the previous reference, Page : 516.
[18] THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA – Board of studies, The preceding reference, Page : 08.
[19] http://searchbusinessintelligence.techtarget.in/search/query?q=PROM.
[20] http://searchbusinessintelligence.techtarget.in/search/query?q=EPROM.
[21] http://searchbusinessintelligence.techtarget.in/search/query?q=EEPROM.

Bubble Memory: Small magnetic bubbles formed on a thin single crystal film of synthetic garnet are used to store the data permanently[22].

Flash Memory: Non-Volatile memory, where data can be erased electrically or reprogrammed. They primarily used in memory cards, USB flash drives, and solid-state drives for general storage and transfer of data between computers and other digital products[23].

Video RAM: Video RAM as "video RAM" means in general all forms of RAM used to store image data for the video display monitor[24].

Secondary Storage:

[Devices that permanently hold data and information as well as programs][25]. Secondary storage as opposed to primary storage is nonvolatile; that is, saved data and programs are permanent, or remain intact, when the power is turned off. These devices Store the data permanently in millions and billions of bytes. The famous types of secondary storage devices are : **Tape Device, Floppy Diskette, Magnetic Disc, Optical Laser Disk.**

Tape Device : is a device that stores computer data on magnetic tape, especially for backup and archiving purposes. In other words, it is an external storage device that can be used for making copies of audio, video, and data[26].

Floppy Diskette: A small plastic disc coated with iron oxide that resembles a small photograph record enclosed in a protective envelope[27].

Magnetic disc : A flat, circular plate with a magnetic surface on which data can be stored by selective magnetization of portions of the curve surface[28].

Optical Laser Disk: A secondary storage medium using CD (computer disk) and DVD (digital versatile disk) technologies to read tiny spots on plastic disks. The disks are currently capable of storing billions of characters of information[29].

[22] THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA – Board of studies, The preceding reference, Page : 08.
[23] THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA – Board of studies, The preceding reference, Page : 08.
[24] http://whatis.techtarget.com/reference/Fast-Guide-to-RAM#vidram.
[25] BRIAN K. WILLIAMS & STACEY C. SAWYER, the preceding reference, Page : 246.
[26] http://searchstorage.techtarget.com/definition/tape-drive.
[27] James A. O'Brien & George M. Marakas, the previous reference, Page : 509.
[28] James A. O'Brien & George M. Marakas, the previous reference, Page :513.
[29] James A. O'Brien & George M. Marakas, the previous reference, Page :515.

●***Varieties of computers :***

In those days, in the 1950s and 1960s, computers were enormous machines affordable only by large institutions. Now they come in a variety of shapes and sizes, which can be classified according to their processing power: **supercomputers**, **mainframe computers**, **workstations**, **microcomputers**, **microcontrollers** and **servers.**

Supercomputers : are high-capacity machines with thousands of processors that can perform more than several trillion calculations per second[30]. The image 1-2 represents an example of main frame computer in large companies.

Mainframe computers: The original kind of computer; associated today with large computers using proprietary hardware and software and often having cost/performance ratios that are worse than smaller computers[31].

Workstations: The workstation is a powerful computer generally assigned to one user; a desktop computer usually having at least a Pentium processor or better or a Sun Workstation; the workstation should have windowing software[32].

Microcomputers: [A **microcomputer** is a complete computer on a smaller scale and is generally a synonym for the more common term, personal computer or PC, a computer designed for an individual][33]. It is often for a single user or a small number of simultaneous
Users.

Microcontrollers: also called embedded computers, are the tiny, specialized microprocessors installed in "smart" appliances and automobiles[34].

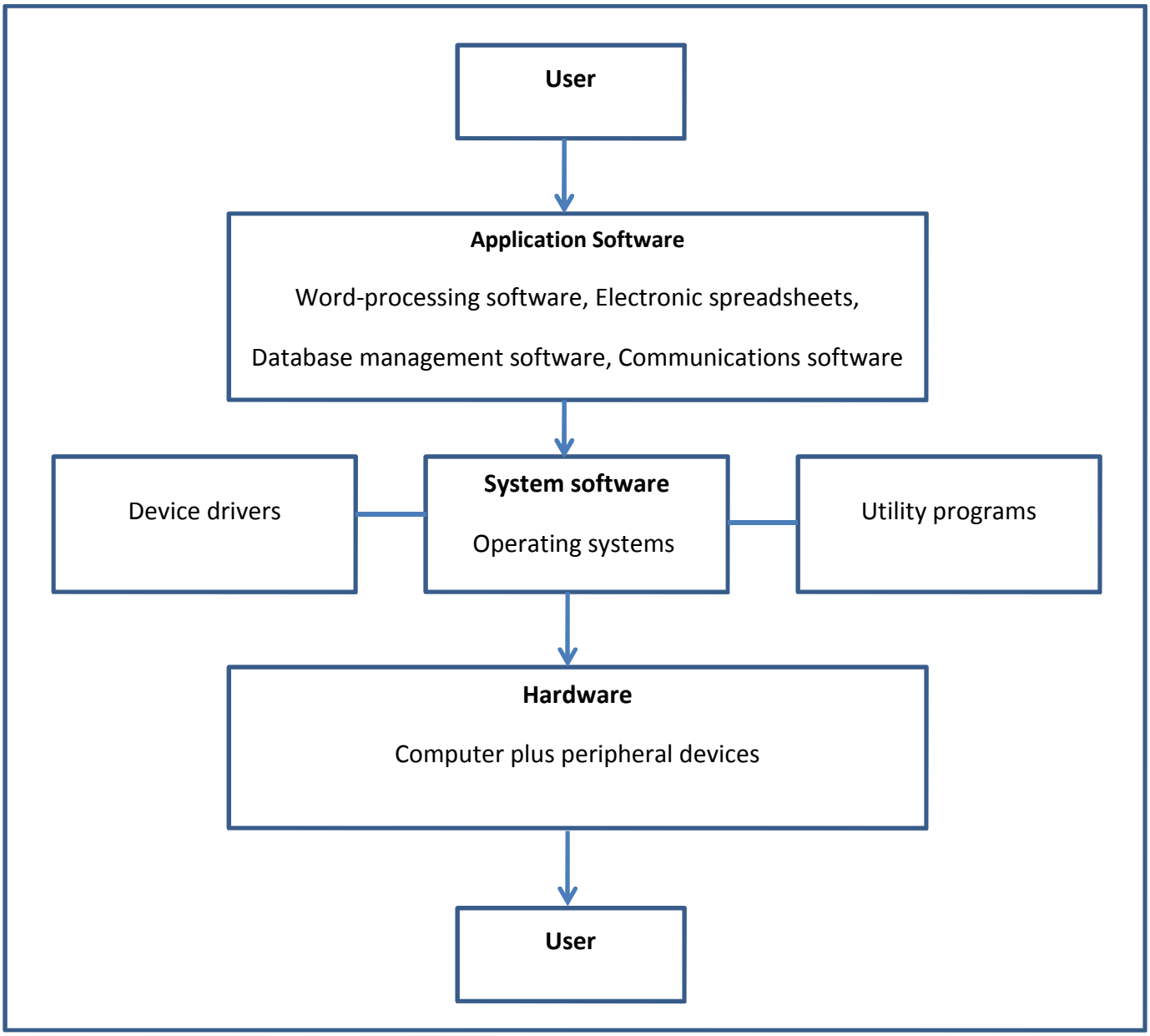
Servers: The computer that provides data and some programs in a client-server architecture. It provides services to other computer programs (and their users) in the same or other computers[35].

1-3-2-Software:

To play a useful role in the firm's information technology infrastructure, computer hardware requires computer software. [Software can be defined as a series of detailed instructions that control the operation of a computer system and exist as programs which are developed by computer programmers][36]. There are two major categories of software; systems software and applications software.

[30] BRIAN K. WILLIAMS & STACEY C. SAWYER, The previous reference, Page: 21.
[31] Henry C. Lucas, Jr, The previous reference, page : 706.
[32] Henry C. Lucas, Jr, The previous reference, page : 712.
[33] http://whatis.techtarget.com/definition/microcomputer
[34] **:** BRIAN K. WILLIAMS & STACEY C. SAWYER, the previous reference, Page: 23.
[35] http://whatis.techtarget.com/definition/server
[36] Elizabeth Hardcastle, The previous reference, Page: 12.

Figure 1-1 : Information technology software



Source : BRIAN K. WILLIAMS & STACEY C. SAWYER, 2011, USING INFORMATION TECHNOLOGY: A PRACTICAL INTRODUCTION TO COMPUTERS & COMMUNICATION: COMPLETE VERSION, 9 th edition.

●System Software:

System software consists of programs that let the computer manage its resources. There are three basic components of system software:

- **Operating systems:** It is the most important piece of system software. The **operating system** is a group of programs that manage and organize resources of the computer.
- **Device drivers:** Device drivers help the computer control peripheral devices.
- **Utility programs:** Utility programs are generally used to support, enhance, or expand existing programs in a computer system[37].

●Application Software:

It is software that has been developed to solve a particular problem for users—to perform useful work on specific tasks or to provide entertainment. There are application packages for many needs.

- **Word-processing software:** allows user to enter text for a paper, report, letter, or memo.
- **Electronic spreadsheets:** allow user to process numerical data.
- **Database management software:** permits you to manage large quantities of data in an organized fashion.
- **Communications software:** includes Web browsers, such as Internet Explorer[38].

1-3-3-Databases Systems:

The purpose of a database is to keep track of things. Databases can exist on paper, for example a telephone directory, but are inefficient and costly to maintain. A computer-based database offers the advantage of powerful search facilities which can be used to locate and retrieve information many times faster than by manual methods[39].

●Databases Models:

Just as computer hardware and software development languages have seen different technological generations. This manifests itself primarily in the conceptual database model i.e. the type and nature of the relationships that are allowed between different data tables.

[37] BRIAN K. WILLIAMS & STACEY C. SAWYER, The previous reference, Page: 121
[38] BRIAN K. WILLIAMS & STACEY C. SAWYER, The previous reference, Page: 121
[39] Kenneth C. Laudon and Jane P. Laudon, 2011, *Essentials of Management Information Systems*, Prentice Hall, 9th edition, Page: 247

- **The Hierarchical Data Model:** The hierarchical data (base) model is the oldest and conceptually simplest model. This structure allows only for one type of relationship, the "parent-child" (or one-to-many) relationship.

- **The Network Model:** The network data model accommodates the "many-to-many" relationships often found in the real world. It allows the explicit linking of sets of entities by means of network relationships.
- **The Relational Model:** More flexible than hierarchical and network database models, the relational database relates, or connects, data in different files through the use of a key, or common data element.
- **Object-Oriented Database :** An *object-oriented database* uses "objects," software written in small, reusable chunks, as elements within database files.
- **Multidimensional Database :** Models data as facts, dimensions, or numerical measures for use in the interactive analysis of large amounts of data for decision-making purposes. A multidimensional database uses the idea of a cube to represent the dimensions of data available to a user, using up to four dimensions[40].

1-3-4-Networks and Telecommunications:

[a network, or communications network, is a system of interconnected computers, telephones, or other communications devices that can communicate with one another and share applications and data][41]. Networks, which consist of various combinations of computers, storage devices, and communications devices, may be divided into several main categories, differing primarily in their geographic range and purposes.

1-3-4-1-Networks according to size:

Networks sizes can range from tiny to very large.

- ***Personal Area Network (PAN):*** consists of two to five computing devices. This not very common term would apply to the network typically found in the home, and may be based on wireless technology e.g. Bluetooth..
- ***Local Area Network (LAN):*** the most common type of network. It consists of from about four up to as many as a couple of hundred of computers linked together with one set of cables, usually within the same building. Most LANs are controlled by a central *file server* that takes care of network communications, security control and the storage of data files.

[40] Elizabeth Hardcastle & Ventus, 2011, Business Information Systems, Pearson Education, Harlow, Page: 14
[41] BRIAN K. WILLIAMS & STACEY C. SAWYER, The preceding reference, Page: 315.

- ***Metropolitan Area Network (MAN):*** a network infrastructure linking various local businesses within a large city area. This is now almost completely superseded by the Internet.
- ***Wide Area Network (WAN):*** the opposite of the LAN. It links computers over large geographical areas. This network usually makes use of the public telecommunications network. The widely dispersed Automatic Teller Machine (ATM) network of a commercial bank is typically part of the bank's WAN.
- ***Value-Added Network (VAN):*** although not relating to size (but it rhymes with the others!), it refers to the provision of a network infrastructure service to other businesses. The service goes beyond the physical cabling and includes "value-added services" such as limited data and transaction processing or message routing. An example for the banking industry is the provision of an inter-bank Electronic Funds Transfer (EFT) and clearing service, linking the computers of different commercial banks (and, possibly, retailers) together[42].

1-3-4-2-Network Topologies:

Networks can be laid out in different ways. **The logical layout, or shape, of a network is called a topology.** The three basic topologies, or configurations, are bus, ring, and star.

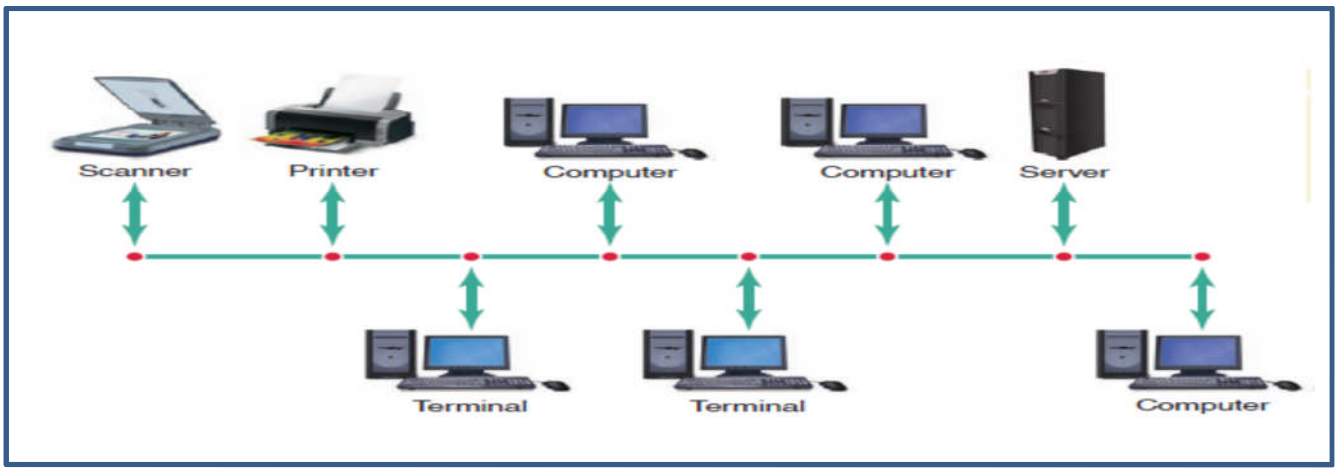
BUS NETWORK : That is, in a bus network, all nodes are connected to a single wire or cable, the bus, which has two endpoints. Each communications device on the network transmits electronic messages to other devices.

RING NETWORK : A ring network is one in which all microcomputers and other communications devices are connected in a continuous loop.

STAR NETWORK : A *star network* is one in which all microcomputers and other communications devices are directly connected to a central server.

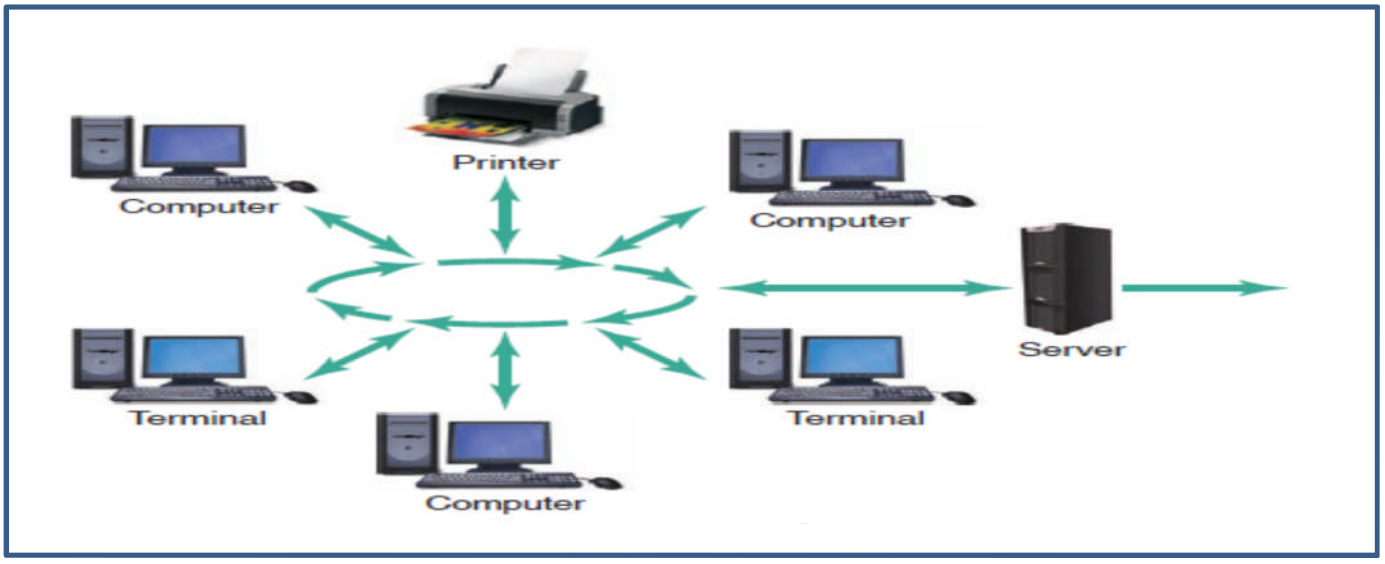
[42] THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA – BOARD OF STUDIES, January, 2011, INFORMATION TECHNOLOGY, PAPER : 7A, VOLUME – II, Page: 64

Figure 1-2 : Bus Network



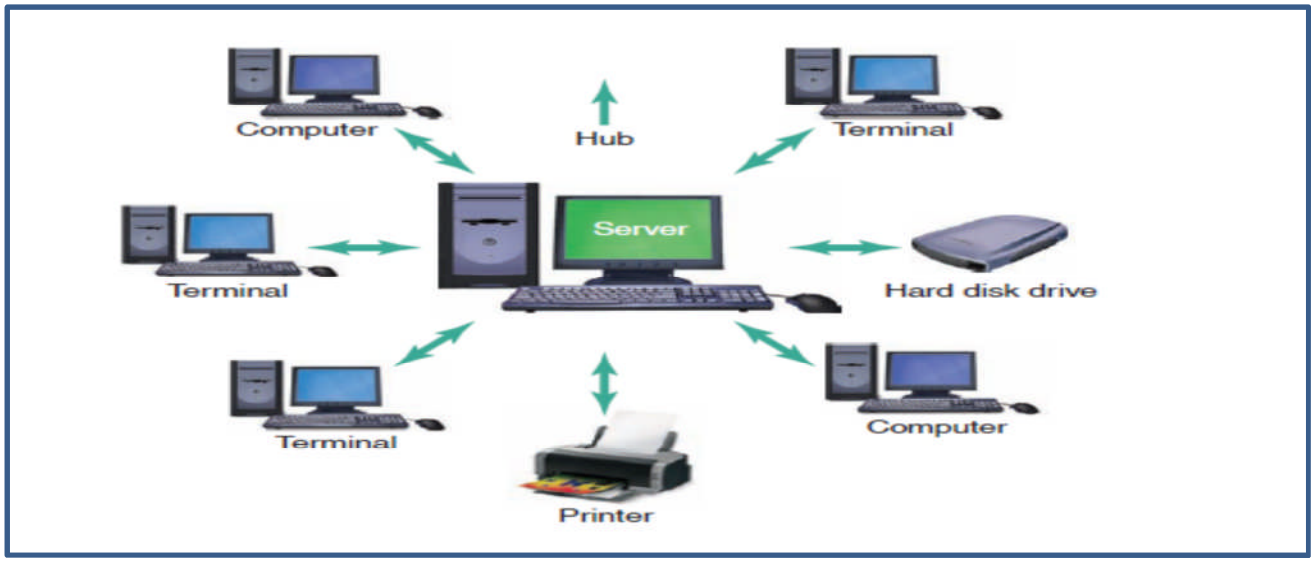
Source : BRIAN K. WILLIAMS & STACEY C. SAWYER, 2011, USING INFORMATION TECHNOLOGY: A PRACTICAL INTRODUCTION TO COMPUTERS & COMMUNICATION: COMPLETE VERSION, 9 th edition.

Figure 1-3 : Ring Network.



Source : BRIAN K. WILLIAMS & STACEY C. SAWYER, 2011, USING INFORMATION TECHNOLOGY: A PRACTICAL INTRODUCTION TO COMPUTERS & COMMUNICATION: COMPLETE VERSION, 9 th edition.

Figure 1-4 : Star Network.



Source : BRIAN K. WILLIAMS & STACEY C. SAWYER, 2011, USING INFORMATION TECHNOLOGY: A PRACTICAL INTRODUCTION TO COMPUTERS & COMMUNICATION: COMPLETE VERSION, 9 th edition.

1-3-4-3-Telecommunications Devices:

[Telecommunications, also called telecommunication, is the exchange of information over significant distances by electronic means. A complete, single telecommunications circuit consists of two stations, each equipped with a transmitter and a receiver][43]. The telecommunication devices are used to connect the different computers and to ensure error-free data transmission between them.

[Network cables: are the physical wires by which computers are linked together.

Network interface cards (NICs): are necessary when computers are connected directly to other computers by means of digital network cables (as opposed to the situation when two computers are connected to each other via a telephone link). Their primary function is to make sure that there are no transmission conflicts with the other computers linked to the network.

Multiplexers: allow a single channel to carry data transmissions simultaneously from many sources, by merging them at one end of the channel and then separating the individual transmissions at the receiving end of the channel.

Front-end processors (FEP): are used in bigger networks that are centrally controlled by large computers – often mainframes. In order to give the expensive mainframe more "time" to

[43] http://searchtelecom.techtarget.com/definition/telecommunications

concentrate on application processing, it needs to be relieved from the rather mundane task of network control. FEPs handle all or most communication processing such as error-checking, data conversion, packaging and transmission control.

Routers and bridges: are computers dedicated to the translation of network protocols and standards between different networks. They are becoming important as more and more organizations are linking their own networks to those of other organizations.

Modem: allows a computer to communicate with another computer by means of the public voice telephone network, rather than by using digital cabling][44].

●Internet and its similar technologies:

❖ ***What is Internet?:***

The Advanced Research Project Agency (ARPA) of Department of Defense, U.S., developed a network named ARPANET in 1970 to share information between networks. [Internet is a network of computers that offers access to information through e-mail, bulletin boards, chatting, and information retrieval services that can access files, directories and database around the world][45]. The Internet is used for Communication, Data retrieval, Data publishing.

World Wide Web (WWW): A global network of multimedia Internet sites for information, education, entertainment, e-business, and e-commerce[46].

Uniform Resource Locators (URLs): [The URL (Uniform Resource Locator) is a string of characters that points to a specific piece of information anywhere on the web][47]. In other words, the URL is the website's unique address.

❖ **Components of Internet :**

- **Electronic Mail (e-mail):** A technique in which messages or documents is sent to another person using Internet.
- **Web Casting or Push Technology:** Allows users to passively receive broadcast information rather than actively search the web for information. For example, Internet news service[48].

❖ **Intranets:**

An *intranet* is an organization's internal private network that uses the infrastructure and standards of the internet and the web. When a corporation develops a public website, it is making selected information available to consumers and other interested parties. When it creates an intranet, it enables employees to have quicker access to internal information and to share knowledge so that they can do their jobs better[49].

❖ **Extranets:**

[44] Henry C. Lucas, Jr., The previous reference, Page: 702

[45] THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA - BOARD OF STUDIES, 2011, PAPER: 7A, INFORMATION TECHNOLOGY, VOLUME – II, Page: 89.

[46] James A. O'Brien & George M. Marakas, the previous reference, Page : 521

[47] Henry C. Lucas, Jr., The previous reference, Page: 705

[48] BRIAN K. WILLIAMS & STACEY C. SAWYER, The previous reference, Page: 65.

[49] Elizabeth Hardcastle, The previous reference, Page: 19

Extranets are private intranets that connect not only internal personnel but also selected suppliers and other strategic parties. Extranets have become popular for standard transactions such as purchasing[50].

1-4- Information systems:

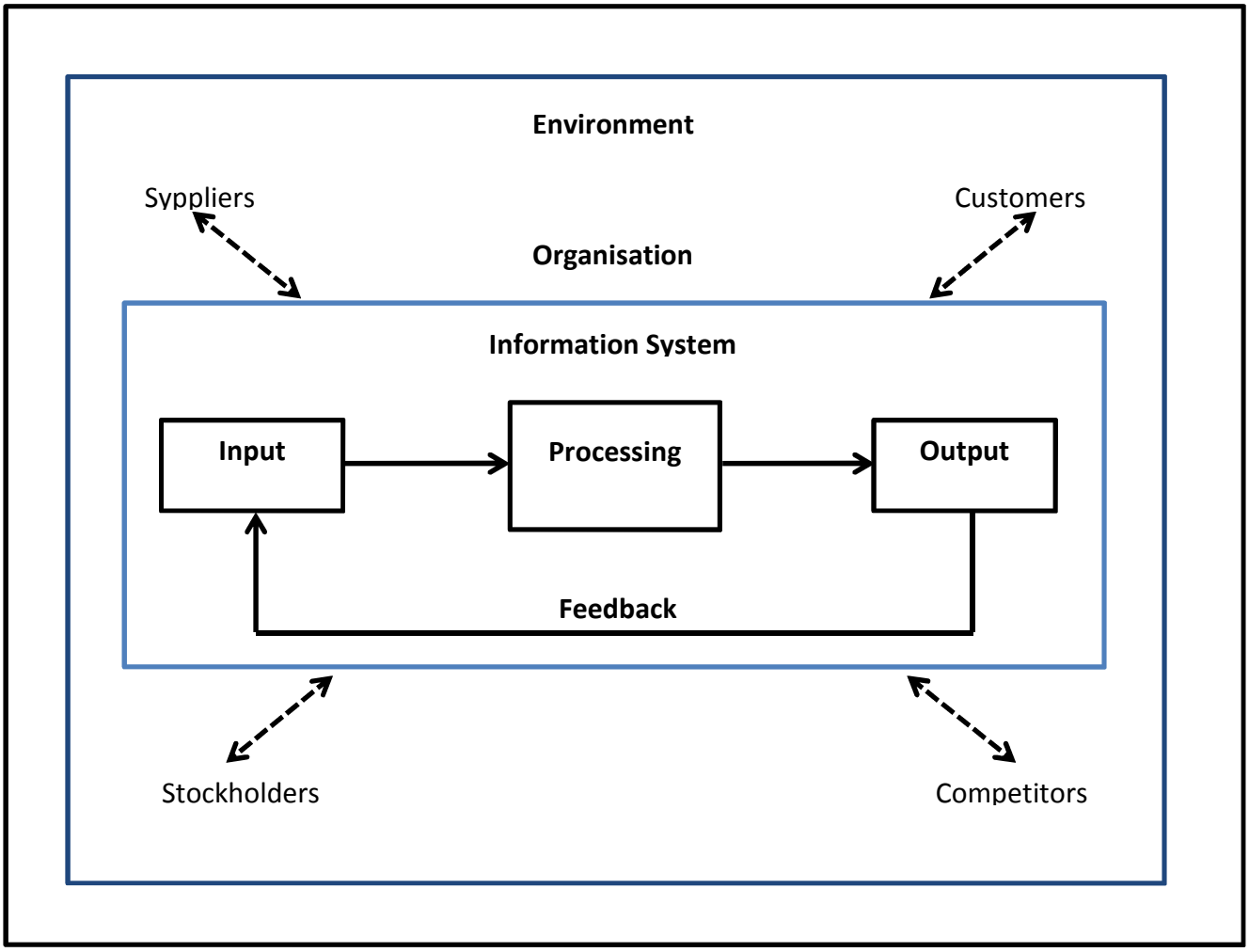
1-4-1- What is Information System?

Information systems play a crucial role in the management of any contemporary enterprise such as a small, medium or large organization; a profit making or a social service set-up; a public or a private sector undertaking; a manufacturing or a service organization; a local or a global corporation; and an upcoming or an established business house. [An **information system (IS)** consists of all the components that work together to process data and produce information][51]. Almost all business information systems consist of many subsystems with sub-goals, all contributing to the organization's main goal.

Ken Laudon & Jane Laudon discuss the components of an information system. They talk about the **input**, **processing**, **output,** and **feedback** processes (**Figure 1-5**). Most important is the feedback process; unfortunately, it's the one most often overlooked. The hardware (input and output) and the software (processing) receive the most attention[52]. The interactions of a system with its environment can take the form of inputs or outputs**. Inputs** take the form of material objects, energy and/or information flowing from the environment into the system. **Outputs** are released or sent from the system back into its environment. This output can either be useful (to some outside system) or waste. Within the system, the inputs usually undergo some kind of **transformation process** so that the outputs are different from the inputs. Often, inputs and outputs undergo further specific transformations *at* the system boundary; the system components responsible for these transformations are called the **interfaces. Feedback** is about the performance of the information system[53].

[50] Elizabeth Hardcastle, The previous reference, Page: 21
[51] EFFY OZ, 2009, Management Information Systems, THOMSON COURSE TECHNOLOGY , Sixth Edition, Boston, USA, Page: 13
[52] Ken Laudon & Jane Laudon, 2012, Management Information Systems, 12th edition, *Prentice Hall, Page: 05*
[53] Mike G. Eccles, Jane M. Nash & Jean-Paul Van Belle, 2003, Discovering Information Systems, Creative Commons Attribution, Page: 24.

Figure 1-5 : Components of Information System

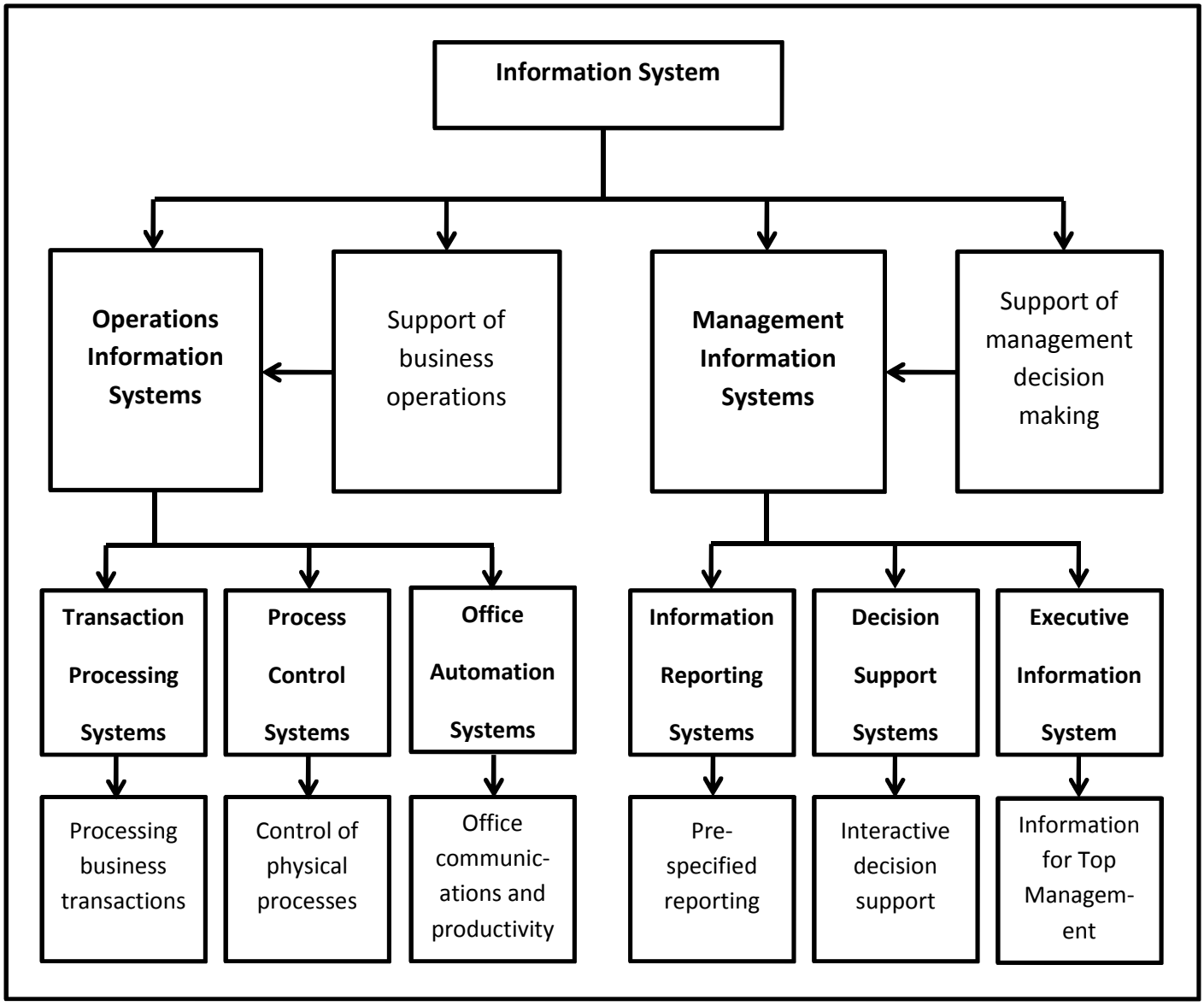


Source : Ken Laudon & Jane Laudon, 2012, Management Information Systems, 12th edition, *Prentice Hall*

1-4-2-Types of Information Systems and sub-systems:

There is no one single information system that will satisfy all of the needs of an organization. At first glance it can be difficult to comprehend all the different systems in a business, and even more difficult to understand how they relate to one another. Often, a system consists of several **subsystems** — components of a larger system—with subgoals, all contributing to meeting the main goal. Subsystems can receive input from, and transfer output to, other systems or subsystems.

Figure 1-6 : Classification of Information System



Source : S.Shajahan & Priadharshini, 2004, Management Information Systems, NEW AGE INTERNATIONAL (P) LIMITED. PUBLISHERS. New Delhi. India

1-4-2-1- Operation Information System:

It consists of transaction processing system, process control system and office automation system. This system supports business operations by providing meaningful information at the time of making operational decisions[54].

- **Transaction Processing System:** The information systems used in this level of the organization are **transaction processing systems (TPS)**, so called because they record the routine transactions that take place in everyday operations[55].
- **Process Control System:** Process Control system helps to monitor a physical process, capture and process data selected by sensors and makes real time adjustments to the process[56].
- **Office Automation System:** Office Automation System also known, as office information systems are systems whose primary goal is to facilitate communications. Office Automation Systems are computer-based information systems that collect, process, store and transmit electronic messages, documents, and other forms of communications among individuals, work groups and organisations[57].

1-4-2-2-Management Information System:

A management information system is used by managers throughout the organization to help them in directing, planning, coordinating, communicating, and decision making. The MIS will help answer structured questions on a periodic basis[58]**.** It consists of information reporting system, decision support system and executive information system.

- **Information Reporting System:** Information reporting systems provide managerial end users with information products that support much of their day-to-day decision-making needs. Processed Information outputs given to managers include displays and reports, which are produced on demand, or on a periodical basis (monthly/weekly etc.) or even during exceptional conditions like Periodic scheduled reports. Exception reports and so on[59].
- **Decision Support System:** [A decision-support system (DSS) is a computer-based system that helps the decision maker utilize data and models to solve unstructured problems][60]. Decision-support systems are used for complex —what-if questions that require internal and external data. Decisions at this management level are mostly semi-structured so the information system must respond to the unique requirements of the executives[61].
- **Executive Information System:** Executive Information System is a set of computer based tools with features such as Color graphics. Touch screens. Voice-activated commands which help managers to quickly retrieve, analyse, navigate, summarise and disseminate large volumes of data. Executive Information System is normally connected with online information services, so that top managers could access data whenever they require for the same[62].

---

[54] **Source :** S.Shajahan & Priadharshini, 2004, Management Information Systems, NEW AGE INTERNATIONAL (P) LIMITED, PUBLISHERS, New Delhi, India, Page: 50

[55] Ken Laudon & Jane Laudon, The previous reference, Page: 14
[56] S.Shajahan & Priadharshini, The previous reference, Page: 51
[57] S.Shajahan & Priadharshini, The previous reference, Page: 51
[58] Ken Laudon & Jane Laudon, The previous reference, Page: 15
[59] S.Shajahan & Priadharshini, The previous reference, Page: 54
[60] Mike G. Eccles, Jane M. Nash & Jean-Paul Van Belle, The previous reference, Page: 56
[61] Ken Laudon & Jane Laudon, The previous reference, Page: 16
[62] S.Shajahan & Priadharshini, The previous reference, Page: 54

II. IT Governance a conceptual background

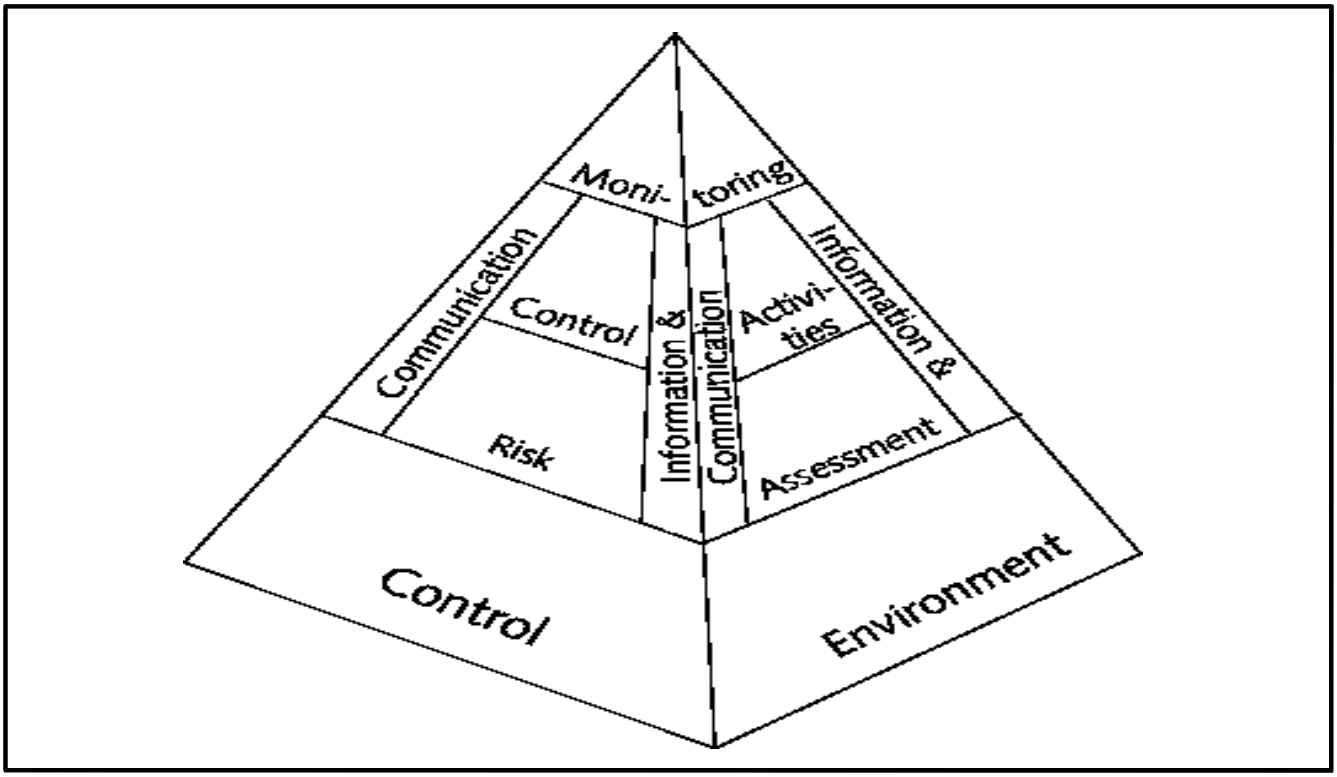
2-1- IT Governance sources:

Regarding governance there are several sources that provide basic knowledge. In the following paragraphs some background on the major sources is presented.

2-1-1-COSO :

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission issued 'Internal Control - Integrated Framework'. This publication established a framework for internal control and provided evaluation tools which business and other entities can use to evaluate their control systems[63].

Figure 1-7: COSO Internal Control - Integrated Framework



Source: COSO. *Internal Control - Integrated Framework (COSO report)*. Committee of Sponsoring Organizations of the Treadway Commission, 1994.

[63] Koen Brand & Harry Boonen, 2007, IT Governance based on CobiT® 4.1 - A Management Guide, Van Haren Publishing, Third edition, first impression, Page: 05

The framework identifies and describes five interrelated components necessary for effective internal control. In 'Internal Control - Integrated Framework', COSO defined internal control as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

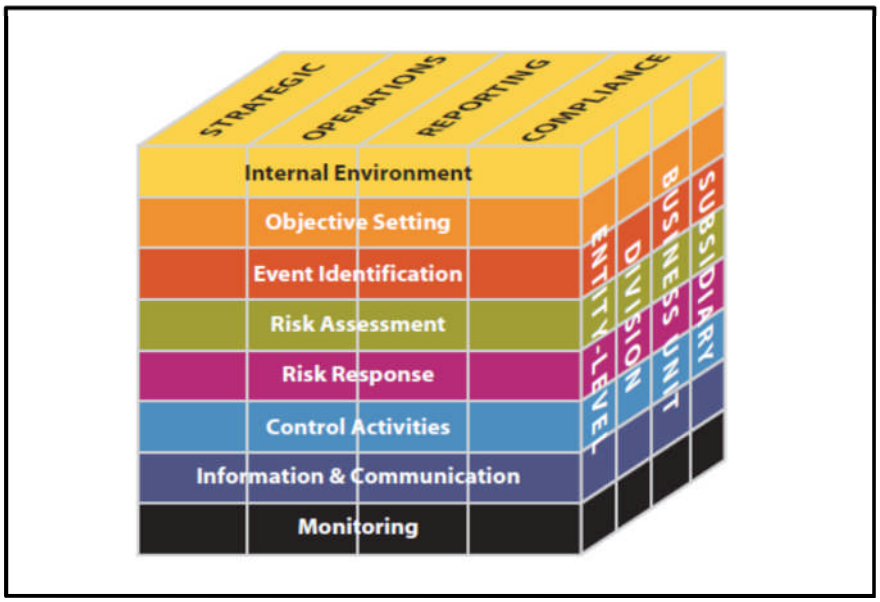
- **Effectiveness and efficiency of operations**
- **Reliability of financial reporting**
- **Compliance with applicable laws and regulations**[64].

In 2004 the COSO Enterprise Risk Management (ERM) was published. Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives[65].

[64] Koen Brand & Harry Boonen, The previous reference, Page: 06

[65] Richard M. Steinberg et al. ,2004. *Enterprise Risk Management - Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission, Available on www.aicpa.org, Page: 12.

Figure 1-8 : Enterprise Risk Management Framework



Source : Richard M. Steinberg et al., 2004. *Enterprise Risk Management - Integrated Framework ,* Committee of Sponsoring Organizations of the Treadway Commission. Available on www.aicpa.org

- **Internal Environment :** The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- **Objective Setting :** Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite[66].
  - **[Strategic objectives:** high-level goals, aligned with and supporting its mission. By focusing first on strategic objectives and strategy, an entity is positioned to develop related objectives at an entity level, achievement of which will create and preserve value.
  - **Operations Objectives :** *These pertain to the effectiveness and efficiency of the* entity's operations, including performance and profitability goals and

[66] Richard M. Steinberg et al. , The previous reference, Page : 22

safeguarding resources against loss. They vary based on management's choices about structure and performance.

- **Reporting Objectives:** These pertain to the reliability of reporting. They include internal and external reporting and may involve financial and non-financial information.
- **Compliance Objectives**: These pertain to adherence to relevant laws and regulations. They are dependent on external factors and tend to be similar across all entities in some cases and across an industry in others][67].

- **Event Identification :** Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
- **Risk Assessment** : Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- **Risk Response :** Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- **Control Activities :** Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- **Information and Communication :** Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- **Monitoring:** The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both[68].

[67] Richard M. Steinberg et al. , The previous reference, Page : 35
[68] Richard M. Steinberg et al. , The previous reference, Page : 22

2-1-2- IT Service Management (ITSM) & IT Infrastructure Library (ITIL):

2-1-2-1- IT Service Management (ITSM):

"IT Service Management is about maximizing the ability of IT to provide services that are cost effective and meet or exceed the needs and expectations of the business to:

- Reduce the costs of operations
- Improve service quality
- Improve customer satisfaction
- Improve compliance"[69].

Principles for Achieving IT Service Management and Delivery Excellence:

- All steady-state operations (e.g. PBX, Data Center, Help Desk, Network Management, etc.) must have a primary owner and secondary (backup) owner
- The overall ITSMD budget should be divided into a set of defined products and services so that all IT costs can be mapped to supportable business processes
- All the IT services should achieve the desired level of efficiency, productivity, reliability and availability as measured by the appropriate key performance indicators (e.g. Service level agreements, customer satisfaction, costs, etc.)
- All ITSMD services should be charged back to the user or customer organization
- A formal ITSMD governance, reporting and escalation process is established to resolve key operational issues, risks, and conduct periodic reviews All steady-state operations have business continuity, backup (including one or more off-site locations), disaster recovery and security policies and procedures
- All ITSMD related processes should be documented in a consistent, repeatable and standard framework such as ITIL (IT Infrastructure Library) and continuously improved.
- Optimizing the utilization of IT assets and resources is critical[70].

2-1-2-2- IT Infrastructure Library (ITIL):

In the 1980s the quality of service provided by both internal and external IT companies to UK government departments was of such a level that the CCTA (Central Computer and Telecommunications Agency, now the Office of Government Commerce, OGC) was instructed by the Government to develop a standard approach for an efficient and effective delivery of IT services. This was to be an approach which was independent of the suppliers (whether internal or external). The result of this instruction was the development and publication of the Information Technology Infrastructure Library™ (ITIL). ITIL is made up of a collection of 'best practices' found across the range of IT service providers. ITIL offers a systematic approach to the delivery of quality of IT services. It gives a detailed description of most of the important

[69] Gad J. Selig et al., 2008, *Implementing IT Governance*: A Practical Guide to World Class IT Management Using Current & Emerging Best Practices, TCMG 533/MGMT – IT Strategy & Governance, GPS Group, Inc., Page: 199.
[70] Gad J. Selig et al., the previous reference, page : 201.

processes in an IT organization, and includes checklists for tasks, procedures and responsibilities which can be used as a basis for tailoring to the needs of individual organizations. At the same time, the broad coverage of ITIL also provides a helpful reference guide for many areas, which can be used to develop new improvement goals for an IT organization, enabling it to grow and mature[71].

Over the years, ITIL has become much more than a series of useful books about IT Service Management. The framework for the 'best practice' in IT Service Management is promoted and further developed by advisors, trainers and suppliers of technologies or products. Since the nineties, ITIL represents not only the theoretical framework, but the approach and philosophy shared by the people who work with it in practice.

Being an extended framework of best practices for IT Service Management itself, the advantages and disadvantages of frameworks in general are also applicable to ITIL. Of course, ITIL was developed because of the advantages mentioned earlier. Many of the pointers from **best practices** are intended to avoid potential problems, or, should they occur after all, to solve them[72].

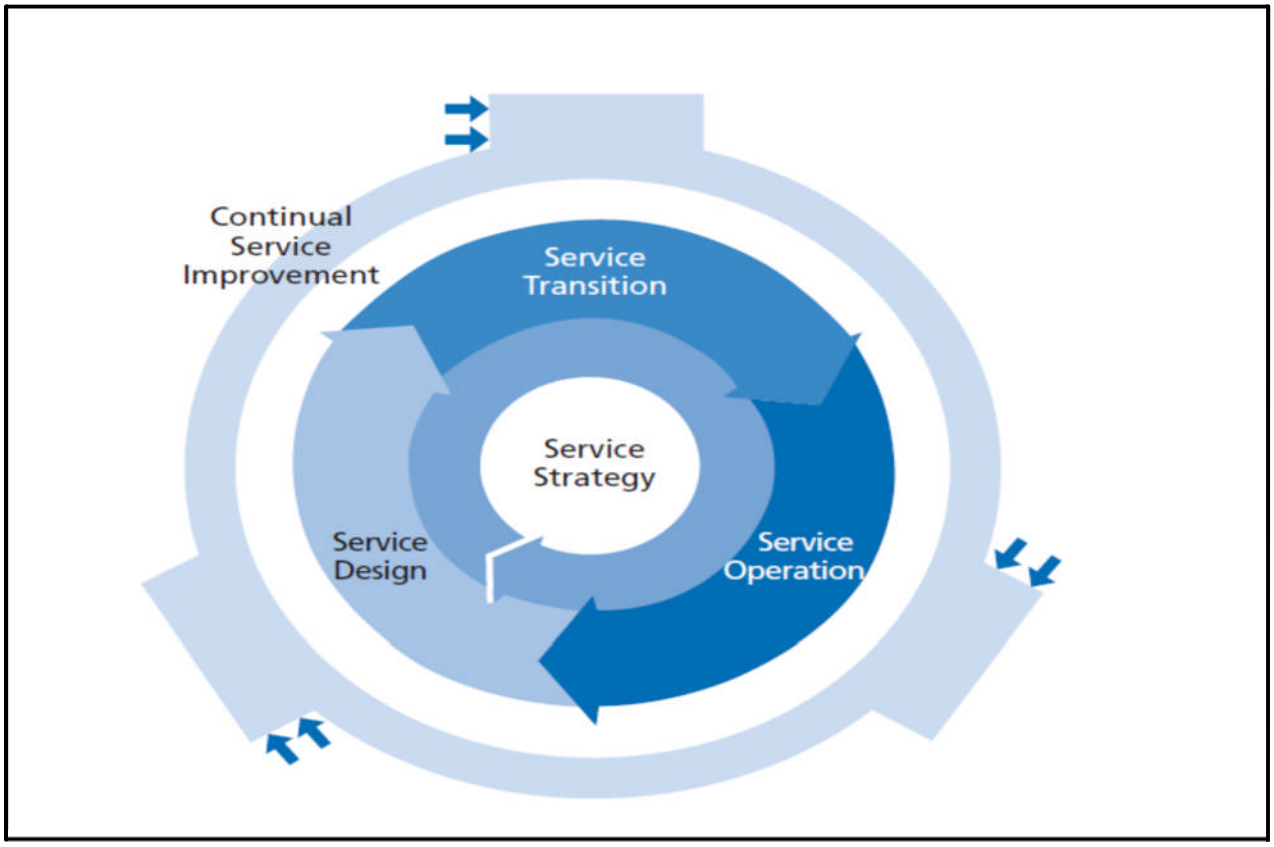
In 2007 the ITIL books have been seriously revised for the second time. The well-known Service Support book (Service Desk, Incident Management, Problem Management, Configuration Management, Change Management and Release Management) and the Service Delivery book (Capacity Management, Financial Management for IT Services, Availability Management, Service Level Management and IT Service Continuity Management) are replaced in this revision. The new ITIL structure consists of five core books, giving best practice guidance; complementary material that offers support for particular market sectors or technologies and information on the web, offering topical support products, process maps and a glossary[73]

[71] Jan van Bon et al., 2007, Foundations of IT Service Management Based on ITIL V3, Van Haren Publishing, Zaltbommel, Third edition, first impression, Page: 09

[72] Jan van Bon et al. , The previous reference, Page: 10

[73] Koen Brand & Harry Boonen, The previous reference, Page: 09.

Figure 1-9 : The ITIL publication structure



Source: Jan van Bon et al., 2007, Foundations of IT Service Management Based on ITIL V3, Van Haren Publishing, Zaltbommel, Third edition.

The books describe a service life-cycle:

• **Service Strategy:** describes the overall IT service management strategy and value planning. It deals with the traditional Business-IT alignment issues and with IT governance issues. Each subsequent book in the ITIL set links to the business goals, requirements and service management principles described in this book.

• **Service Design:** provides policies, architectures and documents for the planning and design of service management processes required to deliver quality services. It covers sourcing policies, and details on various processes that are required to deliver the services to the business.

• **Service Transition:** provides guidance for the transition of designed services into the business environment. It combines best practices on release management, program and risk management, to make sure that the required services are realized in Operations, and support the business.

• **Service Operation:** provides guidance on how to achieve effectiveness and efficiency in the delivery and the support of quality services. It covers most of the content of the service support and service delivery guidance of ITIL v2.

• **Continual Service Improvement:** provides guidance on how to identify and introduce service improvements and issues dealing with service retirement. It combines principles, practices and methods from other areas of quality management, aimed at the improved realization of initial business goals[74].

2-1-2-3- ITIL exams:

In 2007 the APM Group launched a new certification scheme for ITIL, based on ITIL version 3. ITIL version 2 will be maintained for a transition period, continuing until the year 2008. **ITIL version 2** has qualifications on three levels:

• **Foundation** Certificate in IT Service Management

• **Practitioner** Certificate in IT Service Management. There are Practitioner Certificates for various processes or functions from ITIL version 2 (Service Level Management, Capacity Management, etc) and Practitioner Certificates for clusters of the functions and processes (four clusters: Release & Control, Support & Restore, Agree & Define and Plan & Improve)

• **Manager** Certificate in IT Service Management.[75]

The ITIL version 2 exams proved to be a great success. Until 2000, some 60,000 certificates had been distributed, but in the following years the number rocketed, and by 2006 had broken the boundary of 500,000 ITIL certificates[76].

For ITIL version 3 a completely new system of qualification was set up. There are four qualification levels:

• **Foundation level** - This level is aimed at basic knowledge of, and insight into, the core principles and processes of ITIL version 3. At this level the qualification remains very similar to the old ITIL version 2 Foundation.

• Intermediate level:

[74] Koen Brand & Harry Boonen, the previous reference, page: 10.

[75] Jan van Bon et al., 2007, Foundations of IT Service Management Based on ITIL V3, Van Haren Publishing, Zaltbommel, Third edition, first impression, Page: 10.

[76] Jan van Bon et al. , The previous reference, Page : 10

– *Intermediate level 1* - The first middle level is aimed at the Service Lifecycle and is built up around the five core books of ITIL version 3: Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement.

– *Intermediate level 2* - The second middle level is aimed at capabilities and is built up around four clusters: Service Portfolio & relationship management, service design & optimization, service monitoring & control and service operation & support.

The two middle levels are aimed at an insight into, and application of, the knowledge of ITIL version 3. These levels replace the Practitioner and Manager levels of ITIL version 2.

• **Advanced level** - This level was still under development when this book was being written. It is anticipated that this will test the ability to apply ITIL version 3 principles in a real-life situation.

For every element in the scheme a number of *credits* can be obtained. Credits are also awarded for the certificates from the ITIL version 2 scheme. Various 'bridge exams' are offered in order to connect version 2 certificates to the version 3 exams. In order to obtain an ITIL version 3 diploma, the candidate must obtain 22 credits, two at Foundation level and the remainder at the middle levels[77].

2-1-3- Code of Practice for Information Security Management (ISO/IEC 17799/BS7799, ISO 27000 series):

ISO 17799 is a code of practice for information security management. This code of practice takes a baseline approach to information security. It provides 127 information security guidelines structured under 10 major headings to enable readers to identify the security controls that are appropriate to their particular business or specific area of responsibility. The standard provides guidance on the following subjects:

• Security policy
• Security organization
• Asset classification and control
• Personnel security
• Physical and environmental security
• Communications and operations management
• Access control
• System development and maintenance
• Business continuity management
• Compliance[78].

The ISO/IEC 17799 will be integrated as ISO 27002 into the ISO/IEC 27000-series, which has been defined by ISO for a range of information security management standards in similar fashion to the very successful ISO 9000-series quality assurance standards.

The following ISO 27000-series standards are either published or planned:

• **ISO 27000** - Vocabulary and definitions (terminology for all of these standards).

[77] Jan van Bon et al, The previous reference, Page: 10.

[78] Koen Brand & Harry Boonen, the previous reference, page: 07.

• **ISO 27001** - The Information Security Management System requirements standard (specification) against which organizations are formally certified
• **ISO 27002** - This is the Code of Practice describing a comprehensive set of information security control objectives and a menu of best-practice security controls.
• **ISO 27003** - Will be an implementation guide.
• **ISO 27004** - Will be a new Information Security Management Metrics and Measurement standard to help measure the effectiveness of information security management system implementations.
• **ISO 27005** - Will be a new Information Security Risk Management standard
• **ISO 27006** - May be a new standard containing "Guidelines for information and communications technology disaster recovery services", or may possibly be a guide to the accreditation process for certification bodies (we are awaiting further information)[79].

2-1-4- ISO/IEC 20000:

At the end of 2005, the International Organization for Standardization issued a standard on IT service management. This standard was based on the BS15000 standard and is issued in two parts:
• **Part 1**: Specification for information technology service management
• **Part 2**: Code of practice for information technology service management[80]

There are 5 clusters of processes within ISO/IEC 20000 each containing one to six processes:
• **Service Delivery** includes the processes that negotiate, define and agree the actual service levels, and that report performance against targets.
• **Relationship Management** contains the processes dealing with customer and supplier, both internal and external.
• **Resolution Processes** are the closely related processes incident and problem management.
• **Control Processes** are the core in the process model. They aim at controlling the components of service and infrastructure.
• **Release Process** contains only the release management process. Because of the strong relationship with configuration and change management, this process could have been merged with the Control Processes cluster[81].

2-1-5- CMMI / SPICE (ISO/IEC 15504):

The first Capability Maturity Model was developed by the Software Engineering Institute (SEI) of the Carnegie Mellon University and describes the principles and practices underlying software development process maturity. It was intended to help software organizations improve their software processes by following an evolutionary path from ad hoc, chaotic

[79] Tracey Caldwell & Steve Johnson (APM Group), ISO/IEC 27001 Foundation: A new qualification to help you understand this information security standard, available on: www.apmg-international.com/

[80] Gad J. Selig et al., the previous reference, page : 205.
[81] Tracey Caldwell & Steve Johnson (APM Group), ISO/IEC 27001 Foundation: A new qualification to help you understand this information security standard, available on: www.apmg-international.com

processes to mature, disciplined software processes. This CMM (Sw - CMM / Software CMM) was organized into five evolutive maturity levels:

0. Initial: The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.
1. Repeatable: Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.
2. Defined: The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.
3. Managed: Detailed measurements of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.
4. Optimizing: Continual process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies[82].

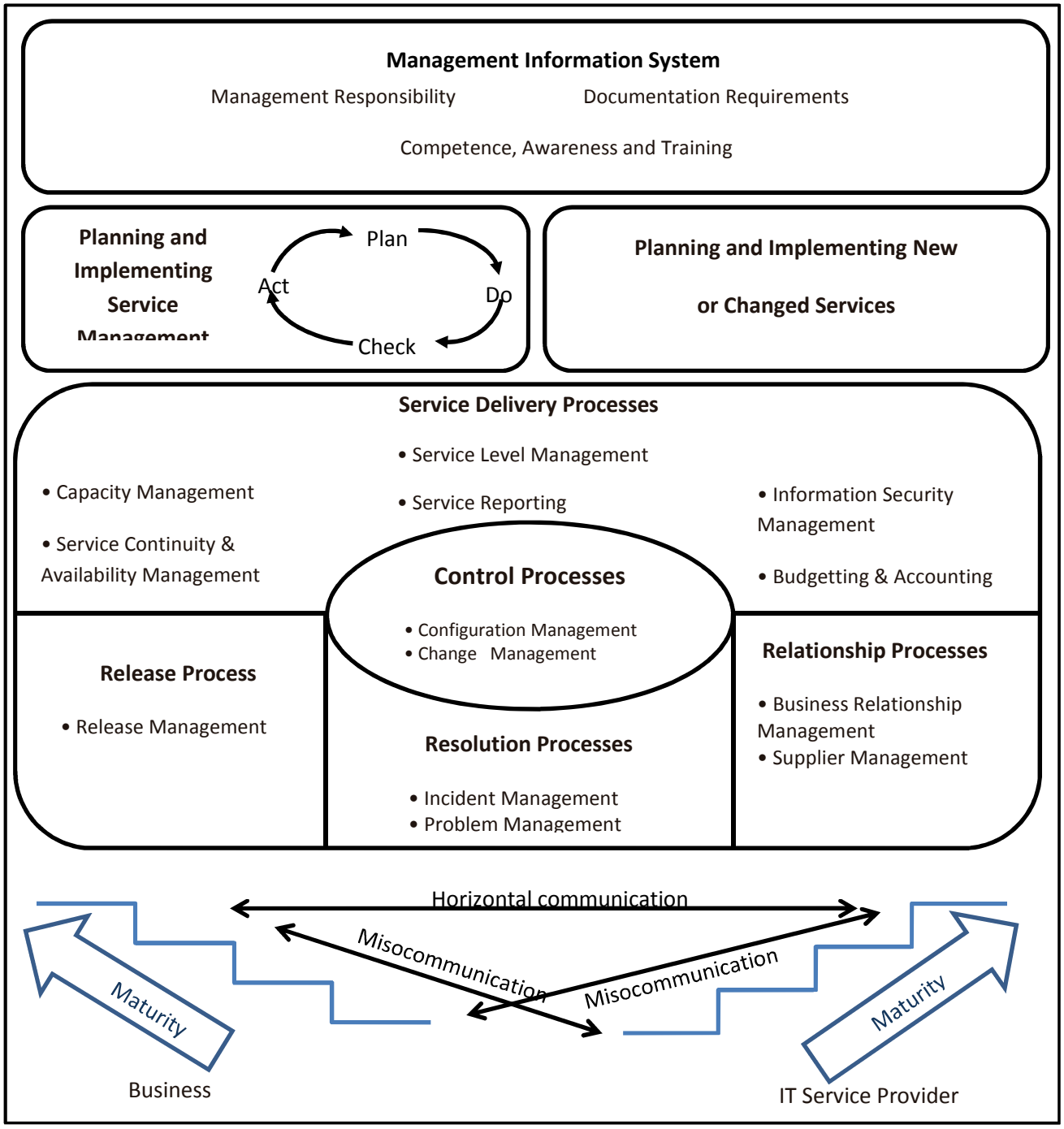
2-1-6- Quality Process models (Deming, BNQP, EFQM, ISO 9000):

Quality is addressed in a number of different models. Quality models aim at controlling and improving products and processes. While quality theory originates from business process environments, in many cases the ideas have also been adopted within IT. Deming's work focused on process improvement in an industrial production environment as a means of improving product quality. Deming created a diagram to illustrate this continuous process, known as the PDCA cycle for Plan, Do, Check, Act:

- **PLAN** - Design or revise business process components to improve results.
- **DO** - Implement the plan and measure its performance.
- **CHECK** - Assess the measurements and report the results to decision makers.
- **ACT** - Decide on changes needed to improve the process[83].

[82] Jan van Bon et al., 2007, Foundations of IT Service Management Based on ITIL V3, Van Haren Publishing, Zaltbommel, Third edition, first impression, Page: 12.
[83] Koen Brand & Harry Boonen, the previous reference, page; 15.

Figure 1-10: Overview of the ISO/IEC 20000 Service Management System



Source: Jan van Bon et al., 2007, Foundations of IT Service Management Based on ITIL V3, Van Haren Publishing, Zaltbommel, Third edition.

2-2-From IT Management to IT Governance:

For many years, some organizations could succeed despite weak IT management practices. But information —and consequently IT— is an increasingly important element of organizational products and services and the foundation of enterprise wide processes. The tight linkage between IT and organizational processes means that the IT unit cannot hear sole—or even primary- responsibility for the effective use of information and information technology. (Getting more value from IT is an increasingly important organizational competency. Leaders throughout an enterprise must develop this competency.

Research shows that top-performing enterprises generate returns on their IT investments up to 40 percent greater than their competitors. These top-performing enterprises proactively seek value from IT in a variety of ways:

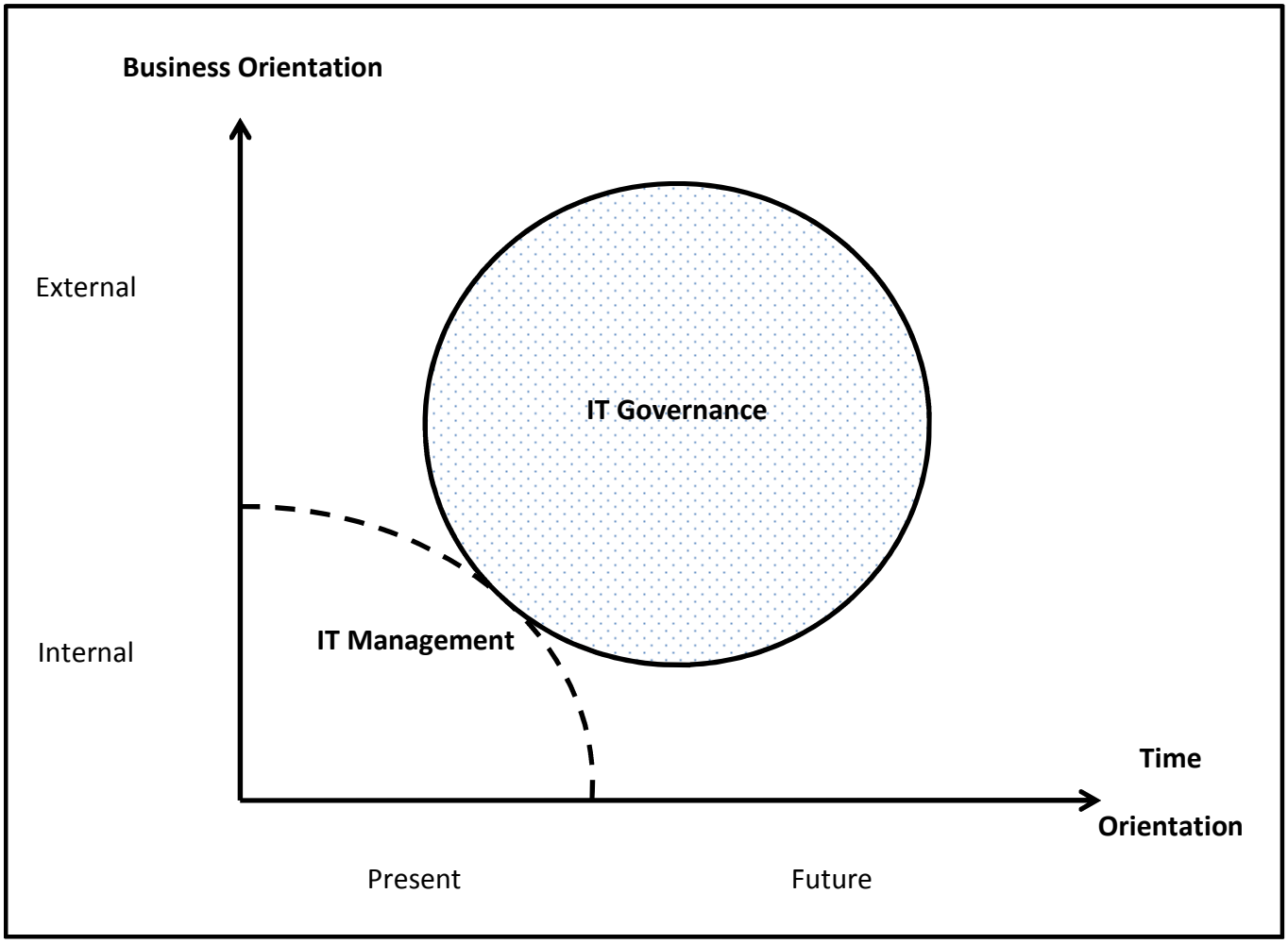
- They clarify business strategies and the role of IT in achieving them.
- They measure and marriage the amount spent on and the value received from IT.
- They assign accountability for the organizational changes required to benefit from new IT capabilities.
- They learn from each implementation, becoming more adept at sharing and reusing IT assets[84].

2-2-1-DIFFERENCES BETWEEN IT GOVERNANCE AND IT MANAGEMENT:

The difference between IT governance and IT management has to be elaborated on. Since the appearance of IT governance, it has had a tendency of being confused with IT management; therefore a clear definition is needed One aspect of IT governance definition is an important and implicit concern regarding the link between information technology and the present and future business objectives. Although there is a distinction between IT governance and IT management it is not always clear.

[84] Peter Weill and Jeanne W. Ross, 2000, IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Library of Congress Cataloging-in-Publication Data, Harvard Business School Press, page: 19.

Figure 1-11: IT Governance and IT Management

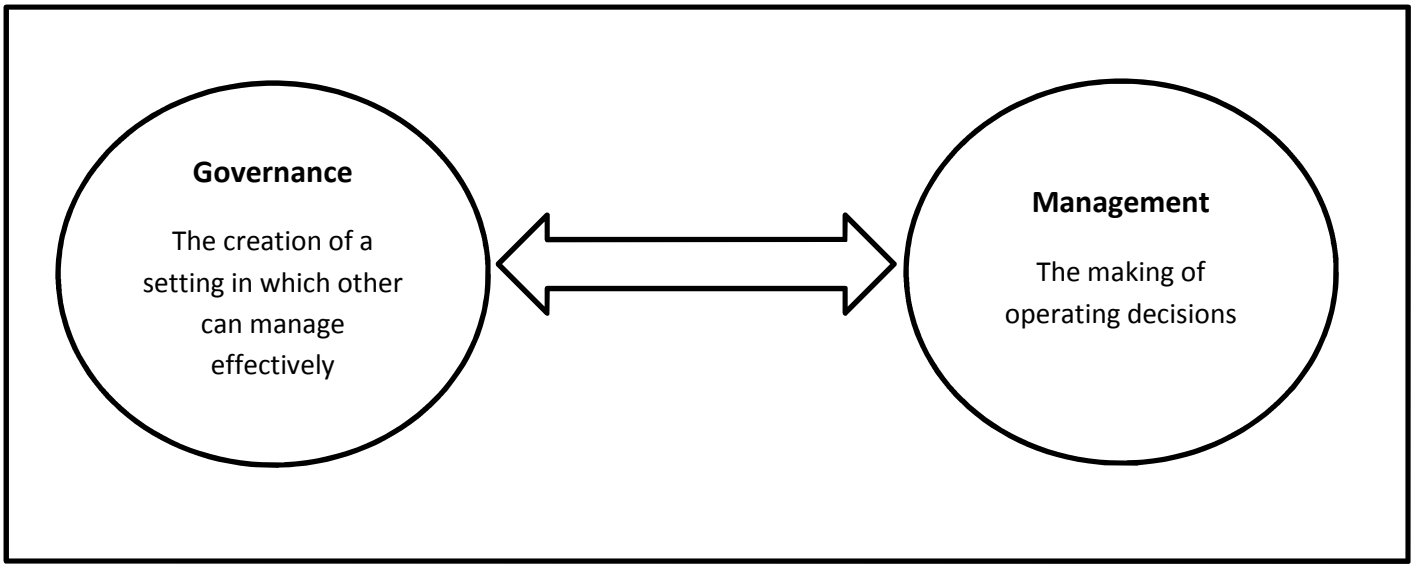


Source : Peterson (2003*). Information Strategies and Tactics for Information Technology Governance. In W. Van Grembergen (Ed.),* Strategies for Information Technology Governance *Hershey, PA: Idea Group Publishing.*

The figure shows that IT management is focused on the management of present IT operations and effective and efficient internal supply of IT services and products. IT governance has a much broader range and a wider time aspect. It also concentrates on performing and transforming IT to meet the demands of internal business and external business (business customers) of both the present and the future requirements. A quote used by van Grembergen was found useful when distinguishing between IT governance and IT management. "This does not undermine the importance and complexity of IT management, but whereas elements of IT management and

the supply of (commodity) IT services and products can be commissioned to an external provider, IT governance is organization specific, and direction and control over IT cannot be delegated to the market (Peterson, 2003)"[85]. IT governance and IT management may be two separate definitions but there exist a coupling between them that is necessary in a successful enterprise.

Figure 1-12 : Coupling between IT governance and IT Management



Source : Van Grembergen, W., DE Haes, S. , 2008, *Implementing Information Technology Governance: Models, Practices and Cases*. IGI Global

2-2-2- The Corporate Governance and IT Governance:

Good corporate governance is important to professional investors. Major institutions rank corporate governance on par with the firm's financial indicators when evaluating investment decisions. [A McKinsey study found that professional investors are even prepared to pay large premiums for investments in firms with high governance standards. Premiums ranged from an average of 13 percent in North America and Western Europe to 20 or 25 percent in Asia and Latin America and even higher in Eastern Europe and Africa. On average, when moving from poorest to best on corporate governance, firms could expect an increase of 10 to 12 percent in market value][86].

[85] Van Grembergen, W., DE Haes, 2008, S. *Implementing Information Technology Governance: Models, Practices and Cases*. IGI Global, Page: 135.

[86] Peter Weill and Richard Woodham, 2002, "Sate Street Corporation: Evolving IT Governance" working paper 327, MIT Sloan School of Management Center for Information Systems Research, Cambridge, Page: 04.

To be able to create an understanding of IT Governance and its role within an organization it is necessary to look at a broader view which can be done through viewing the corporate governance. According to OECD (2004), corporate governance establishes a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Furthermore corporate governance is defined as something that provides structure for determining organizational objectives and monitoring performance to ensure that objectives are determined[87]. This board and the senior management team work with implementation of governance principles and this makes it possible to ensure effectiveness of organizational processes.

Weill and Ross (2004) have made a framework for linking corporate and IT Governance. The framework illustrates the connection between Corporate Governance and the company's key assets governance. In the figure below the parts that touch IT Governance are marked in grey (**Figure 1-13**).

On the top of the framework the board's relationships are depicted. The senior executive team is commissioned by the board and their assignment is to formulate strategies and desirable behaviors for the organization. Below the strategy and desirable behaviors in the framework six key assets are illustrated. These assets create business value for the organization and they are:

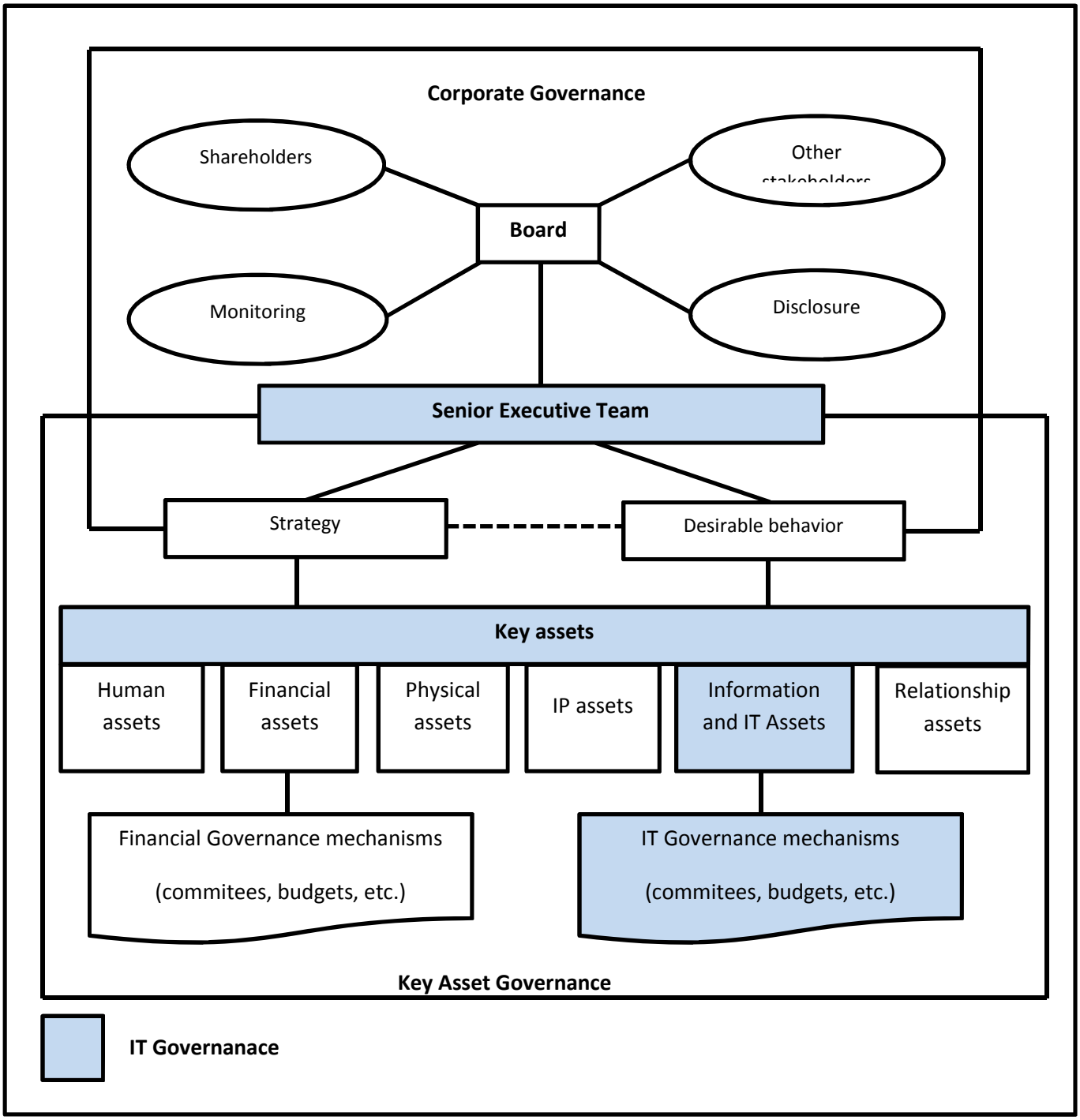
- **Human assets**: People, skills, career paths, training reporting, mentoring, competencies.
- **Financial assets**: Cash, investments, liabilities, cash flow, receivables.
- **Physical assets**: Buildings, plant, equipment, maintenance, security, utilization.
- **IP assets**: Intellectual property (IP), including product, service, and process know-how formally patented, copyrighted, or embedded in the enterprises' people and systems.
- **Information and IT assets**: Digitized data, information, and knowledge about costumers, processes performance, finance, information systems.
- **Relationship assets**: Relationships within the enterprise as well as relationships, brand, and reputation with customers, suppliers, business units, regulators, competitors, channel partners[88].

These key assets need mechanisms to be governed and used and it is the senior executive teams' task. Many of these mechanisms are possible to use within several of the assets but within some of the areas it is necessary to have unique mechanisms. To have joint governance mechanisms to ones' assets does not only increase the integration but also leads to a less amount of mechanisms which create more value.

[87] OECD (Organisation for economic co-operation and development). (2004). *Principles of Corporate Governance*. Paris:Head of Publications Service. Page: 153.

[88] OECD (Organisation for economic co-operation and development). (2004). *Principles of Corporate Governance*. Paris:Head of Publications Service. Page: 155.

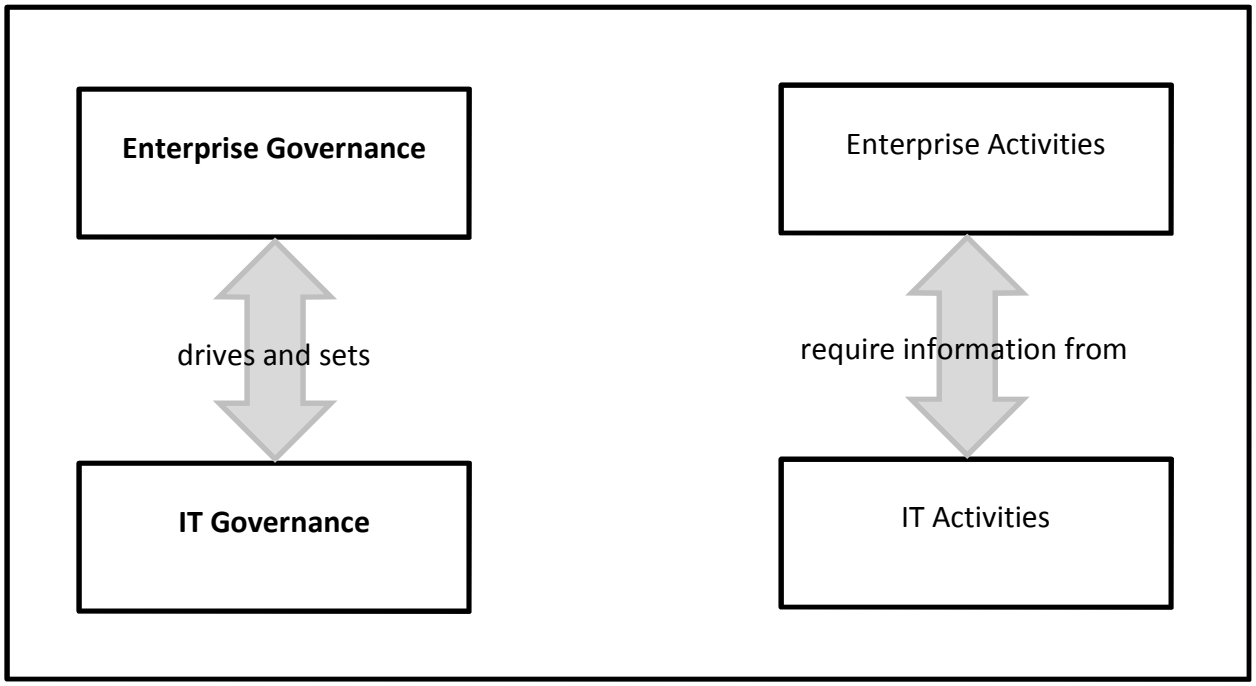
Figure 1-13: Corporate and key asset governance



Source : Peter Weill and Jeanne W. Ross, 2004, *Principles of Corporate Governance*. Paris:Head of Publications Service.

Enterprise Governance is the system by which entities are directed and controlled. The business dependency on information technology has made it so that the enterprise governance issues cannot be solved without considering Information Technology. As shown in the first part of **Figure 1-14**, enterprise governance should therefore drive and set IT Governance. Information Technology in its turn can influence strategic opportunities as outlined by the enterprise and can provide critical input to strategic plans. In this way, IT Governance enables the enterprise to take full advantage of its information, and can be seen as a driver for enterprise governance. Looking at this interplay in more depth (second part of **Figure 1-14**), enterprise activities require information from IT activities to meet business objectives, and IT must be aligned with enterprise activities to take full advantage of its information (ITGI, 2000). IT Governance and Enterprise Governance can therefore not be considered as pure distinct disciplines, and IT Governance needs to be integrated into the overall enterprise governance structure, as denoted by several authors and entities (**Guldentops**, 2003; ITGI, 2001; **Peterson**, 2003; Duffy, 2002)[89].

Figure 1-14: Enterprise Governance and IT Governance



Source: ITGI (2000). CobiT: Governance, Control and Audit for Information and Related Technology. *Available online: www.itgi.org.*

[89] Van Grembergen, De Haes & Guldentops, 2003, Strategies for information technology governance, Idea Group Publishing, Page: 06.

Governance questions are: (1) How do suppliers of finance get managers to return some of the profits to them? (2) How do suppliers of finance make sure that managers do not steal the capital they supply or invest it in bad projects? (3) How do suppliers of finance control managers? The business dependency on IT means that the Corporate Governance issues cannot be solved without considering IT. To make sure that the Corporate Governance matters are covered, IT needs to be governed properly first. This relationship can be made more eloquent by translating the Corporate Governance questions into specific IT Governance questions (**Table 1-4**) which discloses that Corporate Governance issues cannot be addressed without considering IT Governance issues[90].

Table 1-4: IT Governance and Corporate Governance Questions

Corporate Governance questions	IT Governance questions
●How do suppliers of finance get managers to return some of the profits to them?	●How does top management get their CIO and IT organisation to return some business value to them?
● How do suppliers of finance make sure that managers do not steal the capital they supply or invest it in bad projects?	●How does top management make sure that their CIO and IT organisations do not steal the capital they supply or invest in bad projects?
●How do suppliers of finance control managers?	●How does top management control their CIO and IT organisation?

Source: *Shleifer, A. & Vishny, W. (1997). A survey on corporate governance.* The Journal of Finance, 52*(2).*

IT governance integrates and institutionalizes best practices of planning, organizing, acquiring, implementing, delivering, supporting, and monitoring and evaluating IT performance, to ensure that the enterprise's information and related technology support its business objectives. IT governance enables the enterprise to take full advantage of its information, thereby maximizing benefits and capitalizing on opportunities thus leveraging competitive advantage[91]. **Table 1-5** compares the most important characteristics of corporate governance, business governance and IT governance within enterprise governance.

[90] Van Grembergen, De Haes & Guldentops, The previous reference, Page: 06.
[91] Koen Brand & Harry Boonen, The previous reference, Page : 05.

Table 1-5 : Governance characteristics

Corporate Governance	Business Governance	IT Governance
Separation of ownership and control	**Direction and control of the business**	**Direction and control of IT**
Retrospective	**Prospective**	**Prospective**
• Responsibilities, accountability & duties of directors/leaders • Legislative/Fiduciary compliance & control framework • Shareholder rights • Ethics & integrity • Business operations, risks & control • Financial accounting & reporting • Asset management • Risk management	• Business goals & objectives • Business strategic risk management • Business strategy & planning • Business processes & activities • Innovation & research capabilities • Knowledge & intellectual capital • Information management • Human resources management • Customer relations management • In- and external communication • Performance control	• IT objectives • Alignment with enterprise objectives • IT processes • IT resources • IT value delivery • IT performance management • Information knowledge management • IT strategy & planning • IT acquisition & implementation • IT operations, risks & control • IT asset management • IT risk management

Source : Center for International Private Enterprise (CIPE), 2002, Instituting Corporate Governance in developing, emerging and transitional economies: A Handbook.

2-3- Importance of IT Governance:

An ever larger percentage of the market value of enterprises has transitioned from the tangible (inventory, facilities, etc.) to the intangible (information, knowledge, expertise, reputation, trust, patents, etc.). Many of these assets revolve around the use of IT. Moreover, a firm is inherently fragile if its value emanates more from conceptual, as distinct from physical, assets.[92]. In organizations that have good IT governance, the IT organization is better aligned and integrated with the business, risks and costs are reduced, and IT helps the company gain a business advantage. Organizations in which IT governance is lacking have inadequate direction and leadership, lack of accountability, and no measurement of the outcome of IT-related decisions. IT governance is an important tool to ensure the delivery of real value from IT expenditures and to mitigate IT-related risks[93]. Jukka Perko (2008) mentioned in his PHD thesis the benefits of IT Governance set by Weill et al (2002), Weill et al (2004), ITGI (2003), Broadbent & Kitzis (2005), GAO (2004), Gartner (2002), CIPS (2005) as follows:

- **Enterprise alignment:** that is accomplished through
  - Clearly expressed business strategies and the role of IT in achieving them
  - IT strategy that is aligned with the business strategy
  - Organizational structures that facilitate the implementation of strategy and goals
  - Considered decisions about where and how IT resources should be focused
  - Guiding implementation of IT strategy by addressing the level and allocation of IT investments, and balancing the investments between those supporting and growing the enterprise
  - a culture of openness and collaboration[94]

- **Increased value from IT:** that is achieved by
  - A Chief Information Officer (CIO) who provides leadership on both the demand and supply sides
  - Ascertaining that IT delivers against the strategy through clear expectations and measurement
  - Prioritized, cost-effective, reliable IT services which are consistent with the enterprise operations and goals
  - Delivering solutions with the appropriate quality and functionality; on time, on budget, with features and functions initially specified, and with expected benefits
  - Taking an IT portfolio management approach to promote proper ranking and prioritization
  - Knowing which services or processes are to be centralized or delivered as shared services, and which are to be decentralized or provided at individual business levels

---

[92] Robert S. Roussey et al., 2003, Board Briefing on IT Governance, 2nd Edition, available on www.itgi.org, Page: 13

[93] George W. Reynolds, 2010, Information Technology for Managers, Course Technology, Cengage Learning , Boston, USA, Page: 135

[94] Jukka Perko, 2008, IT Governance and Enterprise Architecture as Prerequisites for Assimilation of Service-Oriented Architecture - An Empirical Study of Large Finnish Companies, Thesis for the degree of Doctor of Technology, Tampere University of Technology. Page: 36

- Responsible, efficient use of IT resources and being more adept in sharing and reusing IT assets[95]

❖ **Reduced IT-related risks and increased awareness of them**

- Adopting an IT control framework to achieve clear roles, responsibilities and accountabilities
- Awareness and management of IT's impact on business continuity due to increasing reliance on information and IT in all aspects of the enterprise
- Appropriate management of IT-related risks: mitigation, transfer to partners and insurance, monitoring and accepting current risk levels
- Enabling the implementation of compliance to regulatory requirements such as Sarbanes-Oxley
- Avoidance of IT failures, affecting the enterprise's value and reputation

❖ **Increased business agility and enterprise flexibility from**

- Maintaining IT's ability to support the organization's business growth – both organic and by mergers and acquisitions
- Faster response to new requirements from the business environment
- Effective use of information and knowledge by IT-enabled knowledge collection, building and distribution
- Having a capacity to follow and understand major technological events and trends to enable IT-driven strategic business change
- Taking advantage of IT's enabling capacity for new business models

❖ **Enhanced organizational learning and capabilities through communication**

- More involvement of senior management and board in information technology
- Widespread participation and understanding of governing IT use in the enterprise
- Creating constructive relationships and effective communications between the business and IT, and with external partners
- Assigning accountability for the organizational changes required to benefit from new IT capabilities
- Better and faster IT-related decisions accomplished through learning from each implementation[96]

[95] Jukka Perko, Tha previous reference, Page: 37
[96] Jukka Perko, Tha previous reference, Page: 37

2-4- Entities concerned with IT Governance:

While IT governance is the responsibility of executives and board members, governance activities must flow through various levels of the enterprise. IT governance, like most other governance activities, intensively engages both board and executive management in a cooperative manner. However, due to complexity and specialisation, the board and executive must set direction and insist on control, while needing to rely on the lower layers in the enterprise to provide the information required in decision-making and evaluation activities. To have effective IT governance in the enterprise, the lower layers need to apply the same principles of setting objectives, providing and getting direction, and providing and evaluating performance measures[97]. As a result, Good practices in IT governance need to be applied throughout the enterprise and especially between the IT function and the business units. The business units have a responsibility to work in partnership with IT to ensure that their business requirements are met. To help enable this:

- Board members should take an active role in IT strategy or similar committees.
- CEOs should provide organisational structures to support the implementation of IT strategy.
- CIOs must be business-oriented and provide a bridge between IT and the business.
- All executives should become involved in IT steering or similar committees[98].

So, IT Governance concerns the board of directors, executive management, Chief Information Officers (CIOs), Chief Executive Officers (CEOs), IT Steering Committee and IT Strategy Committee.

2-4-1- The Board:

It is a governing body of an incorporated firm. Its members (directors) are elected normally by the subscribers (stockholders) of the firm (generally at an annual general meeting or AGM) to govern the firm and look after the subscribers' interests[99]. Among the board's responsibilities are reviewing and guiding corporate strategy, setting and monitoring achievement of management performance objectives, and ensuring the integrity of the organisation systems[100].

2-4-2- Executive Management:

The executive's focus is generally on cost-efficiency, revenue enhancement and building capabilities, all of which are enabled by information, knowledge and the IT infrastructure. Because IT is an integral part of the enterprise, and as its solutions become more and more complex (outsourcing, third-party contracts, networking, etc.), adequate governance becomes a critical factor for success[101].

---

[97] Robert S. Roussey et al., The previous reference, Page: 14
[98] Robert S. Roussey et al., The previous reference, Page: 15
[99] www.businessdictionary.com/Board
[100] Wim Van Grembergen, 2004, Strategies for IT Governance, Idea Group Publishing, United States of America, Page: 271
[101] Wim Van Grembergen, The previous reference, Page: 272

2-4-3- Chief Information Officer (CIO) & Chief Executive Officer (CEO):

The CIO can be defined as the highest-ranking IT executive who typically exhibits managerial roles requiring effective communication with top management, a broad corporate perspective in managing information resources, influence on organizational strategy, and responsibility for the planning of IT to cope with a firm's competitive environment[102]. The CIO position emerged in the 1970s as a result of increased importance placed on IT. In the early 1980s, the CIO was often portrayed as the corporate savior who was to align the worlds of business and technology. CIOs were described as the new breed of information managers who were businessmen first, managers second, and technologists third. It was even postulated that in the 1990s, as information became a firm's critical resource, the CIO would become the logical choice for the chief executive officer (CEO) position[103]. CEO (Chief Executive Officer) is a top-ranking corporate position, responsible for overseeing operations. Often the company's president, the CEO reports to the chairman of the board and board members. As a rule, the CEO is the most important spokesperson for the company and is responsible for quarterly results. The CEO is also, typically, the best paid member of the company[104].

2-4-4- IT Steering Committee & IT Strategy Committee:

An IT steering committee is a governance body that reviews, monitors and prioritizes major IT projects from a cross-functional perspective. The two key concerns of a technology steering committee are:

- **Alignment:** The committee helps ensure that IT strategy is aligned with the strategic goals of the organization.
- **Ownership:** The business units represented on the steering committee have ultimate ownership over the larger IT strategic decisions since those decisions will impact their processes[105].

The IT Strategy Committee, composed of Board and non-Board members, should assist the Board in governing and overseeing the enterprise's IT-related matters. The Committee should ensure that IT is a regular item on the Board's agenda and that it is addressed in a structured manner. In addition, the Committee must ensure that the Board has the information it needs to achieve the ultimate objectives of IT Governance[106].

Typically, such a Steering Committee has the specific responsibility for overseeing a major project or managing IT priorities, IT costs, IT resource allocation, etc. While the IT Strategy Committee operates at Board level, the IT Steering Committee is situated at Executive level, which of course implies that these committees have different membership and a different authority[107].

[102] Wim Van Grembergen, The previous reference, Page: 253
[103] Wim Van Grembergen, The previous reference, Page: 254
[104] www.searchcio.techtarget.com/definition/CEO
[105] www.blog.infotech.com/research/it steering committee
[106] Wim Van Grembergen, The previous reference, Page: 23
[107] Wim Van Grembergen, The previous reference, Page: 23

Table 1-6: Comparison of Typical IT Strategy Committee and IT Steering Committee Responsibilities

	IT Strategy Committee	IT Steering Committee
Level	• Board level	• Executive level
Responsibility	• Provides insight and advice to the board on topics such as: — The relevance of developments in IT from a business perspective — The alignment of IT with the business direction — The achievement of strategic IT objectives — The availability of suitable IT resources, skills and infrastructure to meet the strategic objectives — Optimization of IT costs, including the role and value delivery of external IT sourcing — Risk, return and competitive aspects of IT investments — Progress on major IT projects — The contribution of IT to the business (i.e., delivering the promised business value) — Exposure to IT risks, including compliance risks — Containment of IT risks • Provides direction to management relative to IT strategy • Is driver and catalyst for the board's IT governance practices	• Decides the overall level of IT spending and how costs will be allocated • Aligns and approves the enterprise IT architecture • Approves project plans and budgets, setting priorities and milestones • Acquires and assigns appropriate resources • Ensures projects continuously meet business requirements, including reevaluation of the business case • Monitors project plans for delivery of expected value and desired outcomes, on time and within budget • Monitors resource and priority conflict between enterprise divisions and the IT function, and between projects • Makes recommendations and requests for changes to strategic plans (priorities, funding, technology approaches, resources, etc.) • Communicates strategic goals to project teams • Is a major contributor to management's IT governance responsibilities
Authority	• Advises the board and management on IT strategy • Is delegated by the board to provide input to the strategy and prepare its approval • Focuses on current and future strategic IT issues	• Assists the executive in the delivery of the IT strategy • Oversees day-to-day management of IT service delivery and IT projects • Focuses on implementation
Membership	• Board members and (specialist) nonboard members	• Sponsoring executive • Business executive (key users) • CIO • Key advisors as required (IT, audit, legal, finance)

Source: Robert S. Roussey et al., 2003, Board Briefing on IT Governance, 2nd Edition, available on www.itgi.org

2-5- Governance Arrangement Matrix and IT Governance Decisions:

2-5-1- Governance Arrangement Matrix:

Table 1-7 provides a grid called **"Governance Arrangements Matrix"** that addresses the first two IT governance questions: What decisions must be made and who should make them? The column heading of the Governance Arrangements Matrix lists five interrelated IT decisions.

Table 1-7: Governance Arrangements Matrix—Which Governance Archetypes are Used for Different Types of Decisions?

Decision / Archetype	IT Principles	IT Architecture	IT Infrastructure Strategies	Business Application Needs	IT Investment
Business Monarchy					
IT Monarchy					
Feudal					
Federal					
Duopoly					
Anarchy					
Don't know					

Source: Weill, P. and Ross, J.W. (2004). *IT Governance – How top performers Manage IT Decision Rights for Superior Results*. Boston: Harvard Business School Press.

- **IT Principles:** Clarifying the business role of IT[108]. High level statements about how IT is used in the business (eg scale, simplify and integrate; reduce TCO (Total Cost of Operations) and self-fund by re-investing savings; invest in customer facing systems; transform business and IT through business process transformation; strategic plan directions, PMO (project management office), sustain innovation and assure regulatory compliance, etc.)[109]

[108] Weill, P. and Ross, J.W. (2004). *IT Governance – How top performers Manage IT Decision Rights for Superior Results*. Boston: Harvard Business School Press. Page : 10

[109] Gad J Selig PMP COP, 2008, Implementing IT Governance, Van Haren Publishing, Zaltbommel, First edition, first impression, available on www.vanharen.net, Page: 09

- **IT Architecture :** Organizing logic for data, applications and infrastructure captured in a set of policies, relationships, processes, standards and technical choices, to achieve desired business and technical integration and standardization
    - **SOA architecture –** service oriented architecture (SOA) is a business-centric IT architectural approach that supports the integration of the business as linked, repeatable business tasks or services; SOA helps users build composite applications that draw upon functionality from multiple sources within and beyond the enterprise to support business processes[110]

- **IT Infrastructure :** Centrally co-ordinated, based on shared IT services that provide the foundation for the enterprise's IT capability and support[111]
- **Business application needs :** Specifying the business need for purchased or internally developed IT applications[112]
- **IT Investment and Prioritization:** decisions about how much and where to invest in IT (eg capital and expense), including development and maintenance projects, infrastructure, security, people, etc.[113]

The row headings list a set of archetypes for specifying decision rights. Each archetype identifies the type of people involved in making an IT decision:

- **Business Monarchy:** IT decisions in a Business Monarchy are taken by the senior business executives and are decisions affection the whole enterprise. The input for the decisions often comes from CIOs or IT managers in different business units[114].
- **IT Monarchy:** In IT Monarchy strategic decisions affecting IT architecture is taken where the decisions are taken by IT professionals such as IT managers. IT Monarchy can be implemented in various ways, often including IT professionals both from corporate teams and business units[115].
- **Feudal:** The Feudal entity is typical business units, regions or functions where independent decisions that are optimized for the local needs are taken. According to Weill and Ross's (2004) study the feudal model is not very common since enterprises look for synergic business units[116].
- **Federal:** The Federal decision making attempt to balance the responsibilities and accountability of multiple governing bodies, such as county and states. Both the center of the organisation and the business unit is involved in a Federal archetype. Participants can consist of unit leaders, business process owners, IT leaders from different business units and corporate IT leaders. This archetype is the most difficult model for decision making since the enterprise and business unit leaders have different concerns and represent their own unique responsibilities. Generally the biggest, most powerful

[110] Gad J Selig PMP COP, The previous reference, Page: 09
[111] Gad J Selig PMP COP, The previous reference, Page: 09
[112] Weill, P. and Ross, J.W., The previous reference. Page: 11
[113] Gad J Selig PMP COP, The previous reference, Page: 10
[114] Weill, P. and Ross, J.W., The previous reference. Page: 58
[115] Weill, P. and Ross, J.W., The previous reference. Page: 60
[116] Weill, P. and Ross, J.W., The previous reference. Page: 60

business unit is the ones getting most attention and influencing the decisions leaving smaller business units unsatisfied leaving management teams and executive committees to resolve conflicts[117].

- **IT Duopoly:** When decisions are taken in a two-party arrangement between IT executives and another group the IT Duopoly archetype is used. The IT executive group may consists of a central IT group within the enterprise, business units or a combination. The second group may consist of different CIOs, business unit leaders or business process owners. In contrary of the Federal model, IT Duopoly do not have corporate and local representation at the same time, it is always one or another including IT professionals[118].
- **Anarchy:** Decisions in an Anarchy model are taken by individuals or small groups based on their own needs. Anarchies are expensive to support and rarely sanctioned but supported when rapid responsibilities to local or individual customers need is required[119].

2-5-2-IT Governance decisions:

According to Weill and Ross (2004), there are five IT related decisions in every organisation and that these decisions have connections between them. [The five decision area are; IT principles, IT architecture, IT infrastructure, business application needs, and IT investment and prioritization][120]. Each decision needs individual attention but it is important that they are an integrated part to the others decisions, also they cannot be isolated. Weill and Ross (2004) have created a framework (**Table 1-8**) that contains the five different decisions in order to make a clear connection between decisions. IT principles clarify the company's goal for IT and are placed at the top of the framework to illustrate that these decisions will affect the other decisions. [If the IT principles not are clear within a company, the other decisions within the five IT related decision area probably will be meaningless][121].

[117] Weill, P. and Ross, J.W., The previous reference. Page: 61
[118] Weill, P. and Ross, J.W., The previous reference. Page: 62
[119] Weill, P. and Ross, J.W., The previous reference. Page: 63
[120] Peter Weill and Jeanne W. Ross, The previous reference, Page: 27
[121] Peter Weill and Jeanne W. Ross, The previous reference, Page: 27

Table 1-8 : Framework for the key IT Governance decisions

<table>
<tr><td colspan="3">IT principles decisions
High-level statements about how IT is used in the business</td></tr>
<tr><td rowspan="2">IT architecture decisions
Organisation logic for data, application, and infrastructure captured in a set of policies, relationships, and technical choices to achieve desired business and technical standardisation and integration.</td><td>IT infrastructure decisions
Centrally coordinates, shared IT services that provide the foundation for the enterprise's IT capability.</td><td rowspan="2">IT investment and prioritization decisions
Decisions about how much and where to invest in IT, including project approvals and justification techniques.</td></tr>
<tr><td>Business applications needs
Specifying the business need for purchased or internally developed IT applications.</td></tr>
</table>

Source : Weill, P. and Ross, J.W. (2004). *IT Governance – How top performers Manage IT Decision Rights for Superior Results*. Boston: Harvard Business School Press.

[Effectively answering these and similar questions (**Table 1-9**) is the job of the people tasked with making the decisions as designated by the governance design. Does the enterprise have the right people making these decisions? Are they well equipped to deal with the tradeoff?][122]

[122] Weill, P. and Ross, J.W., The previous reference. Page: 54.

Table 1-9: Questions key to each IT Decision

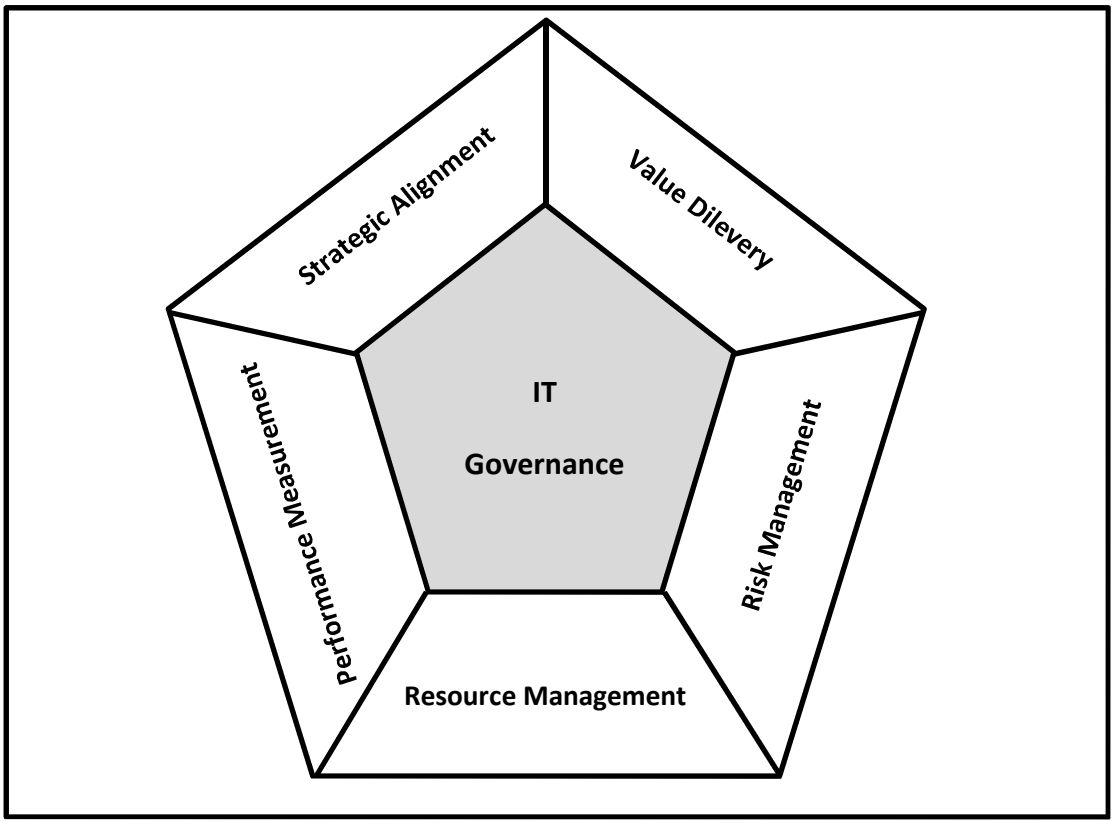
IT Principles	What is the enterprise's operating model? What is the role of IT in the business? What are IT-desirable behaviors? How will IT be funded?
IT Architecture	What are the core business processes of the enterprise? How are they related? What information drives theses core processes? How must the data be integrated? What technical capabilities should be standardized enterprisewide to support IT efficiencies and facilitate process standardization and integration? What activities must be standardized enterprisewide to support data integration? What technology choices will guide the enterprise's approach to IT initiatives?
IT Infrastructure	What infrastructure services are most critical to achieving the enterprise's strategic objectives? For each capabilities cluster, what infrastructure services should be implemented enterprisewide and what are the service-level requirements of those services? How should infrastructure services be priced? What is the plan for keeping underlying technologies up to date? What infrastructure services should be outsourced?
Business application needs	What are the market and business process opportunities for new business applications? How are experiments designed to assess whether they are successful? How can business needs be addressed within architectural standards? When does a business need justify an exception to standard? Who will own the outcomes of each project and institute organizational changes to ensure the value?
IT Investment and prioritization	What process changes or enhancements are strategically most important to the enterprise? What are the current and proposed IT Portfolios? Are these portfolios consistent with the enterprise's strategic objectives? What is the relative importance of enterprisewide versus business unit investments? Do actual investment prices reflect their relative importance?

Source: Weill, P. and Ross, J.W. (2004). *IT Governance – How top performers Manage IT Decision Rights for Superior Results*. Boston: Harvard Business School Press.

III. IT Governance Focus Areas

Fundamentally, IT governance is concerned about two things: IT's delivery of value to the business and mitigation of IT risks. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need to be supported by adequate resources and measured to ensure that the results are obtained. This leads to the five main focus areas for IT governance, all driven by stakeholder value. Two of them are outcomes: value delivery and risk management. Three of them are drivers: strategic alignment, resource management (which overlays them all) and performance measurement[123].

Figure 1-15 : IT Governance Focus Areas



Source : Ed Chavannes & Debbie Lew, 2006, Conducting an IT Governance, available on www.isaca.org

[123] Robert S. Roussey et al., The previous reference, Page: 19

3-1-Strategic Alignment:

Strategic Alignment, focuses on ensuring the linkage of business and IT plan; on defining, maintaining and validating the IT value proposition; on aligning IT operations with the enterprise operations; and establishing collaborative solutions to add value and competitive positioning to the enterprise's products and services Contain costs while improving administrative efficiency and managerial effectiveness[124].

3-1-1- The Strategic Alignment components:

The alignment of information technology and business strategy to leverage the capabilities of IT and to transform the business has increased in importance over the past few years as firms strive for competitive advantage in a diverse and changing marketplace. Firms have been able to change not only their business scope, but also their infrastructure as a result of IT innovation[125]. Luftman (1999) states twelve components for alignment :

[124] Ed Chavannes & Debbie Lew. 2006. Conducting an IT Governance Assessment. ISACA The Annual General Meeting Report. Available on www.ISACA.org. Page:05

[125] Jerry Luftman & Tom Brier, 1999. Achieving and Sustaining Business-IT Alignment. CALIFORNIA MANAGEMENT REVIEW VOL 42, NO. I. Page : 110.

Table 1-10: The Twelve Components of Alignment

Business Strategy
• **Business Scope**—Includes the markets, products, services, groups of customers/clients, and locations where an enterprise competes as well as the competitors and potential competitors that affect the business environment. • **Distinctive Competencies**—The critical success factors and core competencies that provide a firm with a potential competitive edge. This includes brand, services, research, manufacturing and product development, cost and pricing structure, and sales and distribution channels. • **Business Governance**—How companies set the roles and relationship between management, stockholders, and the board of directors. Also included are how the company is affected by government regulations and how the firm manages its relationships and alliances with strategic partners.
Organization Infrastructure and Processes
• **Administrative Structure**—The way the firm organizes its businesses. Examples include central, decentralized, matrix, horizontal, vertical, geographic, federal, and functional. • **Processes**— How the firm's business activities (the work performed by employees) operate or flow. Major issues include value-added activities and process improvement. • **Skills**—H/R considerations such as how to hire/fire, motivate, train/educate, and culture.
IT Strategy
• **Technology Scope**—The important information applications and technologies. • **Systemic Competencies** -Those capabilities (e.g., access to information that is important to the creation/achievement of a company's strategies) that distinguishes the IT services. • **IT Governance**—How the authority for resources, risk, conflict resolution, and responsibility for IT is shared among business partners. IT management, and service providers. Project selection and prioritization issues are included hens.
IT Infrastructure and Processes
• **Architecture** —The technology priorities, policies, and choices that allow applications, software, networks, hardware, and data management to be integrated into a cohesive platform. • **Processes**— Those practices and activities carried out to develop and maintain applications and manage IT infrastructure. • **Skills**—IT human resource considerations, such as how to hire/fire, motivate, train/educate, and culture.

Source: J. Luftman, 1996. Competing in the Information Age: Strategic Alignment in Practice. New York, NY: Oxford University Press.

3-1-2- The Strategic Alignment Model:

The concept of strategic alignment is based on two building blocks: **strategic fit** and **functional integration**. *Strategic fit* recognises that the IT strategy should be articulated in terms of an external domain — how the firm is positioned in the IT marketplace — and an internal domain — how the IT infrastructure should be configured and managed. The position of an organisation in the IT marketplace (external IT domain) involves three decisions:

a. Information technology scope—those specific information technologies (for example, electronic imaging, local- and wide-area networks, expert systems, and robotics) that support current business strategy initiatives or could shape new business strategy initiatives for the firm. This is analogous to business scope, which deals with choices pertaining to product-market offerings in the output market.

b. Systemic competencies—those attributes of **IT** strategy (for example, system reliability, cost-performance levels, interconnectivity, flexibility) that could contribute positively to the creation of new business strategies or better support of existing business strategy. This is analogous to the concept of business distinctive competencies, which deal with those attributes of strategy (pricing, quality, value- added service, superior distribution channels) that contribute to a distinctive, comparative advantage to a firm over its competitors.

c. **IT** governance—selection and use of mechanisms (for example, joint ventures with vendors, strategic alliances, joint research and development for new **IT** capabilities) for obtaining the required **IT** competencies. This is analogous to business governance, which involves make-versus-buy choices in business strategy. Such choices cover a complex array of interfirm relationships such as strategic alliances, joint ventures, marketing exchange, and technology licensing[126].

In a similar vein, the internal **IS** domain must address at least three components, namely:

1. **IS architecture**—choices that define the portfolio of applications, the configuration of hard-ware, software, and communication, and the data architecture that collectively define the technical infrastructure. This is analogous to the choices within the internal business strategy arena to articulate the administrative structure of the firm dealing with roles, respon-sibilities, and authority structures.
2. **IS processes**—choices that define the work processes central to the operations of the **IS** infrastructure such as systems development, maintenance, and monitoring and control systems. This is analogous to the need for designing the business processes that support and shape the ability of the firm to execute business strategies.
3. **IS skills**—choices pertaining to the acquisition, training, and development of the knowledge and capabilities of the individuals required to effectively manage and operate the **IS**

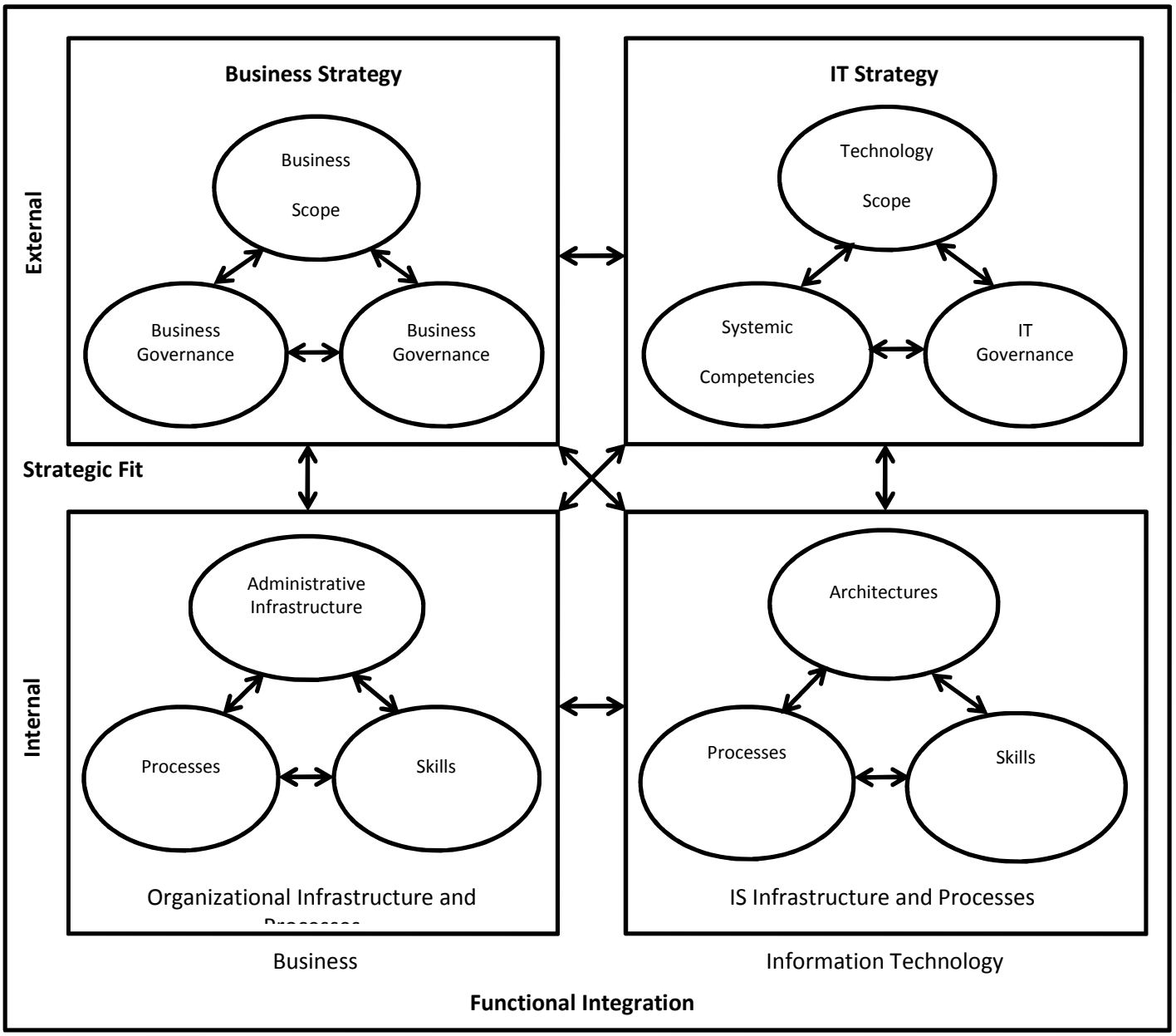
[126] Henserson, J. C. & Venkatraman, (1993). Strategic alignment: Leveraging Information Technology for transforming organizations. IBM Systems Journal. Page: 474.

infrastructure within the organization. This is analogous to the skills required within the business domain to execute a given strategy[127].

Strategic integration is the link between business strategy and IT strategy reflecting the external components, which is as important as IT and for many companies has emerged as a source of strategic advantage. The second type, operational integration, covers the internal domain and deals with the link between organisational infrastructure and processes, and IT infrastructure and process. This emphasises the importance of internal coherence between the requirements and expectations of the business and the capability of IT to deliver against it[128].

[127] Henserson, J. C. & Venkatraman, The previous reference. Page: 475.
[128] Wim Van Grembergen. The previous reference. Page: 09.

Figure 1-15 : Strategic Alignment Model

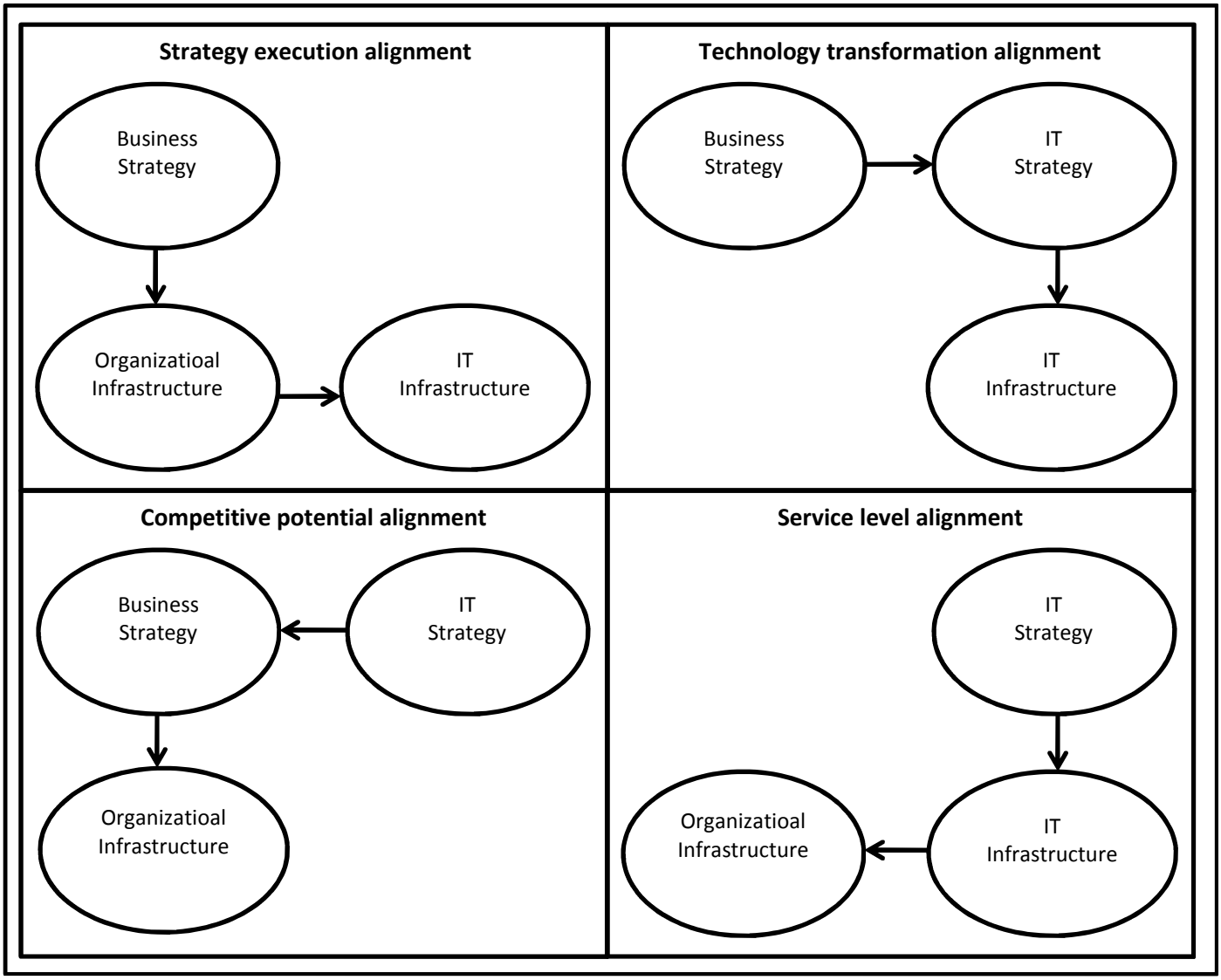


Source : *Henserson, J. C. & Venkatraman, N. (1993). Strategic alignment: Leveraging Information Technology for transforming organizations.* IBM Systems Journal.

Henderson and Venkatraman (1993) describe two cross-domain relationships in which business strategy plays the role of driver, and two relationships where IT strategy is the enabler (**Figure 1-16**). The strategic execution perspective is probably the most widely understood, as it is the classic, hierarchical view of strategic management. The perspective starts from the premise that business strategy is articulated and that this strategy is the driver for the choices in organisational design and the design in IT infrastructure. The technology transformation perspective also starts from an existing business strategy, but focuses on the implementation of this strategy through appropriate IT strategy and the articulation of the required IT infrastructure and processes. The competitive potential perspective allows the adaptation of business strategy through emerging IT capabilities. Starting from the IT strategy, the best set of strategic options for business strategy and a corresponding set of decisions regarding organisational infrastructure and processes are determined. The service level perspective focuses on how to build a world-class IT service organisation. This requires an understanding of the external dimensions of IT strategy with the corresponding internal design of the IT infrastructure and processes[129].

[129] Wim Van Grembergen. The previous reference. Page: 10.

Figure 1-16 : Strategic Alignment Domains



Source : Henserson, J. C. & Venkatraman, N. (1993). Strategic alignment: Leveraging Information Technology for transforming organizations. IBM Systems Journal.

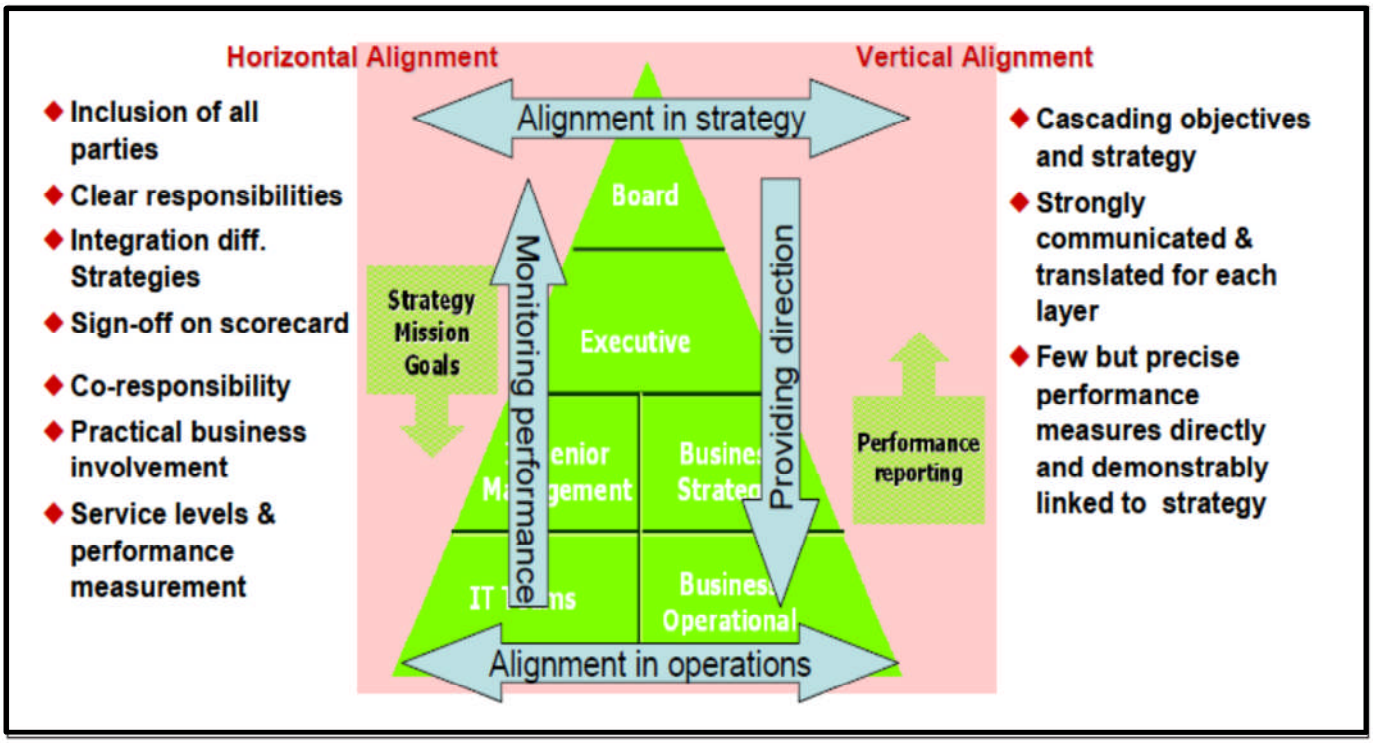
Luftman and Brier (1999) provided an approach for the practical implementation of strategic alignment, they used a six-step approach that is designed to make strategic alignment work in any organization:

- Set the goals and establish a team,
- Understand the business-IT linkage,
- Analyze and prioritize gaps,
- Specify the actions (project management),
- Choose and evaluate success criteria,
- Sustain alignment[130].

Guldentops (2003) also promotes some pragmatic practices to achieve alignment, and makes a distinction between vertical and horizontal alignment (**Figure 1-17**). According to this author, there are two types of practices, re-enforcing the point that alignment is not only needed at the strategic level but also at the operational level. **Vertical alignment** is primarily driven by repeatedly communicating an integrated Business and IT strategy down into the organisation, and translating it at each organisational layer into the language, responsibilities, values and challenges at that level. Furthermore, this 'cascading down' of the strategic objectives should be clearly linked to performance measures that are reported upwards. Horizontal alignment is primarily driven by cooperation between Business and IT on integrating the strategy, on developing and agreeing on performance measures (e.g., IT Balanced scorecard BSC) and on sharing responsibilities (e.g., IT project co-responsibility)[131].

[130] Jerry Luftman & Tom Brier, 1999. Achieving and Sustaining Business-IT Alignment. CALIFORNIA MANAGEMENT REVIEW VOL 42, NO. I. Page : 115.
[131] Wim Van Grembergen. The previous reference. Page: 11.

Figure 1-17: Vertical and Horizontal Alignment Practices



Source : Guldentops, E. (2003). IT Governance: Part and parcel of Corporate Governance. CIO Summit, European Financial Management & Marketing (EFMA) Conference, Brussels.

3-1-3-Strategic Alignment success factors and inhibitors:

Luftman (2000) and Luftman and Brier (1999) have identified some enablers and inhibitors (**Table 1-11**) that help and hinder this alignment process. These points for attention should be closely monitored by management in their effort of aligning the business and IT[132].

[132] Wim Van Grembergen. The previous reference. Page: 12.

Table 1-11: Enablers — Inhibitors of Strategic Alignment

ENABLERS	INHIBITORS
Senior executive support for IT	IT/business lack close relationships
IT involved in strategy development	IT does not prioritise well
IT understands the business	IT fails to meet commitments
Business-IT partnerships	IT does not understand the business
Well-prioritised IT projects	Senior executives do not support IT
IT demonstrates leadership	IT management lack leadership

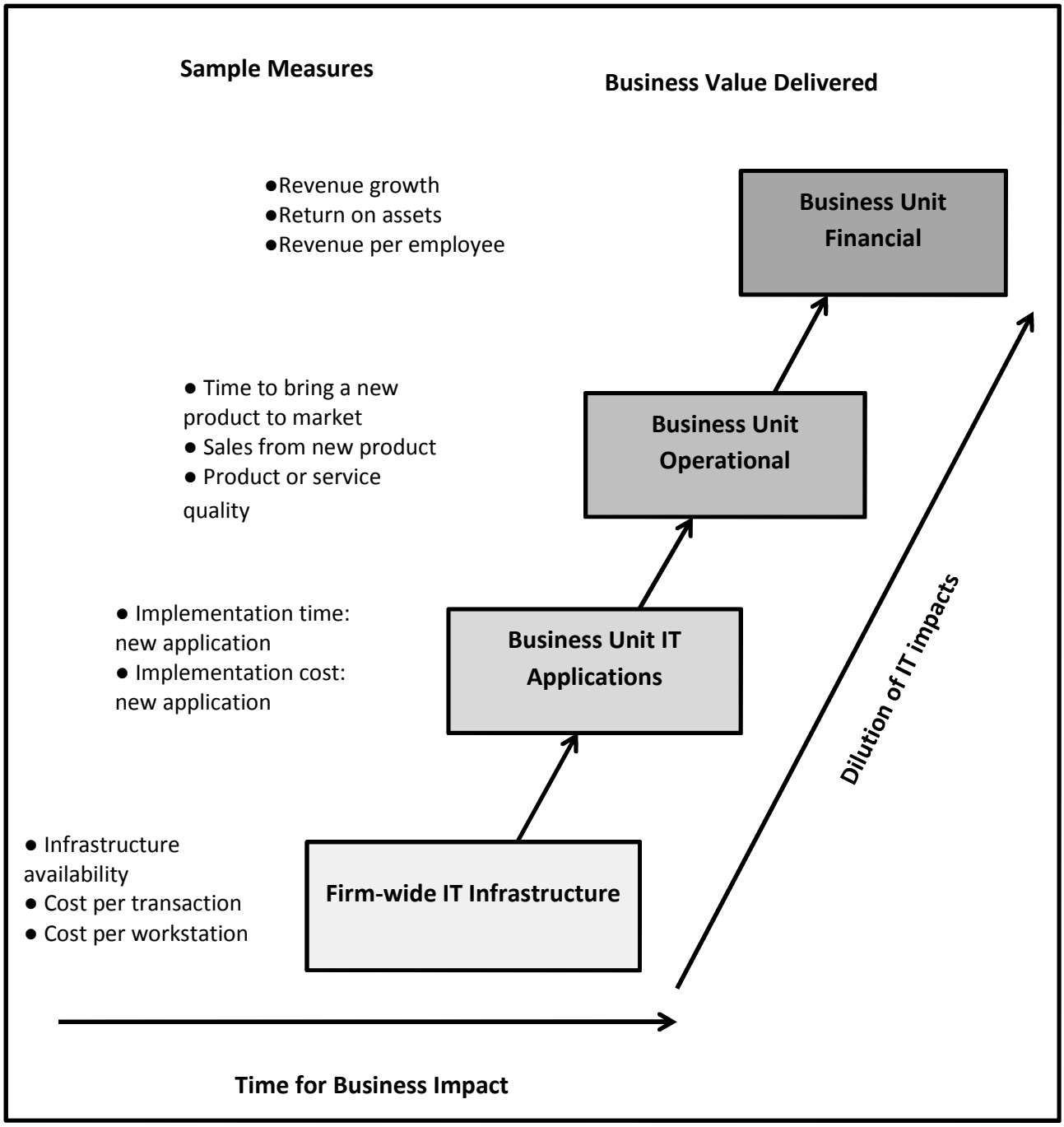
Source : Luftman, J. & Brier, T. (1999). Achieving and sustaining Business-IT alignment. California Management Review, 42(1), 109-122.

3-2- Value Delivery:

Value Delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing expenses and proving the value of IT, and on controlling projects and operational processes with practices that increase the probability of success (quality, risk, time, budget, cost ….etc.)[133]. "The value that IT adds to the business is a function of the degree to which the IT organisation is aligned with the business and meets the expectations of the business" (ITGI, 2001)[134]. The question is how investments in IT will results in measurable value for the entire business. The basic principles of IT value are delivery on time, within budget and with the benefits that were promised. In business terms, this is often translated into: competitive advantage, elapsed time for order/service fulfillment, customer satisfaction, customer wait time, employee productivity and profitability. Several of these items are either subjective or difficult to measure, something all stakeholders need to be aware of[135]. Broadbent and Weill (1998) refer in this context to the **'Business Value Hierarchy' (Figure 1-18)**.

[133] Ed Chavannes & Debbie Lew. The previous reference. Page: 06.
[134] ITGI (2001). *Board briefing on IT Governance.* Available online: www.itgi.org.
[135] Wim Van Grembergen. The previous reference. Page: 16.

Figure 1-18 : Business Value Hierarchy

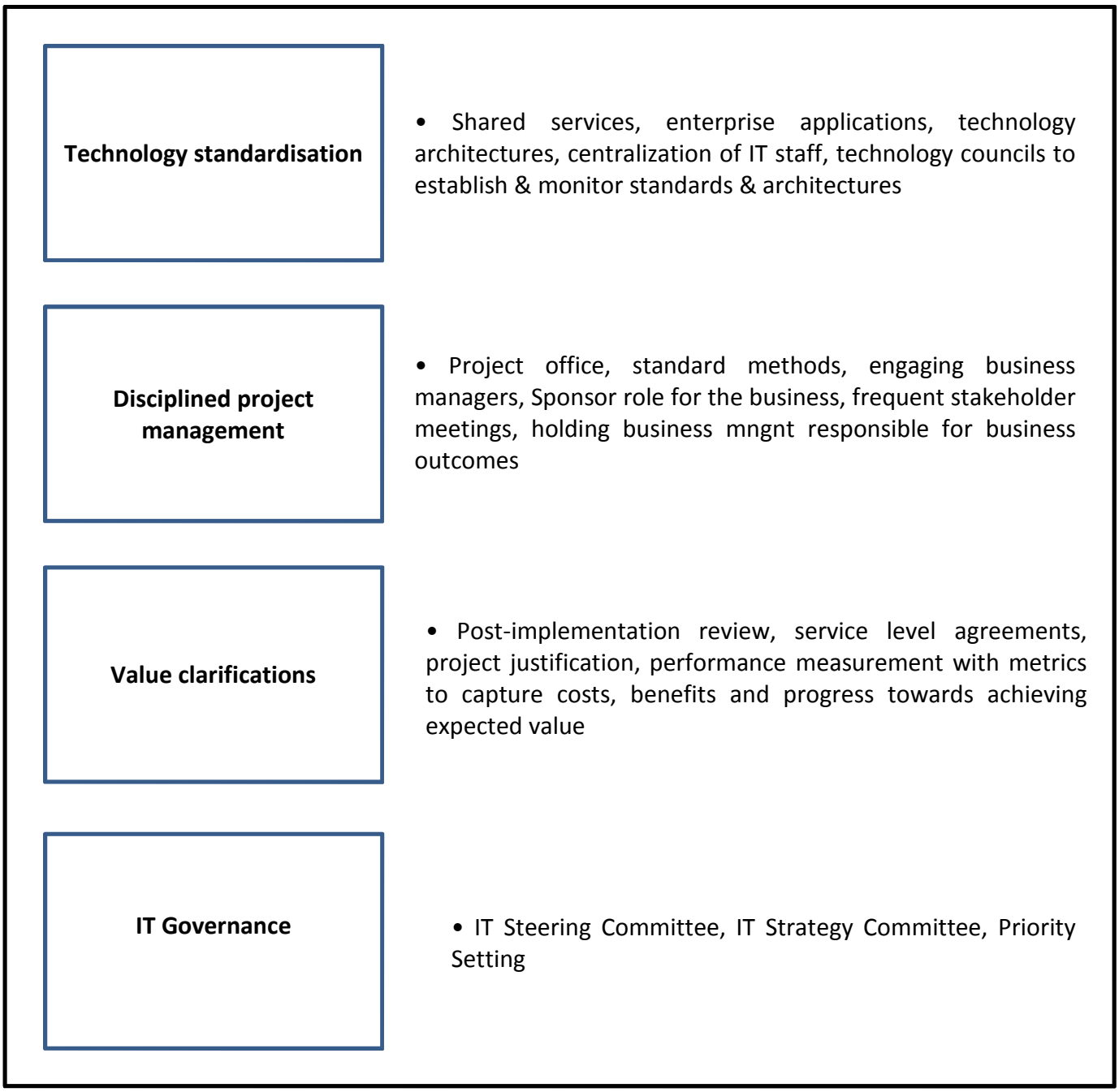


Source : Broadbent, M. & Weill, P. (1998). Leveraging the new infrastructure – How market leaders capitalize on Information Technology. Harvard Business School Press.

This hierarchy is composed of four layers: firm-wide IT infrastructure business value, business unit IT applications business value, business unit operational business value and business unit financial business value[136]. "The first level of business value is provided by firm-wide Information Technology infrastructure, with measures such as infrastructure availability (e.g., percentage of downtime), and cost per transaction and workstation. The second level of business value is provided by business-unit Information Technology performance of the business, with measures such as time and cost to implement new applications. The third level is provided by the operational performance of the business, with measures such as quality and time to market for new products. The top and most important level is the financial performance of the firm, with measures such as return on assets (ROA) and revenue growth. Investments in Information Technology are made at the bottom two levels in the hierarchy by both information systems departments and line managers. Measuring Information Technology investments at the bottom two levels and performance at all four levels is key to assessing business value. Then we can track the impact of Information Technology investments up this hierarchy of business value, providing solid evidence and insight on how value is or is not created" (Broadbent & Weill, 1998)[137]. But how can business value now pragmatically be achieved through IT? Weill (2002) identified some emerging management practices that lead to IT-enabled business value. Implementing these practices implies the use of a number of mechanisms (**Figure 1-19**).

[136] Wim Van Grembergen. The previous reference. Page: 16.
[137] Wim Van Grembergen. The previous reference. Page: 17.

Figure 1-19: Management Practices that Lead to IT-Enabled Business Value



Source : Based on: Weill, P. (2002). Research Briefing. MIT Sloan,2

3-3-Risk Management:

Risk Management requires risk awareness of senior corporate officers, a clear under-standing of the enterprise's appetite for risk and transparency about the significant risks to the enterprise; it embeds risk management responsibilities in the operation of the enterprise and specifically addresses the safeguarding of IT assets, disaster recovery and continuity of operations[138]. The management of risks is a cornerstone of IT Governance, ensuring that the strategic objectives of the business are not jeopardized by IT failures. IT related risks are increasingly a Board level issue as the impact on the business of an IT failure, be it an operational crash, security breach or a failed project, can have devastating consequences. However, managing IT risks and exercising proper governance is a challenging experience for business managers faced with technical complexity, a dependence on an increasing number of service providers, and limited reliable risk monitoring information. As a consequence, management is often concerned whether risks are being cost effectively addressed, and they need assurance that risks are under control[139].

The universal need to demonstrate good enterprise governance to shareholders and customers is the driver for increased risk management activities in large organisations. Enterprise risk comes in many varieties, not only financial risk. Regulators are specifically concerned about operational and systemic risk, within which technology risk and information security issues are prominent. The Bank for International Settlements, for example, supports that view because all major past risk issues studied in the financial industry were caused by breakdowns in internal control, oversight and IT. Infrastructure protection initiatives in the US and the UK point to the utter dependence of all enterprises on IT infrastructures and the vulnerability to new technology risks. The first recommendation these initiatives make is for risk awareness of senior corporate officers[140].

3-3-1-Classifying IT Risk:

To help organizations understand and analyze IT Risk and organize their mitigation strategies, **Figure 1-20** outlines a framework for classifying risks according to their impact on the organization. The framework classifies IT Risks as:

- **Security risk** – that information will be altered, accessed or used by unauthorized parties
- **Availability risk** – that information or applications will be inaccessible due to system failure or natural disaster, including any recovery period
- **Performance risk** – that underperformance of systems, applications, or personnel – or IT as a whole – will diminish business productivity or value

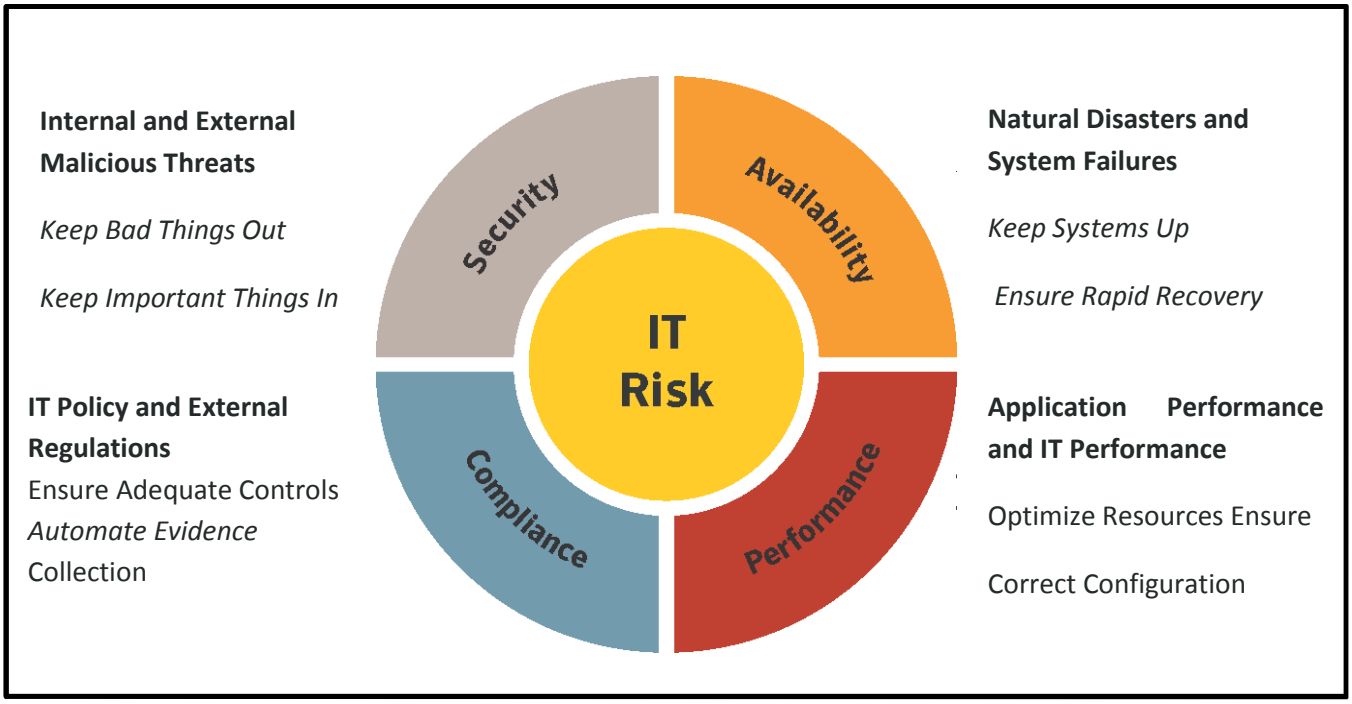
[138] Ed Chavannes & Debbie Lew. The previous reference. Page: 07.

[139] The National Computing Centre (UK). 2005. IT Governance Developing a successful governance strategy A Best Practice guide for decision makers in IT. Available on www.ncc.co.uk. Page : 28

[140] The National Computing Centre (UK). 2005. IT Governance Developing a successful governance strategy A Best Practice guide for decision makers in IT. Available on www.ncc.co.uk. Page : 28

• **Compliance risk** – that information handling or processing will fail to meet regulatory, IT or business policy requirements[141].

Figure 1-20: IT Risk spans four areas, each with its own set of drivers and potential impacts



Source: Greg Hughes, 2007, IT Risk Management Report, Symantec Corporation World, Available on www.symantec.com

3-3-2- Process and Technology Controls for IT Risk Management:

While acknowledging the relevance of Risk Management to IT, organizations often struggle to put its principles into practice. Participants' ratings of their organizations' effectiveness deploying processes and technologies for IT Risk Management depend not only on their organizations' industry, size, range of operation and other demographic factors, but on the differing perceptions of professionals within the organizations[142].

[141] Greg Hughes, 2007, IT Risk Management Report, Symantec Corporation World, Available on www.symantec.com, Page:08

[142] Greg Hughes, The previous reference, Page: 14

Table 1-12: Process and Technology Controls for IT Risk Management

Process Controls	Technology Controls
IT and Security Strategic Management, Policy and Architecture – architectures, policies and strategies defined to run IT services	**Application Design, Development and Testing** – processes, procedures, and methodologies to ensure that new and updated applications are appropriate, efficient and secure
Organizational Structure, Roles and Responsibilities – standards for interactions between groups; authority for security and external security-related communications	**Systems Build and Deployment** – systems and technologies to assure effective, secure deployment of new and updated systems
Training and Awareness – processes to increase visibility and knowledge of security risks	**Data Life Cycle Management** – technology to move, replicate and protect data
Assessment and Auditing – processes to assess the environment, controls, policies and processes used to implement strategy	**Configuration and Change Management** – tools and processes to regulate change
Authentication, Authorization and Access Management – processes and technology to verify users' identities and control access to resources	**Resilient Infrastructure** – technology to detect and correct vulnerabilities related to availability
Operational Design, Workflows and Automation – design and implementation of automated solutions; workflow and resource management	**Performance Management** – technology to monitor and manage system performance
Asset Inventory, Classification and Management – processes to identify and classify assets, supporting execution of asset-class-based policies	**Network, Protocol and Host Security** – network design and infrastructure including segmentation, protocols, perimeter defense and availability
Incident Readiness and Response – standards for preparation for and response to incidents	**Physical Security** – technologies governing access to IT infrastructure and facilities

Source: Greg Hughes, 2007, IT Risk Management Report, Symantec Corporation World, Available on www.symantec.com

3-4- Resource Management:

Along with the development of an increasingly complicated environment, the complexity of the management environment increases and traditional management tools can no more satisfy the needs of managers. To assist IT staff to solve system related problems promptly, ITRM incorporates preventive concepts to provide an integrated platform for monitoring and management. Through service level monitoring and precautionary facilities, managers can find the potential issues and take preventive measures. This will dramatically decrease the possibility of the problem actually occurring, and effectively enhance the service operation performance of the enterprise as a whole[143].

A key to successful IT performance is the optimal investment, use and allocation of IT resources (people, applications, technology, facilities, data) in servicing the needs of the enterprise. Most enterprises fail to maximize the efficiency of their IT assets and optimise the costs relating to these assets. In addition, the biggest challenge in recent years has been to know where and how to outsource and then to know how to manage the outsourced services in a way that delivers the values promised at an acceptable price. Boards need to address appropriate investments in infrastructure and capabilities by ensuring that:

- The responsibilities with respect to IT systems and services procurement are understood and applied
- Appropriate methods and adequate skills exist to manage and support IT projects and systems
- Improved workforce planning and investment exist to ensure recruitment and, more important, retention of skilled IT staff
- IT education, training and development needs are fully identified and addressed for all staff
- Appropriate facilities are provided and time is available for staff to develop the skills they need[144].

In most enterprises, the biggest portion of the IT budget relates to ongoing operations. Effective governance of IT operational spending requires effective control of the cost base: the IT assets and their focus where they are needed most. Enterprises should align and prioritise the existing IT services that are required to support business operations based on clear service definitions. These definitions and related performance metrics enable business-oriented service level agreements providing a basis for effective oversight and monitoring of both internal and outsourced IT services. The IT assets should be organised optimally so that the required quality of service is provided by the most cost-effective delivery infrastructure. Companies that achieve

[143] http://www.iisigroup.com (10/04/2013)
[144] Robert S. Roussey et al., 2003, Board Briefing on IT Governance, 2nd Edition, available on www.itgi.org, Page: 28

this not only realise great cost savings but also are well placed to take on the next new IT initiative, judiciously introducing new technologies and replacing or updating obsolete systems.

IT assets are complex to manage and continually change due to the nature of technology and changing business requirements. Effective management of the life cycle of hardware, software licences, service contracts and permanent and contracted human resources is a critical success factor not only for optimising the IT cost base, but also for managing changes, minimizing service incidents and assuring a reliable quality of service. Of all the IT assets, human resources represent the biggest part of the cost base and, on a unit basis, the one most likely to increase. It is essential to identify and anticipate the required core competencies in the workforce. When these are understood, an effective recruitment, retention and training programme is necessary to ensure that the organisation has the skills to utilize IT effectively to achieve the stated objectives. The ability to balance the cost of infrastructure assets with the quality of service required (including those services provided by outsourced external service providers) is critical to successful value delivery. It is also a powerful reason for adopting sound performance measurement systems like the balanced scorecard[145].

3-5- Performance Measurement:

One of the greatest challenges faced by those trying to manage IT in today's fast moving economy and complex technical environment is knowing whether the "ship is on course" and being able to predict and anticipate failures before it is too late. Like driving a car or steering a ship, good instruments are essential. The use of measures to help steer the IT function has for many years been a challenge that few appear to have successfully addressed, which is why the expression "it's like driving a car with a blacked out windscreen and no instruments" is often used. There is no doubt that a practical and effective way to measure IT performance is an essential part of any IT Governance programme, just as transparency and reliability of financial results is a Corporate Governance necessity. Performance management is important because it verifies the achievement of strategic IT objectives and provides for a review of IT performance and the contribution of IT to the business (i.e. delivery of promised business value). It is also important in providing a transparent assessment of IT's capability and an early warning system for risks and pitfalls that might otherwise have been missed. Performance measurement provides transparency of IT related costs, which increasingly account for a very significant proportion of most organizations' operating expenses[146].

Stakeholders play a key part in IT Governance, since at the heart of the governance responsibilities of setting strategy, managing risks, allocating resources, delivering value and measuring performance, are the stakeholder values, which drive the enterprise and IT strategy. For performance measurement to be successful, it is important to understand who the

[145] Robert S. Roussey et al., The previous reference , Page: 29.

[146] The National Computing Centre (UK). 2005. IT Governance Developing a successful governance strategy A Best Practice guide for decision makers in IT. Available on www.ncc.co.uk. Page : 09.

stakeholders are and what their specific requirements and drivers are so that the performance measurements will be meaningful to them. An IT Governance best practice is the approval of measures by stakeholders. A performance measurement system is only effective if it serves to communicate to all who need to know what is important and then motivates positive action and alignment to common objectives. The measures are not an end in themselves but a means to take corrective action and to learn from real experiences. Concise and understandable communication and clear accountabilities are therefore critical success factors if measures are to be turned into effective actions[147].

Strategy has taken on a new urgency as enterprises mobilise intangible and hidden assets to compete in an information-based global economy. The means of value creation has shifted from tangible to intangible assets, and intangible assets generally are not measurable through traditional financial means. Balanced scorecards translate strategy into action to achieve goals with a performance measurement system that goes beyond conventional accounting, measuring those relationships and knowledge-based assets necessary to compete in the information age: customer focus, process efficiency and the ability to learn and grow.

Each perspective is designed to answer one question about the enterprise's way of doing business:

• Financial perspective—To satisfy our stakeholders, what financial objectives must we accomplish?

• Customer perspective—To achieve our financial objectives, what customer needs must we serve?

• Internal process perspective—To satisfy our customers and stakeholders, in which internal business processes must we excel?

• Learning perspective—To achieve our goals, how must our organisation learn and innovate?[148]

3-5-1- Areas to measure:

The ownership of measures and accountability for achieving targets should be clear. Furthermore, ownership and the collection of measurement data will not always be an IT responsibility, e.g. measurement of customer-focused outcomes. It should therefore also be clear whose responsibility collection is. Where appropriate, measures should be formalized in Service Level Agreements (SLAs) based on service descriptions written in a language and using terms meaningful to the customer. For third party service providers an SLA should form part of the contractual agreement so that performance measurement can be backed up with contractual recourse in the event of performance failure. To support IT Governance the following top fifteen areas to measure are recommended, with an indication of who has a primary interest and therefore who should approve the measures[149].

---

[147] The National Computing Centre (UK). 2005. IT Governance Developing a successful governance strategy A Best Practice guide for decision makers in IT. Available on www.ncc.co.uk. Page : 09.

[148] Robert S. Roussey et al., The previous reference. Page: 29.

[149] The National Computing Centre (UK). 2005. IT Governance Developing a successful governance strategy A Best Practice guide for decision makers in IT. Available on www.ncc.co.uk. Page : 12.

Table 1-13: Areas to measure

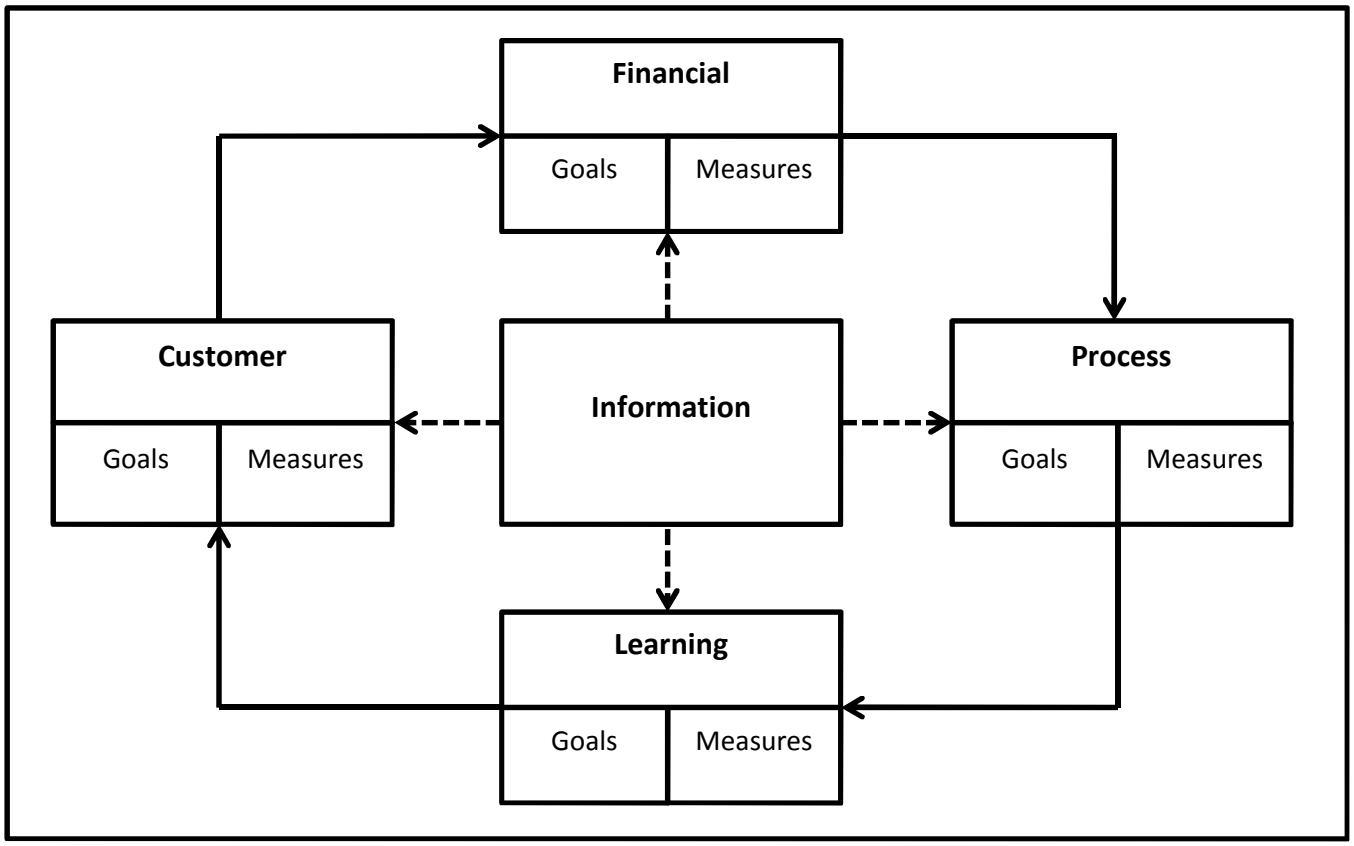
Area	Investors	Controllers	Providers
Business & IT alignment	√		
Major project delivery performance (objectives, time and budget)	√		√
Overall financial performance (costs v. budgets)	√	√	√
ROI for IT investments (business benefit)	√		√
Status of critical risks	√	√	√
Performance with respect to reliability and availability of critical services	√		√
Complaints (QOS) and customer perception	√		
Number of significant reactive fixes to errors			√
Service Level Agreements (SLA) performance by third parties	√		√
Relationships with suppliers (quality & value)	√		√
Capability e.g. process maturity			√
HR measures for people involved in IT activities			√
Internal and external benchmarks	√		√
Audit weaknesses		√	√
Business continuity status	√	√	√

Source : The National Computing Centre (UK). 2005. IT Governance Developing a successful governance strategy A Best Practice guide for decision makers in IT. Available on www.ncc.co.uk.

3-5-2- The Balanced Scorecard:

The Balanced Scorecard is a management system that enables organizations to clarify their vision and strategy and translate them into action. It provides feedback about both the internal business processes and external outcomes enabling the continual improvement of strategic performance and results.[150] By using the balanced scorecard, managers rely on more than short-term financial measures as indicators of the company's performance. They also take into account such intangible items as level of customer satisfaction, streamlining of internal functions, creation of operational efficiencies and development of staff skills. This unique and more holistic view of business operations contributes to linking long-term strategic objectives with short-term actions[151].

Figure 1-21: Balanced Scorecard Dimensions

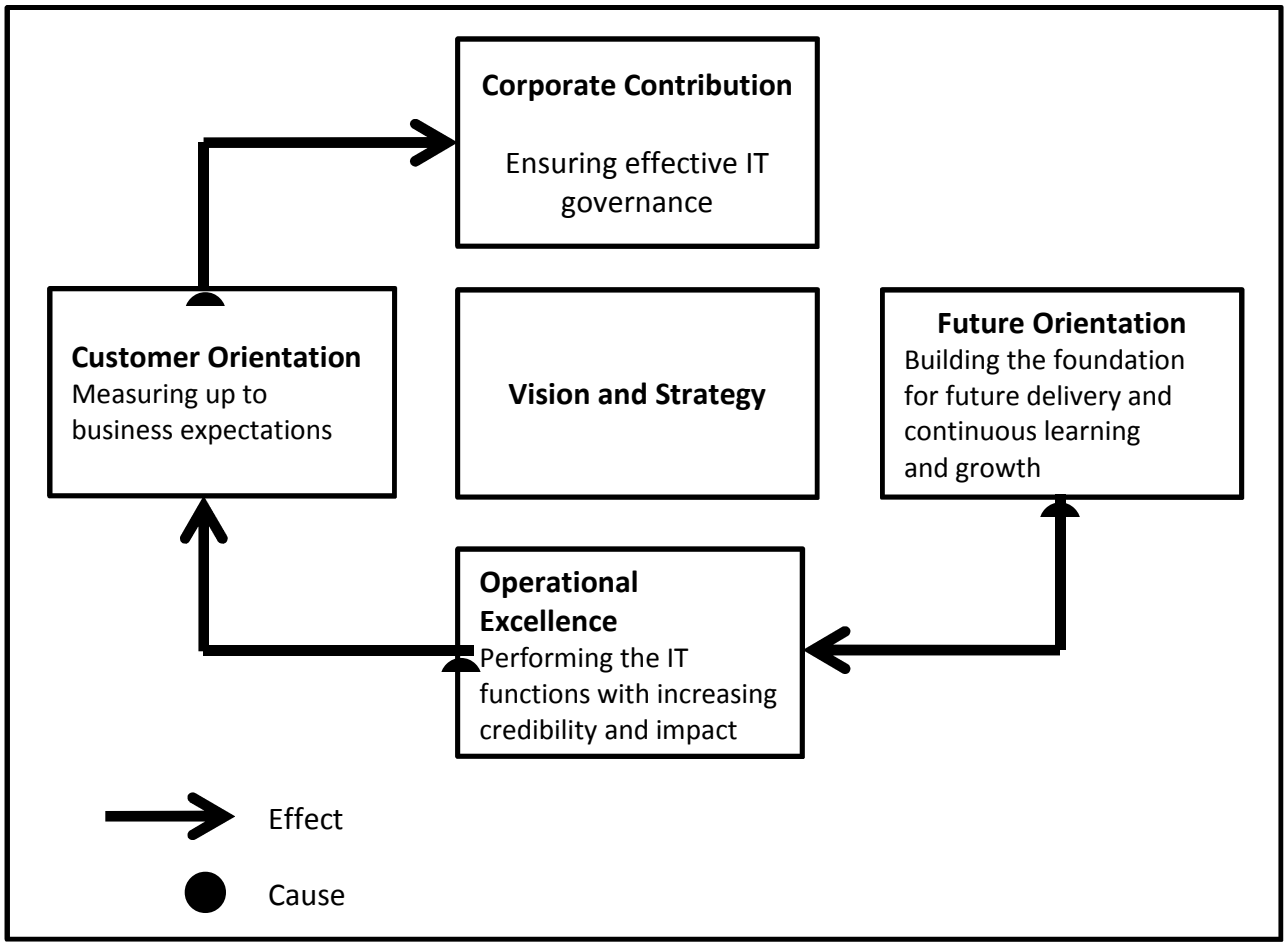


Source : Robert S. Roussey et al., 2003, Board Briefing on IT Governance, 2nd Edition, available on www.itgi.org

[150] Koen Brand & Harry Boonen, The previous reference, Page: 16
[151] Robert S. Roussey et al., The previous reference, Page : 29

Use of an IT balanced scorecard (IT BSC) is one of the most effective means to aid the board and management to achieve IT and business alignment. The objectives are to establish a vehicle for management reporting to the board, to foster consensus among key stakeholders about IT's strategic aims, to demonstrate the effectiveness and added value of IT and to communicate about IT's performance, risks and capabilities[152].

Figure 1-22: Cause and Effect Relationships Between Scorecard Dimensions



Source : Robert S. Roussey et al., 2003, Board Briefing on IT Governance, 2nd Edition, available on www.itgi.org

[152] Robert S. Roussey et al., The previous reference, Page : 30

3-5-3- How to assess IT Governance:

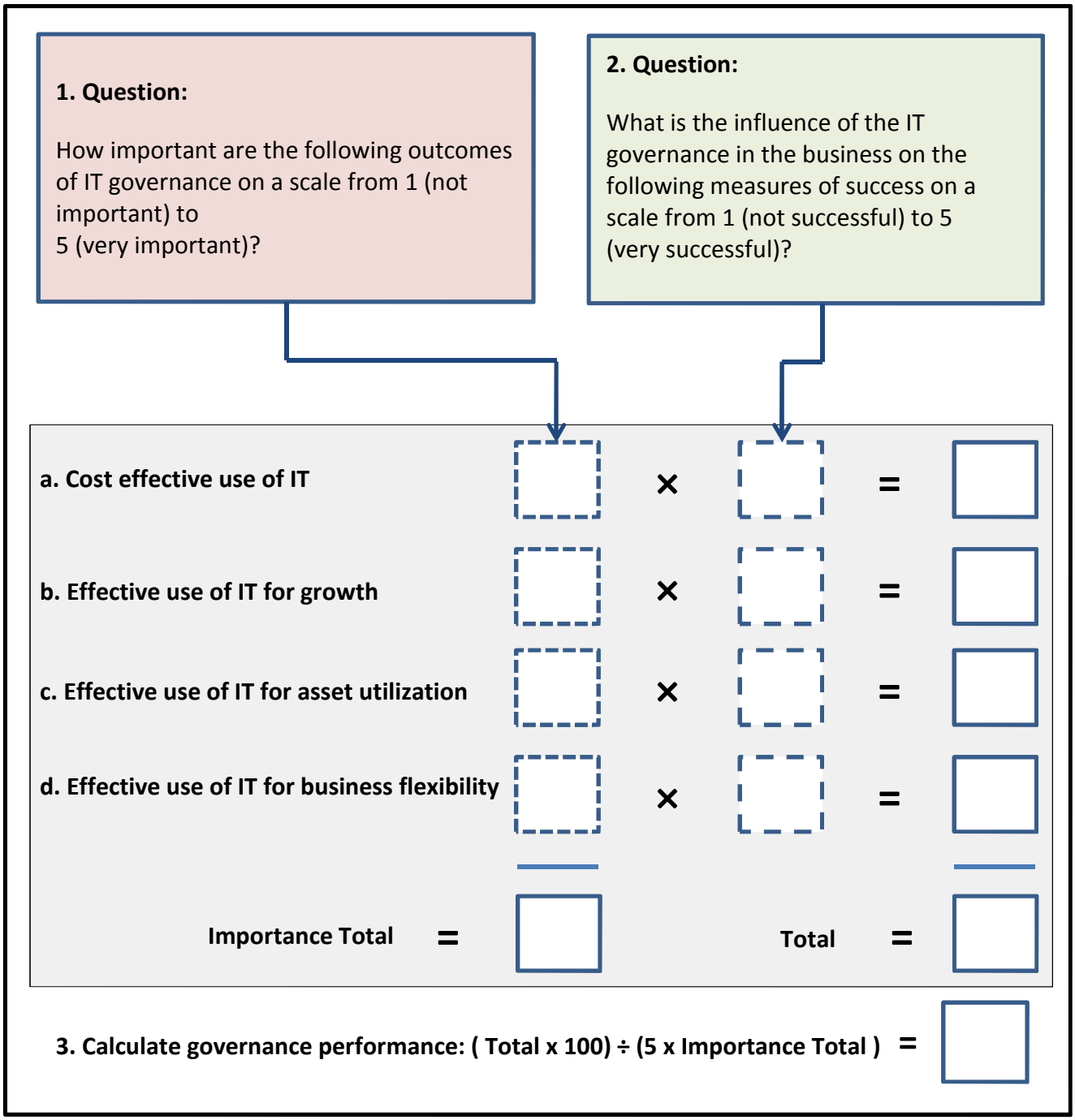
The board assesses an enterprise's or business unit's governance performance by evaluating the effectiveness of IT governance in delivering four objectives weighted by their importance to the enterprise:

- Cost effective use of IT
- Effective use of IT for asset utilization
- Effective use of IT for growth
- Effective use of IT for business flexibility.

When assessing governance performance senior managers first identify the relative importance of each of the four factors in their enterprises and then rate enterprise performance on each factor. Using a weighted average formula a score out of 100 is calculated[153]. **Figure 1-23** contains the questions and formula to calculate governance performance.

[153] Weill, P. and Ross, J.W., The previous reference. Page: 121

Figure 1-23 : IT Governance assessment



Source : Weill, P. and Ross, J.W. (2004). *IT Governance – How top performers Manage IT Decision Rights for Superior Results*. Boston: Harvard Business School Press.

CHAPTER 02

COBIT 5 AND ITS USE IN IT GOVERNANCE

INTRODUCTION:

Managers seek to find most effective frameworks for practicing IT Governance successfully. This led to make a string of studies from 2004 until now. COBIT 5 is the latest framework, it has established for the purpose of providing further guidance, and more details about how to govern the use of information technology, develop strategy, manage investments in information technology, deliver value, optimise resources, manage performance and govern IT risks. This chapter reviews the literature concerning COBIT 5 and its critical role in IT Governance. It has been divided into three parts.

The first part deals with COBIT 5 theoretical content between past and present, it begins by historical emergence and development of Cobit over different chorological phases. It will then go on to comparing COBIT 5 with other relevant standards and frameworks; highlighting common and different points. Finally, it will list COBIT 5 principles.

The second part aims to show various COBIT 5 structures and processes. In the first place, it will introduce goals' hierarchy for different corporate entities, which is called as Goals Cascade. It will then move on COBIT 5 enablers, which affect a set of processes, these latest will be involved in an integrated framework that is scientifically known as Process Reference Model. The last point is about Process Capability Model as an assessment tool for COBIT 5.

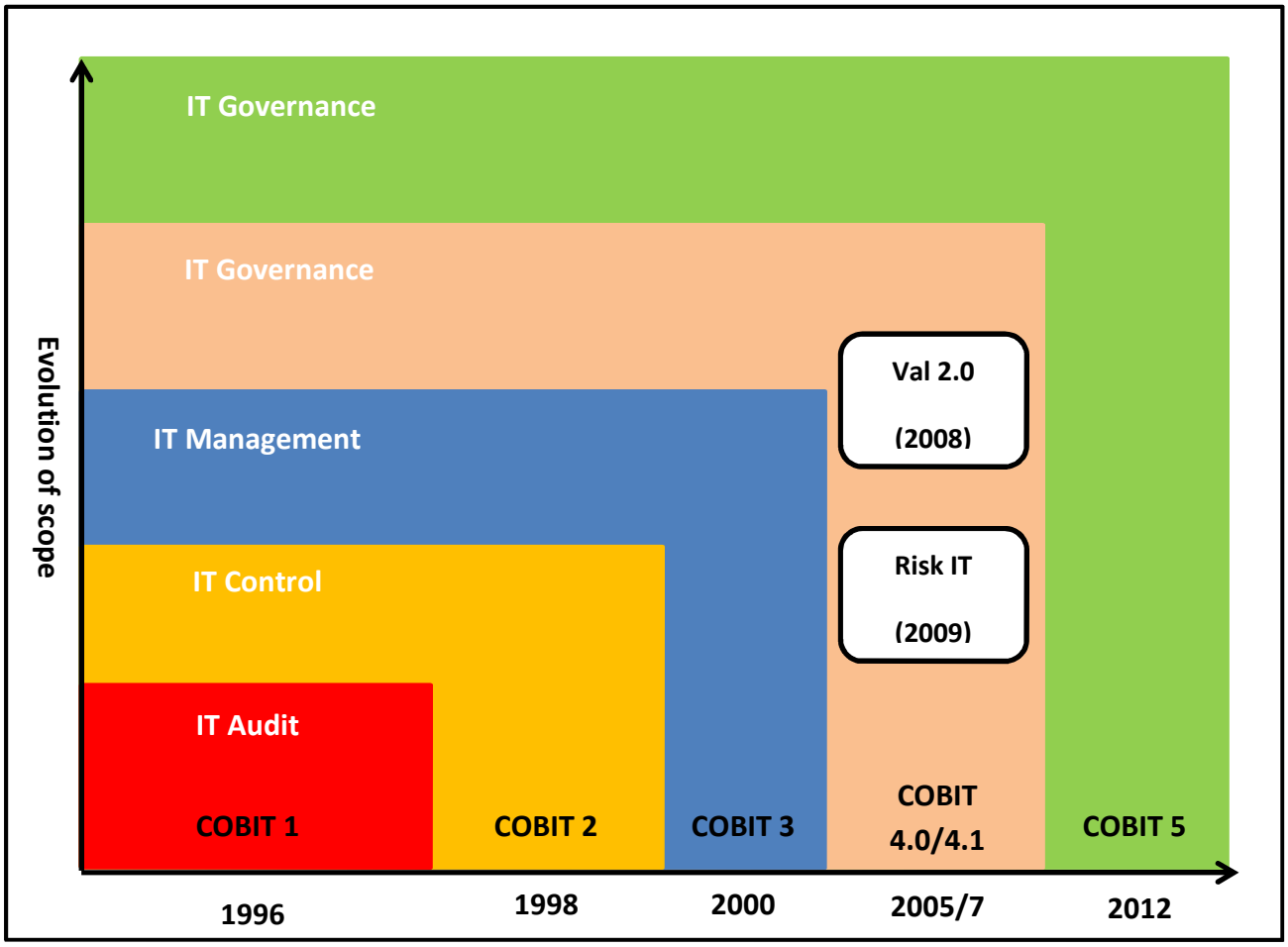
The third part gives account of usefulness of using COBIT 5 for implementing IT Governance. Firstly, it will set the light on the preparative steps towards IT Governance. Secondly, it will represent in detail the implementation life cycle tasks, roles, and responsibilities. Lastly, it will seek to clarify the impact of COBIT 5 framework on IT Governance through both its output, and its components.

I. COBIT 5: A CONCEPTUAL BACKGROUND

1-1- Historical Evolution of Cobit:

COBIT has had four major releases; in 1996, the first edition of COBIT was released. In 1998, the second edition added "Management Guidelines". In 2000, the third edition was released. In 2003, an on-line version became available. In December 2005, the fourth edition was initially released. In May 2007, the 4.1 revision was released. COBIT 5 is the latest edition of ISACA's globally accepted IT governance framework that ISACA has officially released by on April 12, 2012. It consolidates and integrates the COBIT 4.1, Val IT 2.0 and Risk IT frameworks, and also draws significantly from the Business Model for Information Security (BMIS) and ITAF.

Figure 2-1: Historical evolution of Cobit Releases

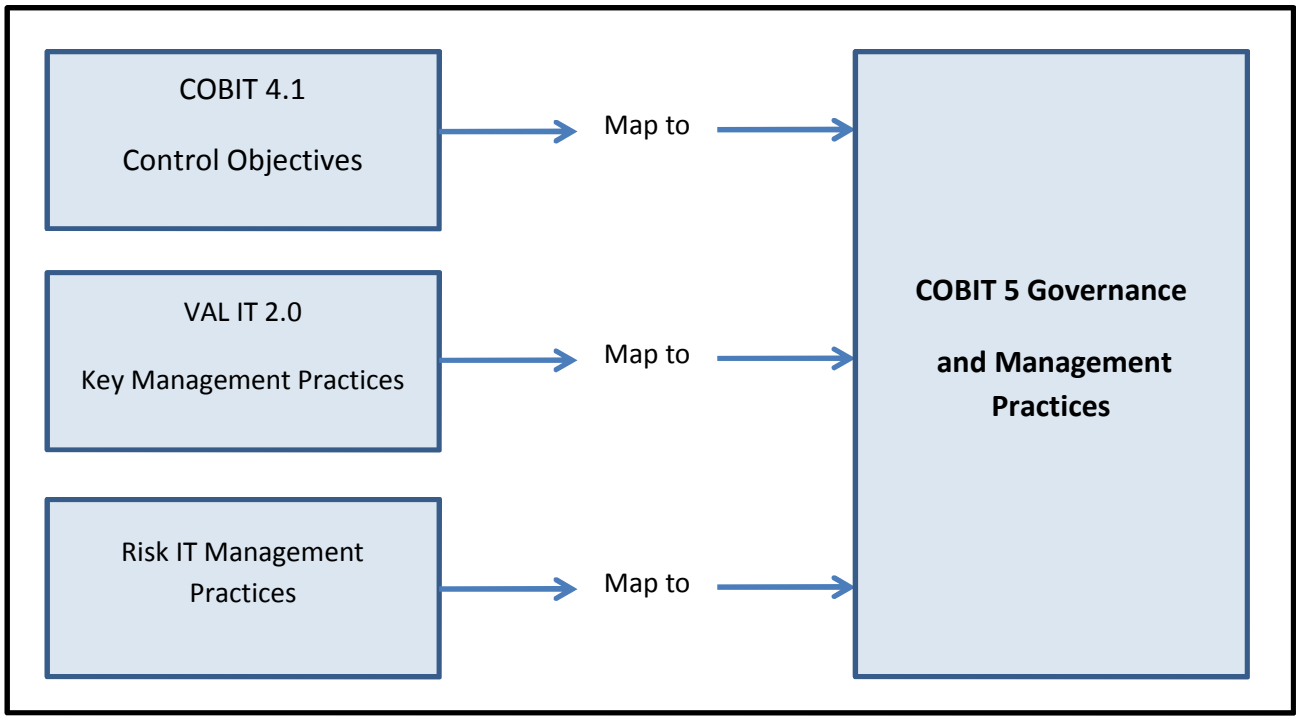


Source: Rob Johnson, 2012, Migrating to COBIT 5 for Auditors - ISACA COBIT 5 for Assurance, ISACA, 2nd Publication. USA.

- Cobit 5 is a foundational enterprise IT Governance framework, providing a basis to effectively integrate other complimentary frameworks, standards, and practices.
- As a single overarching framework it serves as a consistent and integrated source of guidance in non-technical, technology-agnostic, common language.
- Cobit 5 addresses the governance and management of information and related technology from enterprise-wide, end-to-end perspective, including the activities and responsibilities of both the functional and non-IT business functions.
- The end-to-end aspect is further supported by Cobit 5 coverage of all critical business elements[1].

COBIT 5 integrates a set related ISACA guidance (**COBIT 4.1**, **Val IT 2.0**, **Risk IT**) and aligns with the latest relevant other standards and frameworks, and thus provides the unique overarching framework.

Figure 2-2: ISACA Frameworks included in Cobit 5



Source : Indranil Mukherjee, 2013, CLOUD SECURITY THROUGH COBIT, ISO 27001 ISMS CONTROLS, ASSURANCE AND COMPLIANCE, International Standards Certification, Singapore, available on www.isc-worldwide.com

[1]Steven Hunt & Michael Nelson, 2012, Foundational IT Governance – A Foundational Framework for Governing Enterprise IT adapted from the "ISACA Cobit 5 framework". ISACA Publications. USA Page: 10

1-2-Mapping of COBIT 5 with the Most Relevant Related Standards and Frameworks:

COBIT 5 was developed taking into account a number of other standards and frameworks; this study includes a brief discussion of each framework or standard is included, indicating to which areas and domains in COBIT 5 it relates.

1-2-1-Improvements in COBIT:

Considerable improvements have been made to the COBIT framework to position it as a model for the corporate governance of information technology. Unlike its predecessor (COBIT 4.1) and ITIL® v3, the COBIT 5 framework addresses all three levels of an IT governance framework. Both COBIT 4.1 and ITIL® v3 are process models that describe IT practices at the operational level providing a useful source of good practices. However neither COBIT 4.1 or ITIL® v3 address the management practices necessary to marshal and use IT resources effectively and efficiently nor does COBIT 4.1 or ITIL® v3 describe the corporate governance processes essential for directing and controlling the use of IT.[2]

The improvements to COBIT 5 include restructuring the description of the individual processes, identifying the previous base practices within each process and describing the key activities within each base practice. The most significant change to COBIT is the reorganisation of the framework from being an IT process model into an IT governance framework with a set of governance practices for IT, a management system for the continuous improvement of IT activities and a process model with baseline practices.

1-2-2- Upgrading from COBIT 4.1 to COBIT 5:

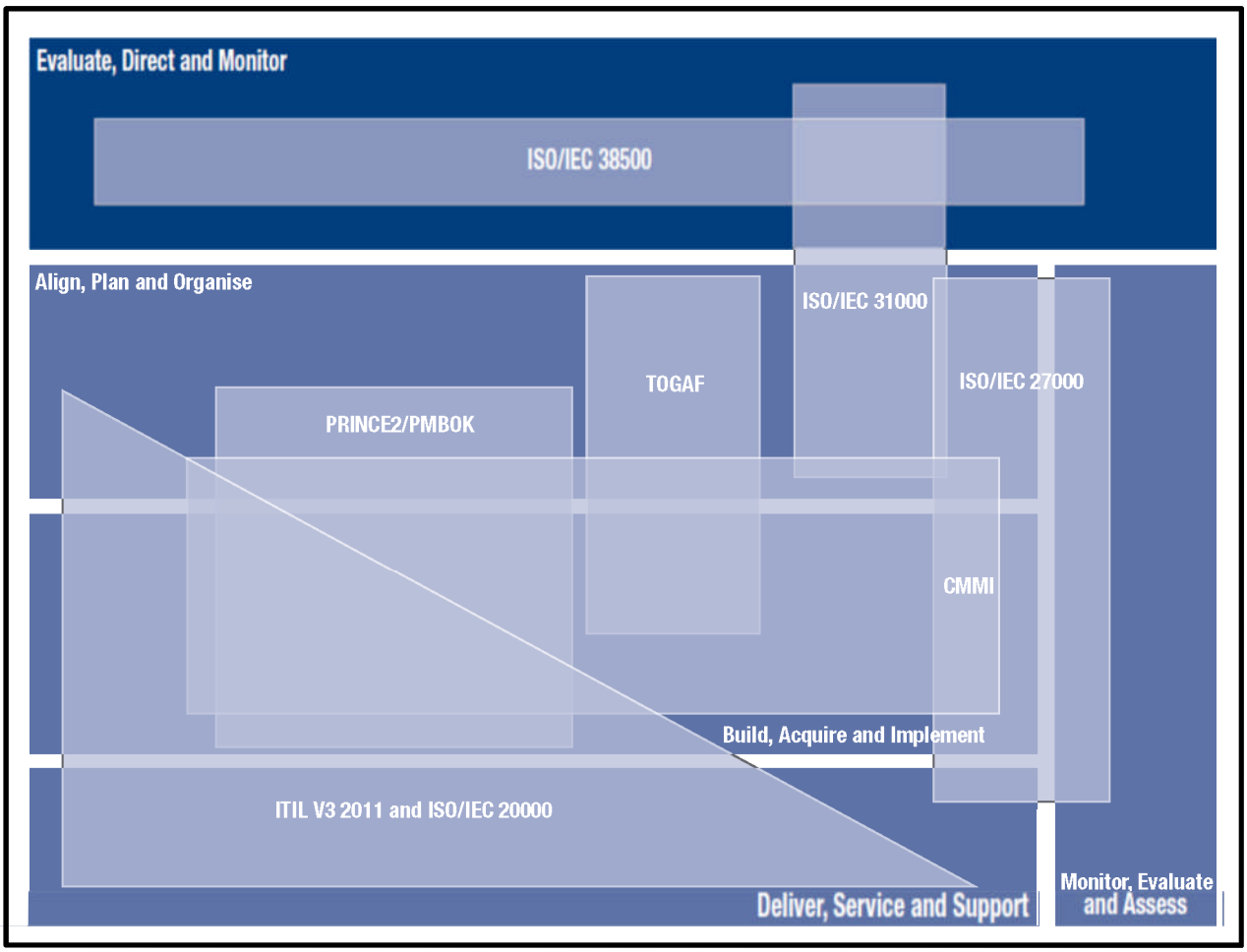
COBIT 5 builds on the process model previously defined in earlier releases of COBIT. It is an evolutionary change that has rationalised the previous processes through combining and reassigning practices within the existing processes and including additional processes and practices for the management and governance of information technology. Upgrading previous implementations of the COBIT process model required:

- Combining previous processes;
- Moving practices from one process to another;
- Adding additional operational processes and practices;
- Adding management processes and practices;
- Adding governance practices.[3]

[2] IT Governance Network, 2012, COBIT 5 Readiness, Published on www.itgovernance.com/COBIT 5 readiness, In 23/09/2012

[3] IT Governance Network, 2012, COBIT 5 Readiness, Published on www.itgovernance.com/COBIT 5 readiness, In 23/09/2012

Figure 2-3: COBIT 5 Coverage of Other Standards and Frameworks



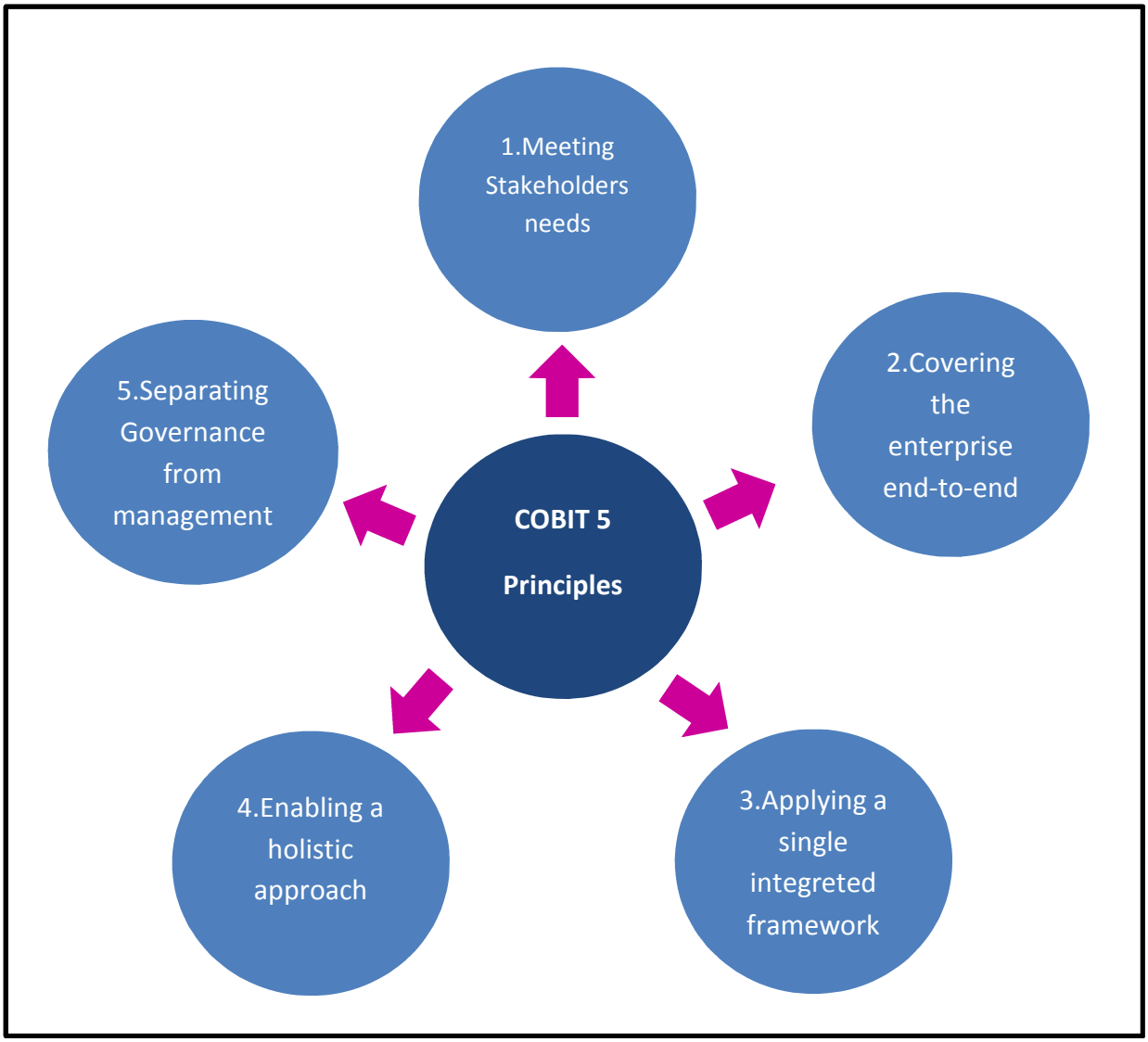
Source : John W. Lainhart et al. , 2012, COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT, ISACA, 1st Edition. USA.

1-3- Principles of Cobit 5:

Studies describe five principles for COBIT 5:

Principle 1: Meeting stakeholder needs
Principle 2: Covering the enterprise end-to-end
Principle 3: Applying a Single Integrated Framework
Principle 4: Enabling a holistic approach
Principle 5: Separating governance from management.

Figure 2-4 : COBIT 5 Principles

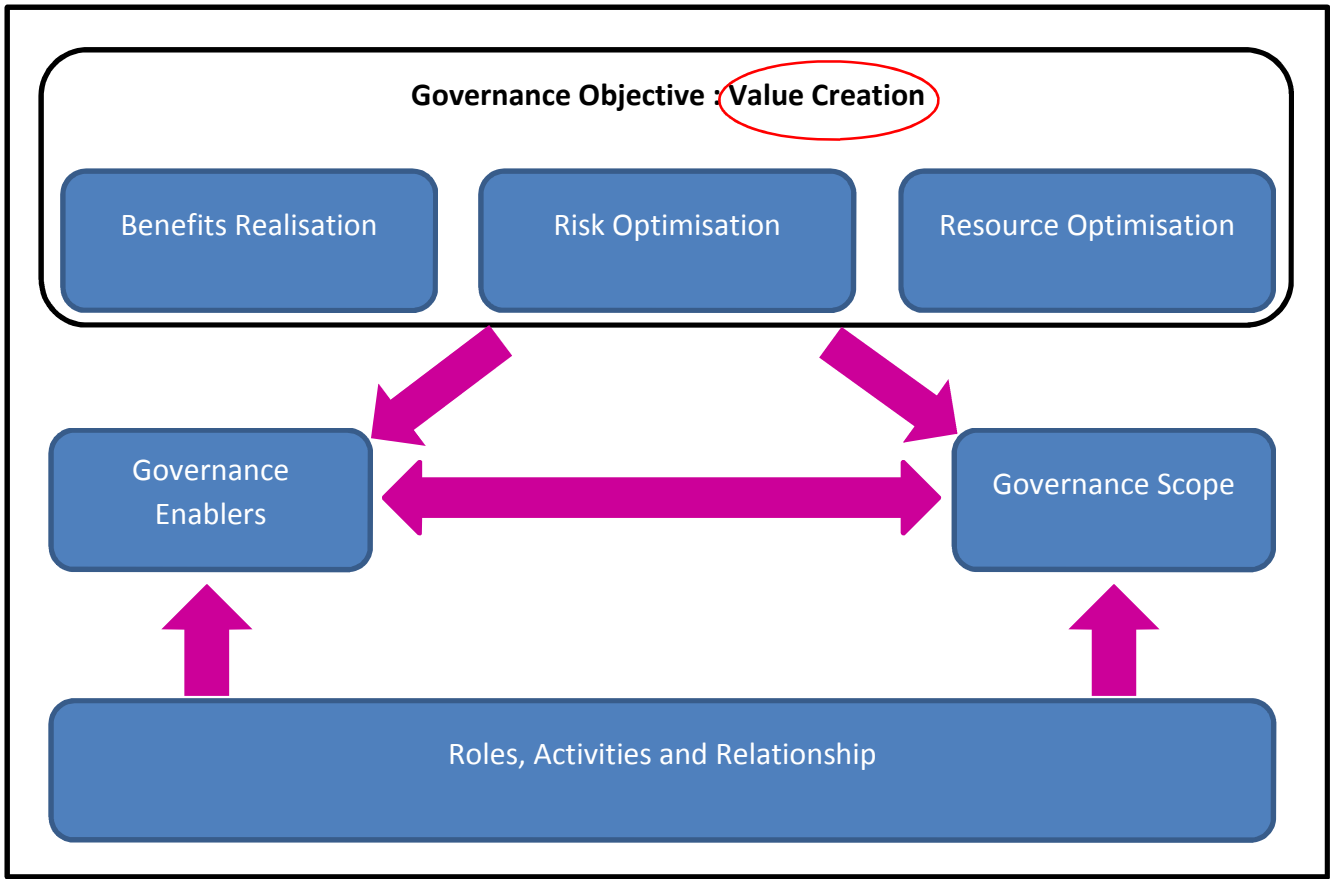


Source : Robert E Stroud, 2012, COBIT 5 :What is new and innovative and of Extreme Value!, ISACA, USA.

1-3-1- Principle 1: Meeting stakeholder needs:

Stakeholder needs are influenced by a number of drivers; **strategy changes**, **changing business (mission) and regulatory environment**, and **technology evolution**[4]. Enterprises exist to create value for their stakeholders by maintaining a balance between **the realization of benefits** and **the optimization of risk and use of resources**. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT[5].

Figure 2-5: Governance and Management in COBIT 5



Source : Robert E Stroud, 2012, COBIT 5 :What is new and innovative and of Extreme Value!, ISACA, USA.

[4] Steven Hunt & Michael Nelson, The previous reference, Page: 23.
[5] Indranil Mukherjee, 2013, ISC Pte Ltd, International Standards Certification – Asia Conference, Singapore, available on www.isc-worlwide.com, Page : 34

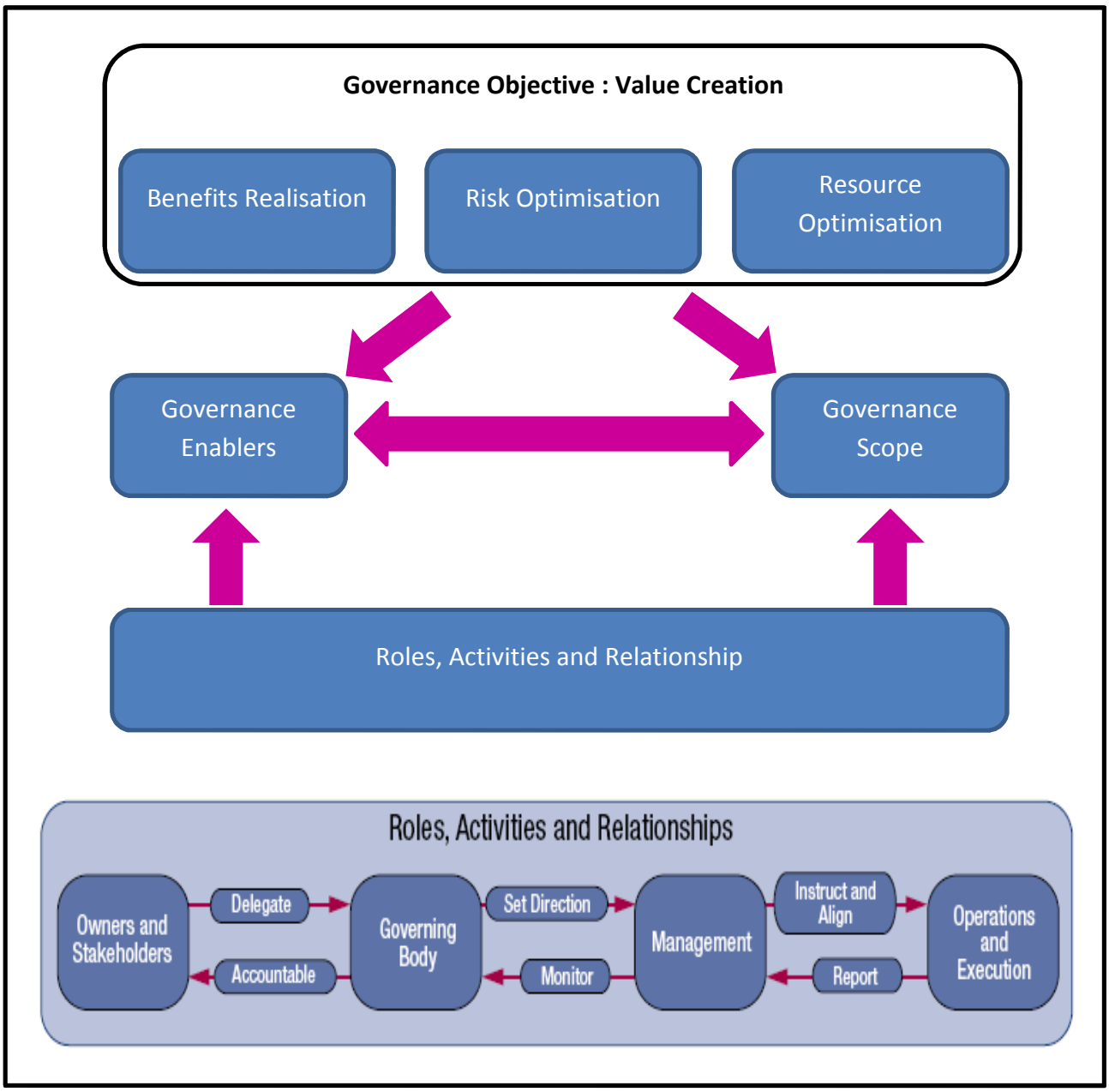
1-3-2- Principle 2: Covering the enterprise end-to-end

End-to-end coverage is achieved by identifying all stakeholder needs and determining how they link to governance and management decisions and activities. COBIT 5 addresses the governance and management of information and related technology from an enterprisewide, end-to-end perspective. This means that COBIT 5:

- Integrates governance of enterprise IT into enterprise governance, i.e., the governance system for enterprise IT proposed by COBIT 5 integrates seamlessly in any governance system because COBIT 5 aligns with the latest views on governance.
- Covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise[6].

[6] Steven Hunt & Michael Nelson, The previous reference, Page: 26

Figure 2-6: Key Components of a Governance System



Source : Mike O. Villegas, 2012, COBIT 5 Update FEI/CFIT Meeting, ISACA. USA

1-3-3- Principle 3: Applying a Single Integrated Framework:

COBIT 5 integrates the previous ISACA guidance on governance and management of enterprise IT, it aligns with the latest relevant other standards and frameworks used by enterprises:

- Enterprise: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
- IT-related: ISO/IEC 38500, ITIL, ISO/IEC 27000 series, TOGAF, PMBOK/PRINCE2, CMMI[7]

This allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator. ISACA plans a capability to facilitate COBIT user mapping of practices and activities to third-party references[8].

1-3-4- Principle 4: Enabling a holistic approach:

Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise[9].

1-3-5- Principle 5 : Separating governance from management:

The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines Encompass different types of activities, require different organisational structures, and serve different purposes[10].

Governance: In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson[11]. Firstly, it ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions and options. Secondly, it sets **direction** through prioritization and decision making. Thirdly, it **monitors** performance, compliance, and progress against the agreed upon direction and objectives[12].

Management: In most enterprises, management is the responsibility of the executive management under the leadership of the CEO[13]. It **plans**, **builds**, **runs**, and **monitors** activities in alignment with direction set by the governance body to achieve enterprise objectives[14].

---

[7] Steven Hunt & Michael Nelson, The previous reference, Page: 50
[8] Mike O. Villegas, 2012, COBIT 5 Update FEI/CFIT Meeting, ISACA. USA, Page: 23
[9] Steven Hunt & Michael Nelson, The previous reference, Page: 53
[10] Mike O. Villegas, The previous reference, Page: 29
[11] Mike O. Villegas, The previous reference, Page: 29
[12] Steven Hunt & Michael Nelson, The previous reference, Page: 69
[13] Mike O. Villegas, The previous reference, Page: 29
[14] Steven Hunt & Michael Nelson, The previous reference, Page: 69

II. COBIT 5 Fundamental Structures and Processes

2-1- Goals Cascade:

Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the **goals cascade (Figure 2-7)**, translating high-level enterprise goals into manageable, specific, **IT-related goals** and mapping these to **specific processes and practices**[15]. More precisely, goals cascade provides the link between stakeholder needs and practical goals by translating these into increasing levels of detail and specificity: drivers, stakeholder needs, enterprise goals, IT related goals, and enabler goals. Furthermore, it allows setting specific goals at every level of the enterprise in support of the overall goals and stakeholders requirements[16] (**Table 2-1** and **Table 2-2**).

As a provider to its stakeholders enterprise needs to remember that its goals are a proxy for stakeholder needs. From a stakeholders' point of view it is valuable to understand how their needs relate to enterprise and IT-related goals[17] .

[15] Ernst & Young, 2013, A globally accepted business framework for the governance and management of enterprise IT, EYGM Limited, United Kingdom, available on www.ey.com, Page: 44
[16] Steven Hunt & Michael Nelson, The previous reference, Page: 24
[17] Steven Hunt & Michael Nelson, The previous reference, Page: 27

Figure 2-7 : Goals Cascade

Step 1. **Stakeholder Drivers** influence Stakeholder Needs.

- **Drivers:** Strategy changes, a changing business and regulatory environment, and new technologies.

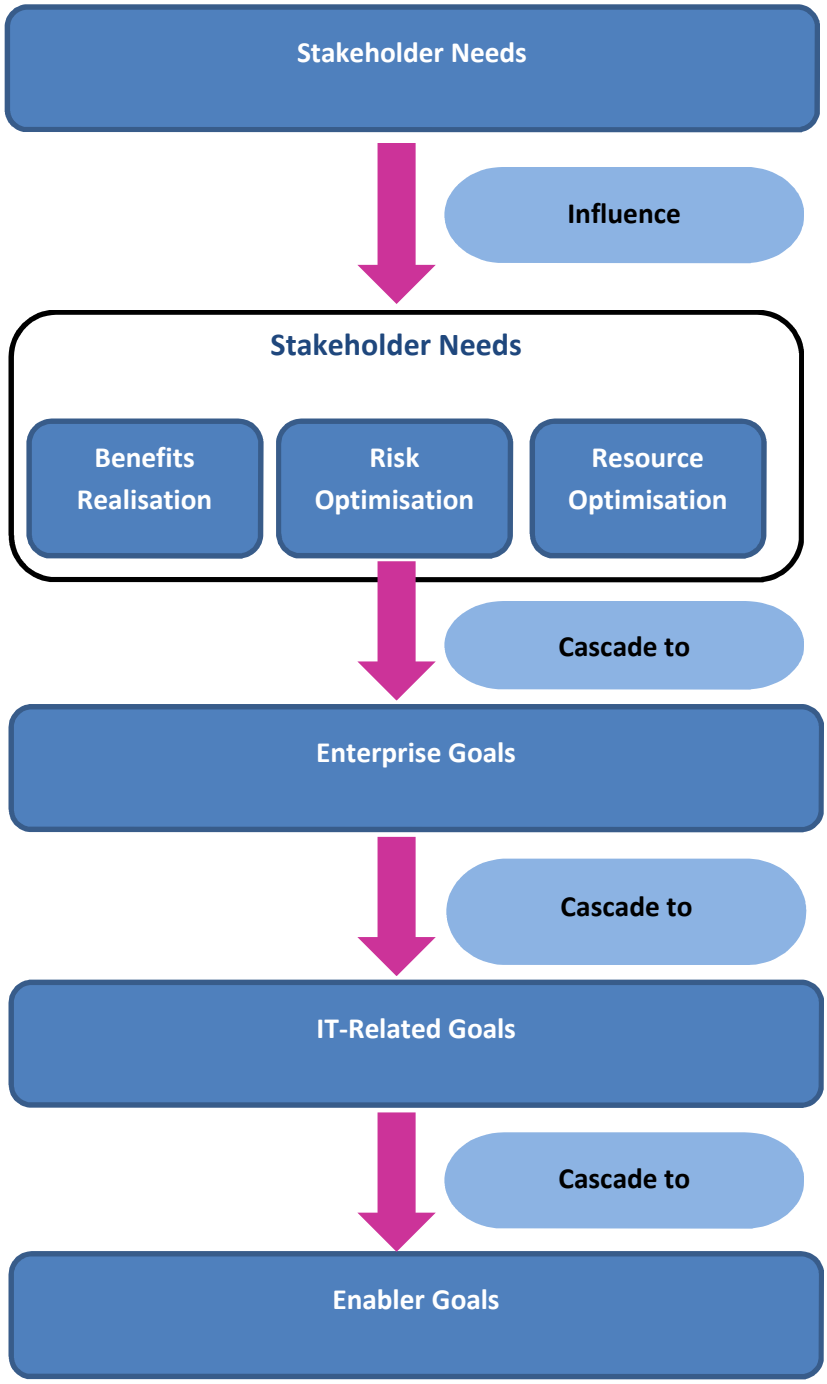
Step 2. **Stakeholder Needs** cascade to Enterprise Goals.

- These Enterprise Goals have been developed using the Balanced Scorecard (BSC) dimensions.

Step 3. **Enterprise Goals** cascade to IT-related Goals.

- IT-related stands for information and related technology, and IT-related Goals are structured along the dimensions of IT Balanced Scorecard (IT BSC). COBIT 5 defines 17 IT-related Goals.

Step 4. **IT-related Goals** cascade to Enabler Goals



Source: Steven Hunt & Michael Nelson, 2012, Foundational IT Governance – A Foundational Framework for Governing Enterprise IT adapted from the "ISACA Cobit 5 framework", available on www.isaca.org

Table 2-1: COBIT 5 Enterprise Goals

BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1.Stakeholder value of business investments	P		
	2.Portfolio of competitive products and services	P		S
	3.Managed business risks		P	S
	4.Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6.Customer oriented service culture	P		S
	7.Business service continuity and availability		P	
	8.Agile responses to changing environment	P		S
	9.Information based strategic decision making	P	P	P
	10.Optimisation of service delivery costs	P		S
Internal	11.Optimisation of business process functionality	P		P
	12.Optimisation of business process costs	P		P
	13.Managed business process changes	P	P	S
	14.Operational and staff productivity	P		P
	15.Compliance with internal policies		P	
Learning and Growth	16.Skilled and motivated people	S	S	P
	17.Product and business innovation culture	P		

BSC: Balanced Scorecard
P: Primary
S: Secondary

Source: Patrick Soenen, 2012, COBIT 5 Framework, The Institute of Internal Auditors, Belgium, Available on www.qualified-audit-partners.be

Table 2-2: COBIT 5 IT-related Goals

IT BSC Dimension	Description
Financial	1. Alignment of IT and business strategy
	2. IT compliance and support for business compliance with external laws and regulations
	3. Commitment of executive management for making IT related decisions
	4. Managed IT related business risks
	5. Realised benefits form IT-enabled investments and services portfolio
	6. Transparency of IT costs, benefits and risks
Customer	7. Delivery of IT services in line with business requirements
	8. Adequate use of applications, information and technology structure
Internal	9. IT agility
	10. Security of information, processing infrastructure and applications
	11. Optimisation of IT assets, resources and capabilities
	12. Enablement and support of business processes by integration
	13. Delivery of programme on time, on budget, and on business requirements
	14. Availability of reliable and useful information
	15. IT compliance with internal policies
Learning and Growth	16. Competent and motivated IT personnel
	17. Knowledge, expertise and initiatives of business motivation

Source: Patrick Soenen, 2012, COBIT 5 Framework, The Institute of Internal Auditors, Belgium, Available on www.qualified-audit-partners.be

Table 2-3: Stakeholder Needs

Internal Stakeholders	Internal Stakeholder Questions
• Board • CEO • Chief Financial Officer (CFO) • CIO • Chief Risk Officer • Business executives • Business process owners • Business managers • Risk managers • Security managers • Service managers • Human Resource (HR) managers • Internal audit • Privacy officers • IT users • IT managers • Etc.	How do I get value from use of IT? Are end users satisfied with the quality of IT service? How do I manage performance of IT? How can I best exploit new technology for new strategic opportunities? How do I best build and structure my IT department? How dependent am I on external providers? How well are IT outsourcing agreements being managed? How do I obtain assurance over external providers? What are the (control) requirements for information? Did I address all IT-related risk? Am I running an efficient and resilient IT operation? How do I control the cost of IT? How do I use IT resources in the most effective and efficient manner? What are the most effective and efficient sourcing options? Do I have enough people for IT? How do I develop and maintain their skills, and how do I manage their performance? How do I get assurance over IT? Is the information I am processing well secured? How do I improve business agility through a more flexible IT environment? Do IT projects fail to deliver what they promised—and if so, why? Is IT standing in the way of executing the business strategy? How critical is IT to sustaining the enterprise? What do I do if IT is not available? What concrete vital primary business processes are dependent on IT, and what are the requirements of business processes? What has been the average overrun of the IT operational budgets? How often and how much do IT projects go over budget? How much of the IT effort goes to fighting fires rather than to enabling business improvements? Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives? How long does it take to make major IT decisions? Are the total IT effort and investments transparent? Does FT support the enterprise in complying with regulations and service levels? How do I know whether I am compliant with all applicable regulations?
External Stakeholders	**External Stakeholder Questions?**
• Business partners • Suppliers • Shareholders • Regulators/government • External users • Customers • Standardisation organisations • External auditors • Consultants • Etc.	How do I know my business partner's operations are secure and reliable? How do I know the enterprise is compliant with applicable rules and regulations? How do I know the enterprise is maintaining an effective system of internal control? Do business partners have the information chain between them under control?

Source: Steven Hunt & Michael Nelson, 2012, Foundational IT Governance – A Foundational Framework for Governing Enterprise IT adapted from the "ISACA Cobit 5 framework", available on www.isaca.org

2-2- COBIT 5 Enablers:

Enablers are tangible and intangible elements that make governance and management over enterprise IT work. The enablers are driven by the goal cascade[18]. The COBIT 5 framework defines seven categories of enablers:

1. Principles, policies and frameworks — Are the vehicle to translate the desired behavior into practical guidance for day-to-day management.

2. Processes — Describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT related goals.

3. Organisational structures — Are the key decision-making entities in an organisation

4. Culture, ethics and behaviour — Of individuals and of the organisation; very often underestimated as a success factor in governance and management activities.

5. Information — Is pervasive throughout any organisation, i.e., deals with all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, information is very often the key product of the enterprise itself.

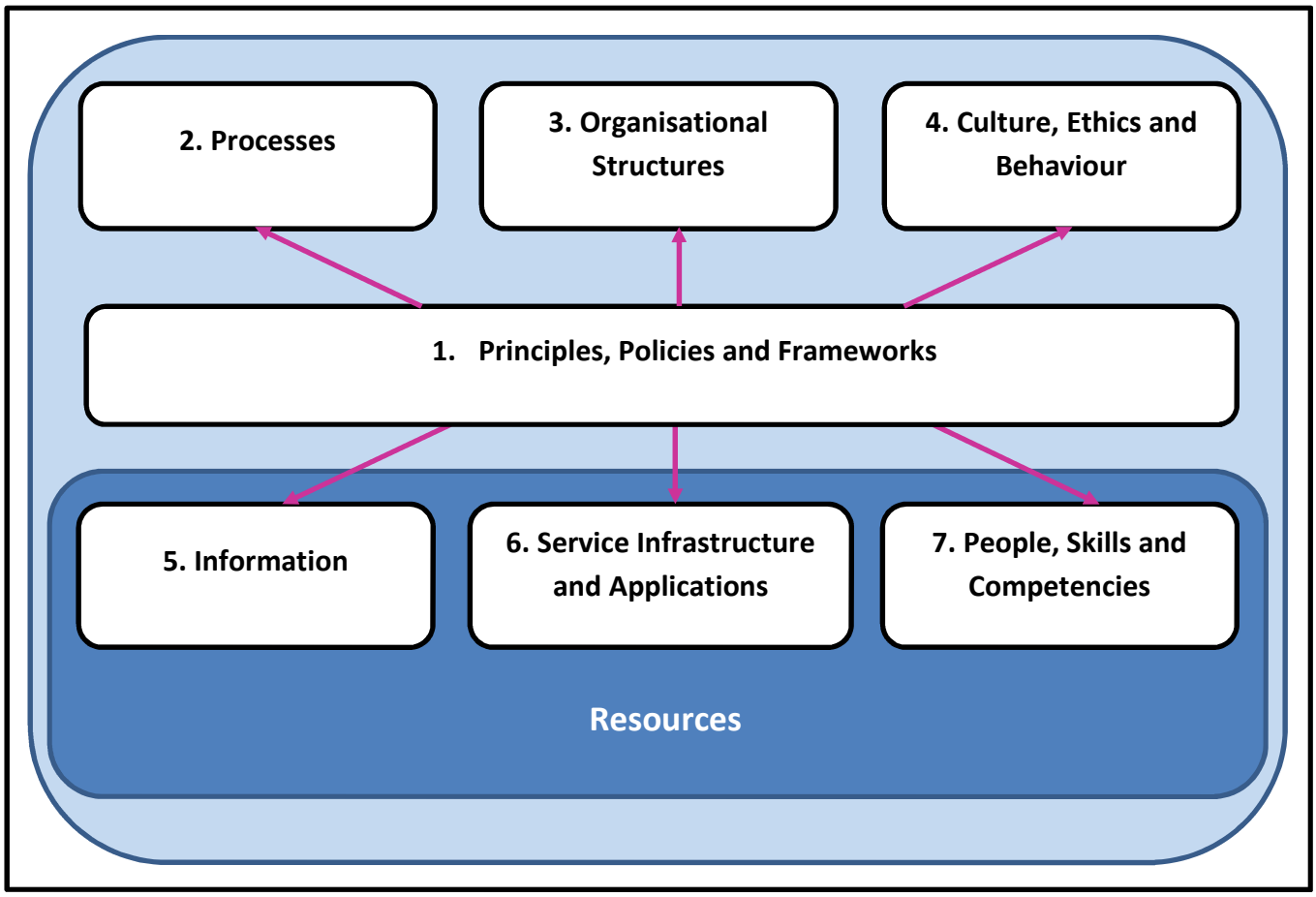
6. Services, infrastructure and applications — Include the infrastructure, technology and applications that provide the enterprise with information technology processing and services

7. People, skills and competencies— Are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions[19].

[18] Patrick Soenen, 2012, COBIT 5 Framework, The Institute of Internal Auditors, Belgium, Available on www.qualified-audit-partners.be, Page: 17

[19] M. Garsoux, 2012, COBIT 5 ISACA's new framework for IT Governance, Risk, Security and Auditing, An overview, ISACA, 1st Edition, United Kingdom, Page: 23

Figure 2-8: COBIT 5 Enablers



Source: Steven Hunt & Michael Nelson, 2012, Foundational IT Governance – A Foundational Framework for Governing Enterprise IT adapted from the "ISACA Cobit 5 framework", available on www.isaca.org

2-2-1-Dimensions of COBIT 5 Enablers:

A governance system is a complex interaction amongst all enablers. Having a simple, structured, and uniform way to analyze each enabler can facilitate adoption and successful integration. Enablers all have certain elements in common therefore a generic model standardizes conceptualization[20]. The four common dimensions for enablers are:

● Stakeholders:

Each enabler has stakeholders, i.e., parties who play an active role and/or have an interest in the enabler. For example, processes have different parties who execute process activities and/or who have an interest in the process outcomes; organisational structures have stakeholders—each with his/her own roles and interests—that are part of the structures. Stakeholders can be internal or external to the enterprise, all having their own, sometimes conflicting, interests and needs. Stakeholders' needs translate to enterprise goals, which in turn translate to IT-related goals for the enterprise.[21]

● Goals:

Each enabler has a number of goals, and enablers provide value by the achievement of these goals. Goals can be defined in terms of:
– Expected outcomes of the enabler
– Application or operation of the enabler itself

The enabler goals are the final step in the COBIT 5 goals cascade. Goals can be further split up in different categories such as:
– **Intrinsic quality**—The extent to which enablers work accurately, objectively and provide accurate, objective and reputable results
– **Contextual quality**—The extent to which enablers and their outcomes are fit for the purpose, given the context in which they operate.
– **Access and security**—The extent to which enablers and their outcomes are accessible and secured:
• Enablers are available when, and if, needed.
• Outcomes are secured, i.e., access is restricted to those entitled to and needing it.[22]

● Lifecycle:

Each enabler has a life cycle, from inception through an operational/useful life until disposal. This applies to information, structures, processes, policies, etc. The phases of the life cycle consist of:
– Plan (which includes concepts development and concepts selection)
– Design
– Build/acquire/create/implement

[20] Steven Hunt & Michael Nelson, The previous reference, Page: 55
[21] Steven Hunt & Michael Nelson, The previous reference, Page: 55
[22] Steven Hunt & Michael Nelson, The previous reference, Page: 56

– Use/operate

– Evaluate/monitor

– Update/dispose

● **Good Practices:**

For each of the enablers, good practices can be defined. Good practices support the achievement of the enabler goals. Good practices provide examples or suggestions on how best to implement the enabler, and what work products or inputs and outputs are required[23].

2-2-2-Enabler Performance Management:

To manage performance of enablers, metrics associated with the following enabler dimensions must be developed, implemented, and monitored:

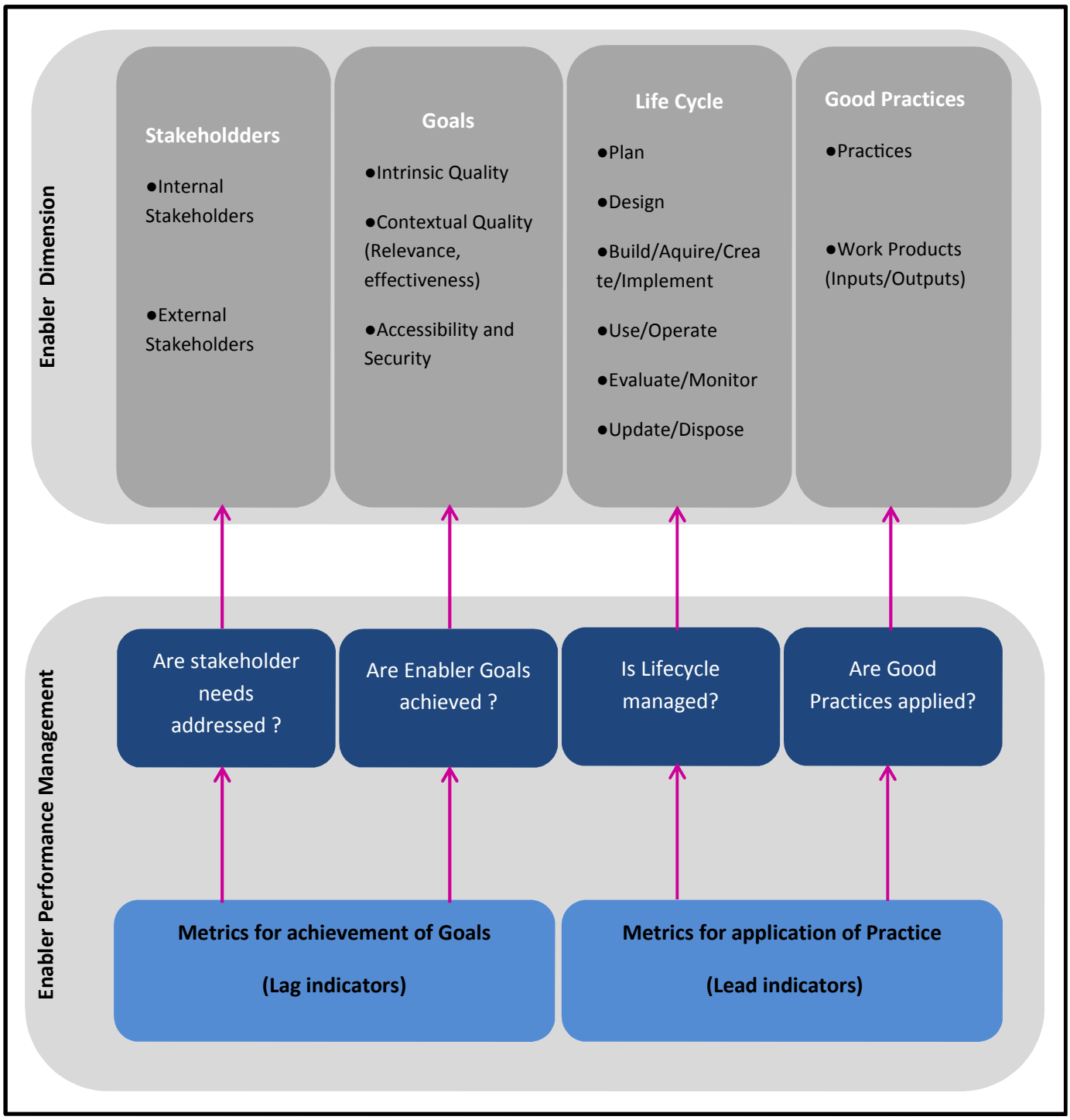
- **Stakeholders:** Are stakeholder needs addressed?
- **Goals:** Are enabler goals achieved?
- **Lifecycle:** Is the enabler lifecycle managed?
- **Good Practices:** Are good practices applied?

The first two bullets deal with the actual outcome of the enabler. The metrics used to measure to what extent the goals are achieved can be called 'lag indicators'. The last two bullets deal with the actual functioning of the enabler itself, and metrics for this can be called 'lead indicators'[24].

[23] John W. Lainhart et al. , 2012, COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT. ISACA. 1st Edition. USA. Page:65

[24] John W. Lainhart et al., The previous reference, Page : 66

Figure 2-9: Generic Enabler Model

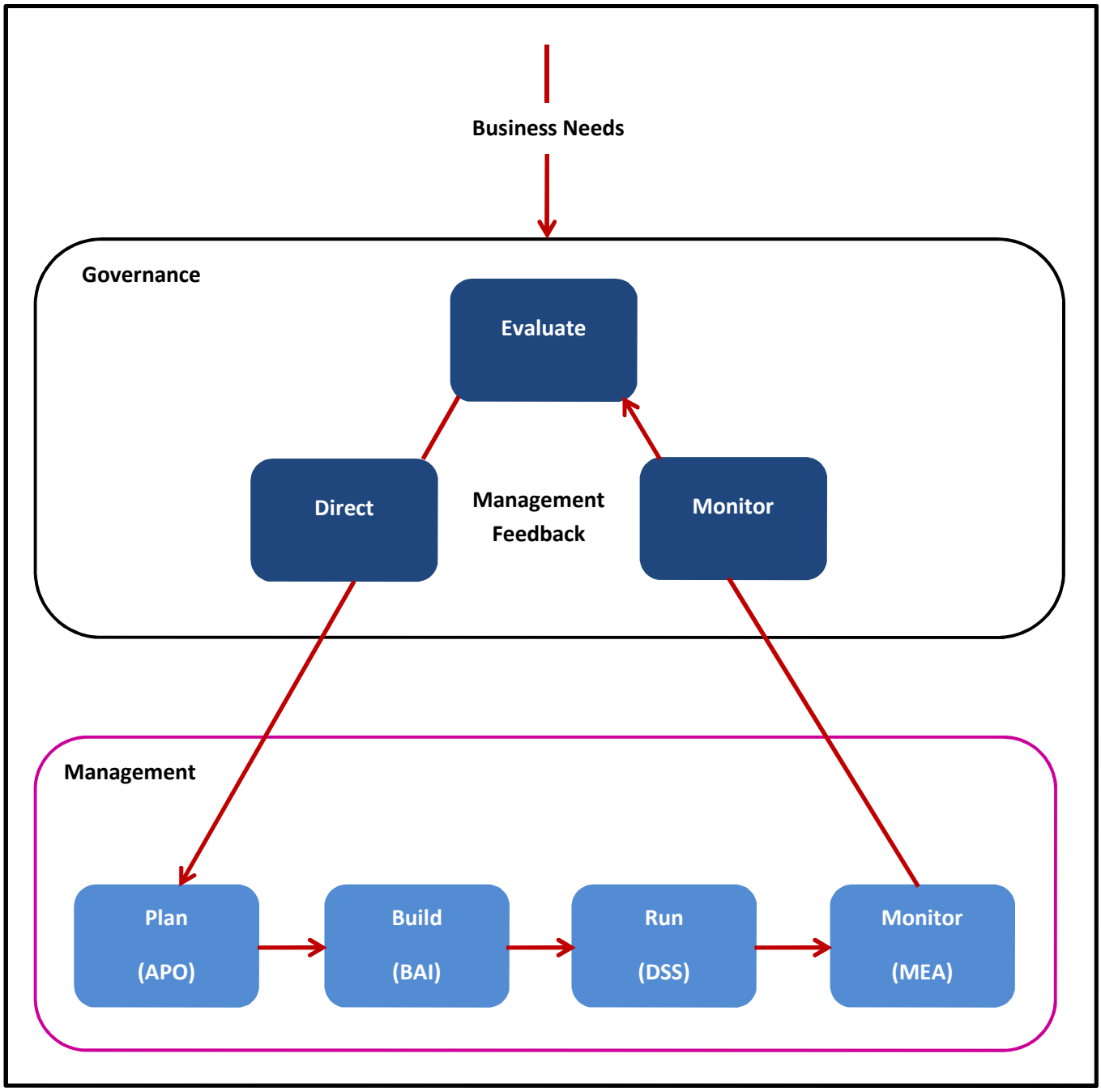


Source : Steven Hunt & Michael Nelson, 2012, Foundational IT Governance – A Foundational Framework for Governing Enterprise IT adapted from the "ISACA Cobit 5 framework", available on www.isaca.org

2-3- COBIT 5 Process Reference Model:

COBIT 5 is not prescriptive, but it advocates that enterprises implement governance and management processes such that the key areas are covered, as shown in **figure 2-11**.

Figure 2-10: COBIT 5 Governance and Management Key Areas



Source: John W. Lainhart et al. , 2012, COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT. ISACA. 1st Edition. USA.

An enterprise can organise its processes as it sees fit, as long as all necessary governance and management objectives are covered. COBIT 5 includes a process reference model, which defines and describes in detail a number of governance and management processes. It represents all of the processes normally found in an enterprise relating to IT activities, providing a common reference model understandable to operational IT and business managers. The proposed process model is a complete, comprehensive model, but it is not the only possible process model. Each enterprise must define its own process set, taking into account its specific situation. The COBIT 5 process reference model divides the governance and management processes of enterprise IT into two main process domains:

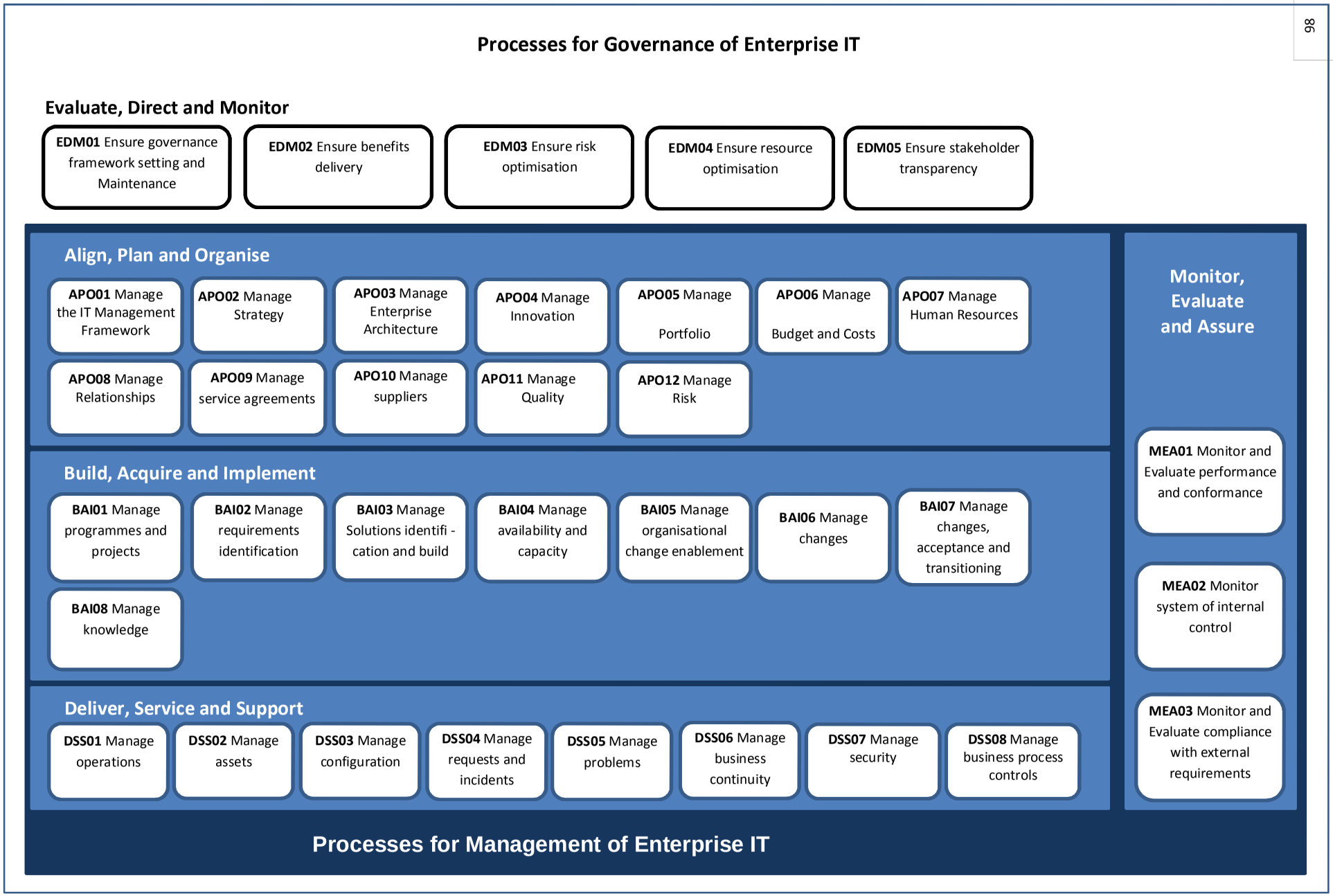
• **Governance**—Contains five governance processes; within each process, Evaluate, Direct and Monitor (**EDM**) practices are defined.

• **Management**—Contains four domains, in line with the responsibility areas of Plan, Build, Run and Monitor (**PBRM**), and provides end-to-end coverage of IT. The names of the domains are chosen in line with these main area designations, but contain more verbs to describe them:
– Align, Plan and Organise (APO)
– Build, Acquire and Implement (BAI)
– Deliver, Service and Support (DSS)
– Monitor, Evaluate and Assess (MEA)[25]

Figure 2-11 shows the complete set of 37 governance and management processes within COBIT 5.

[25] John W. Lainhart et al., The previous reference, Page : 32

Figure 2-11 : COBIT 5 Process Reference Model



Source : John W. Lainhart et al. , John W. Lainhart et al. , 2012, COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT. ISACA. 1st Edition. USA.

The details of all processes, according to the process model described previously are described as follows:

2-3-1- Domain 01: Evaluate, Direct and Monitor (EDM):

- **EDM01**: **Ensure Governance Framework Setting and Maintenance:** Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.[26]
- **EDM02: Ensure Benefits Delivery:** Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from IT-enabled investments at an acceptable cost.[27]
- **EDM03: Ensure Risk Optimisation:** Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and risks to enterprise value related to the use of IT are identified and managed.[28]
- **EDM04: Ensure Resource Optimisation:** Ensure that adequate and sufficient IT-related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost.[29]
- **EDM05: Ensure Stakeholder Transparency:** Ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions.[30]

2-3-2- Domain 02: Align, Plan and Organise (APO):

- **APO01: Manage the IT Management Framework:** Clarify and maintain the enterprise IT mission and vision. Ensure that the right mechanisms and authorities are put in place, in line with guiding principles and policies, and are continually improved and aligned with enterprise requirements.[31]
- **APO02: Manage Strategy:** Provide a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment, leveraging enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives.[32]
- **APO03: Manage Enterprise Architecture:** Establish a common framework consisting of business process, information, data, application and technology architecture layers for effectively and efficiently realising enterprise and IT strategies by creating key models and practices that describe the baseline and target architectures. Define

[26] Floris Ampe et al. 2012. COBIT 5: Process Reference Guide Exposure Draft. ISACA Publications. UK. Page: 18
[27] Floris Ampe et al. The previous reference : Page : 23
[28] Floris Ampe et al. The previous reference : Page : 27
[29] Floris Ampe et al. The previous reference : Page : 31
[30] Floris Ampe et al. The previous reference : Page : 34
[31] Floris Ampe et al. The previous reference : Page : 37
[32] Floris Ampe et al. The previous reference : Page : 44

requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as re-use of building block components.[33]

- **APO04: Manage Innovation:** Maintain an awareness of information technology and related service trends, identify innovation opportunities, and plan how to benefit from innovation in relation to business needs. Analyse what opportunities for business innovation or improvement can be created by emerging technologies, services or IT-enabled business innovation, as well as through existing established technologies and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions.[34]
- **APO05: Manage Portfolio:** Execute the strategic direction set for investments in line with the enterprise architecture vision, and the desired characteristics of the investment portfolio, and consider the different categories of investments and the resources and funding constraints. Evaluate, prioritise and balance programmes within resource and funding constraints, based on their alignment with strategic objectives, enterprise worth and risk, and move selected programmes into the active portfolio for execution. Monitor the performance of the overall portfolio, proposing adjustments to it as necessary in response to programme performance or changing enterprise priorities.[35]
- **APO06: Manage Budget and Cost:** Manage the IT-related financial activities in both the business and IT functions, covering budgeting, cost and benefit management, and prioritisation of spending through the use of formal budgeting practices and a fair and equitable system of allocating costs to the enterprise. Consult stakeholders to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed.[36]
- **APO07: Manage Human Resources:** Provide a structured approach to ensure optimal structuring, placement, decision rights and skills of human resources. This includes communicating the defined roles and responsibilities, learning and growth plans, and performance expectations, supported with competent and motivated people.[37]
- **APO08 Manage Relationships:** Manage the relationship between the business and IT in a formalised and transparent way that ensures a focus on achieving a common and shared goal of successful enterprise outcomes in support of strategic goals and within the constraint of budgets and risk tolerance. The relationship should be based on mutual trust, using open and understandable terms and common language and a willingness to take ownership and accountability for key decisions.[38]

[33] Floris Ampe et al. The previous reference : Page : 50
[34] Floris Ampe et al. The previous reference : Page : 57
[35] Floris Ampe et al. The previous reference : Page : 62
[36] Floris Ampe et al. The previous reference : Page : 67
[37] Floris Ampe et al. The previous reference : Page : 72
[38] Floris Ampe et al. The previous reference : Page : 77

- **APO09 Manage Service Agreements:** Align IT-enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators.[39]
- **APO10: Manage Suppliers:** Ensure that IT-related services provided by all types of suppliers meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance.[40]
- **APO11: Manage Quality:** Define and communicate quality requirements in all processes, procedures and the related enterprise outcomes, including controls, ongoing monitoring and the use of proven practices and standards in continuous improvement and efficiency efforts.[41]
- **APO12: Manage Risk**: Continually identify, assess and reduce IT-related risks within levels of tolerance set by enterprise executive management.[42]

2-3-3- Domain 03: Build, Acquire & Implement (BAI):

- **BAI01: Manage Programmes and Projects:** Manage all programmes and projects from the investment portfolio in a co-ordinated way. Initiate, plan, control, and execute programmes and projects, and close with a post-implementation review.[43]
- **BAI02: Manage Requirements Definitions:** Identify solutions and analyse requirements before acquisition or creation to ensure that they are in line with enterprise requirements covering business processes, applications, information/data, infrastructure and services. Review feasible options including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.[44]
- **BAI03: Manage Solutions Identification and Build:** Establish and maintain identified solutions in line with enterprise requirements covering design, development, procurement/sourcing, configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.[45]
- **BAI04: Manage Availability and Capacity:** Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.[46]

[39] Floris Ampe et al. The previous reference : Page : 83
[40] Floris Ampe et al. The previous reference : Page : 88
[41] Floris Ampe et al. The previous reference : Page : 93
[42] Floris Ampe et al. The previous reference : Page : 99
[43] Floris Ampe et al. The previous reference : Page : 105
[44] Floris Ampe et al. The previous reference : Page : 115
[45] Floris Ampe et al. The previous reference : Page : 120
[46] Floris Ampe et al. The previous reference : Page : 127

- **BAI05: Manage Organisational Change Enablement:** Maximise the likelihood of successfully implementing sustainable enterprisewide organisational change quickly and with reduced risk covering the complete life cycle of the change and all affected stakeholders in the business and IT.[47]
- **BAI06: Manage Changes:** Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation.[48]
- **BAI07: Manage Changes, Acceptance and Transitioning:** Formally accept and make operational new solutions, including implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and IT services, early production support, and a post-implementation review.[49]
- **BAI08: Manage Knowledge:** Ensure that relevant knowledge is available, current, validated and reliable to facilitate decision making, and plan for the identification, gathering, organising, maintaining, use and retirement of knowledge.[50]

2-3-4- Domain 04: Deliver, Service & Support (DSS):

- **DSS01: Manage Operations:** Co-ordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services, including the execution of pre-defined standard operating procedures and the required monitoring activities.[51]
- **DSS02: Manage Assets:** Account for all IT assets and optimise the value provided by these assets.
- **DSS03: Manage Configuration:** Provide sufficient information about service assets to enable the service to be effectively managed, to assess the impact of changes and to deal with service incidents.
- **DSS04: Manage Service Requests and Incidents:** Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose) they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available. Manage software licences to ensure that the optimum number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements[52]

[47] Floris Ampe et al. The previous reference : Page : 131
[48] Floris Ampe et al. The previous reference : Page : 137
[49] Floris Ampe et al. The previous reference : Page : 142
[50] Floris Ampe et al. The previous reference : Page : 148
[51] Floris Ampe et al. The previous reference : Page : 152
[52] Floris Ampe et al. The previous reference : Page : 153

- **DSS05 Manage Problems:** Increase availability, improve service levels, reduce costs, and improve customer convenience and satisfaction, by reducing the number of operational problems.
- **DSS06: Manage Business Continuity:** Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption.
- **DSS07: Manage Security:** Improve the services' security level by Keeping the impact and occurrence of information security incidents within the enterprise's risk appetite levels.[53]
- **DSS08: Manage Business Process Controls:** Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements and manage and operate adequate controls to ensure that information and information processing satisfy these requirements.[54]

2-3-5- Domain 05: Monitor, Evaluate and Assure (MEA):

- **MEA01: Monitor and Evaluate Performance and Conformance**: Collect, validate and evaluate business, IT and process goals and metrics. Monitor that processes are performing against agreed performance and conformance goals and metrics and provide reporting that is systematic and timely.[55]
- **MEA02: Monitor System of Internal Control:** Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. Enable management to identify management deficiencies and inefficiencies and to initiate improvement actions. Plan, organise and maintain standards for internal control assessment and assurance activities.[56]
- **MEA03: Monitor and Evaluate Compliance with External Requirements:** Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with and integrate IT compliance with overall enterprise compliance.[57]

[53] Alpaslan Menevse, 2012, Toward Better IT Governance With COBIT 5, ISACA - COBIT FOCUS. 1st Edition. USA, Page: 52
[54] Floris Ampe et al. The previous reference : Page : 185
[55] Floris Ampe et al. The previous reference : Page : 190
[56] Floris Ampe et al. The previous reference : Page : 196
[57] Floris Ampe et al. The previous reference : Page : 201

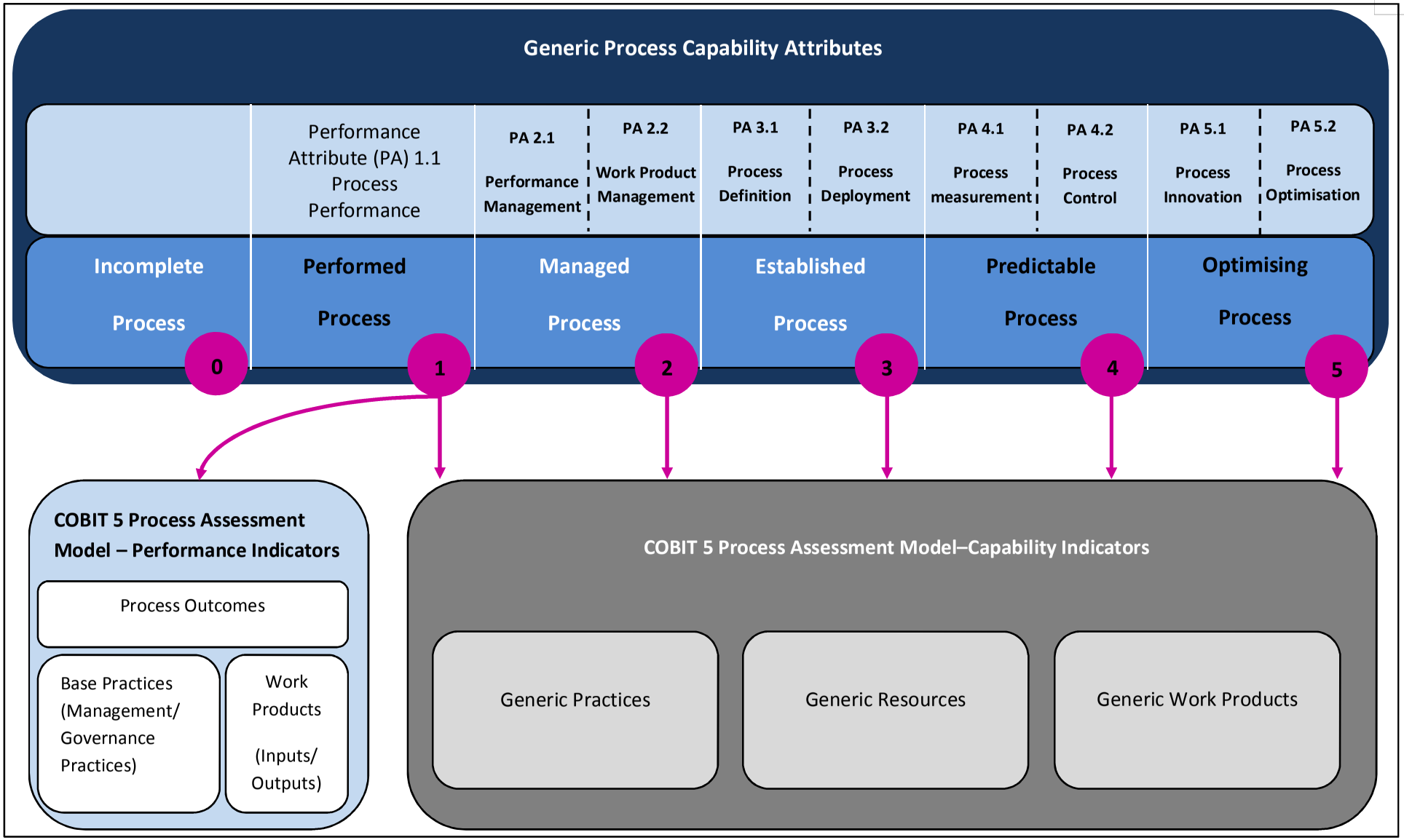
2-4- COBIT 5 Process Capability Model:

The COBIT 5 product set includes a process capability model, based on the internationally recognised ISO/IEC 15504 Software Engineering—Process Assessment standard. This model will achieve the same overall objectives of process assessment and process improvement support, i.e., it will provide a means to measure the performance of any of the governance (EDM-based) processes or management (PBRM-based) processes, and will allow areas for improvement to be identified (**Figure 2-12**). There are six levels of capability that a process can achieve, including an 'incomplete process' designation if the practices in it do not achieve the intended purpose of the process:

- **0 Incomplete process**—The process is not implemented or fails to achieve its process purpose. At this level, there is little or no evidence of any systematic achievement of the process purpose.
- **1 Performed process** (one attribute)—The implemented process achieves its process purpose.
- **2 Managed process** (two attributes)—The previously described performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
- **3 Established process** (two attributes)—The previously described managed process is now implemented using a defined process that is capable of achieving its process outcomes.
- **4 Predictable process** (two attributes)—The previously described established process now operates within defined limits to achieve its process outcomes.
- **5 Optimising process** (two attributes)—The previously described predictable process is continuously improved to meet relevant current and projected business goals[58].

[58] John W. Lainhart et al., The previous reference, Page : 42

Figure 2-12: Summary of the COBIT 5 Process Capability Model



Source: John W. Lainhart et al. , 2012, COBIT 5 : A Business Framework for the

III. Implementing IT Governance using COBIT 5:

3-1- Primary Steps towards IT Governance:

3-1-1- Creating the Appropriate Environment:

It is important for the appropriate environment to exist when implementing IT Governance improvements. This helps ensure that the initiative itself is governed and adequately guided and supported by management. Major IT initiatives often fail due to inadequate management direction, support and oversight. IT Governance implementations are no different; they have more chance of success if they are well governed and well managed.

An appropriate environment should therefore be created and maintained to ensure that IT Governance is implemented as an integral part of an overall governance approach within the enterprise. This should include adequate direction and oversight of the implementation initiative, including guiding principles. The objective is to provide sufficient commitment, direction and control of activities so that there is alignment with enterprise objectives and appropriate implementation support from the board and executive management.

Whether the implementation is a small or major initiative, executive management must be involved in and drive creation of the appropriate governance structures. The initial activities usually include assessment of current practices and the design of improved structures. In some cases it can lead to reorganisation within the business as well as the IT function and its relationship with business units. Executive management should set and maintain the governance framework—this means specifying the structures, processes and practices for IT Governance in line with agreed governance design principles, decision-making models, authority levels and the information required for informed decision making. Executive management should also allocate clear roles and responsibilities for directing the IT Governance improvement programme.

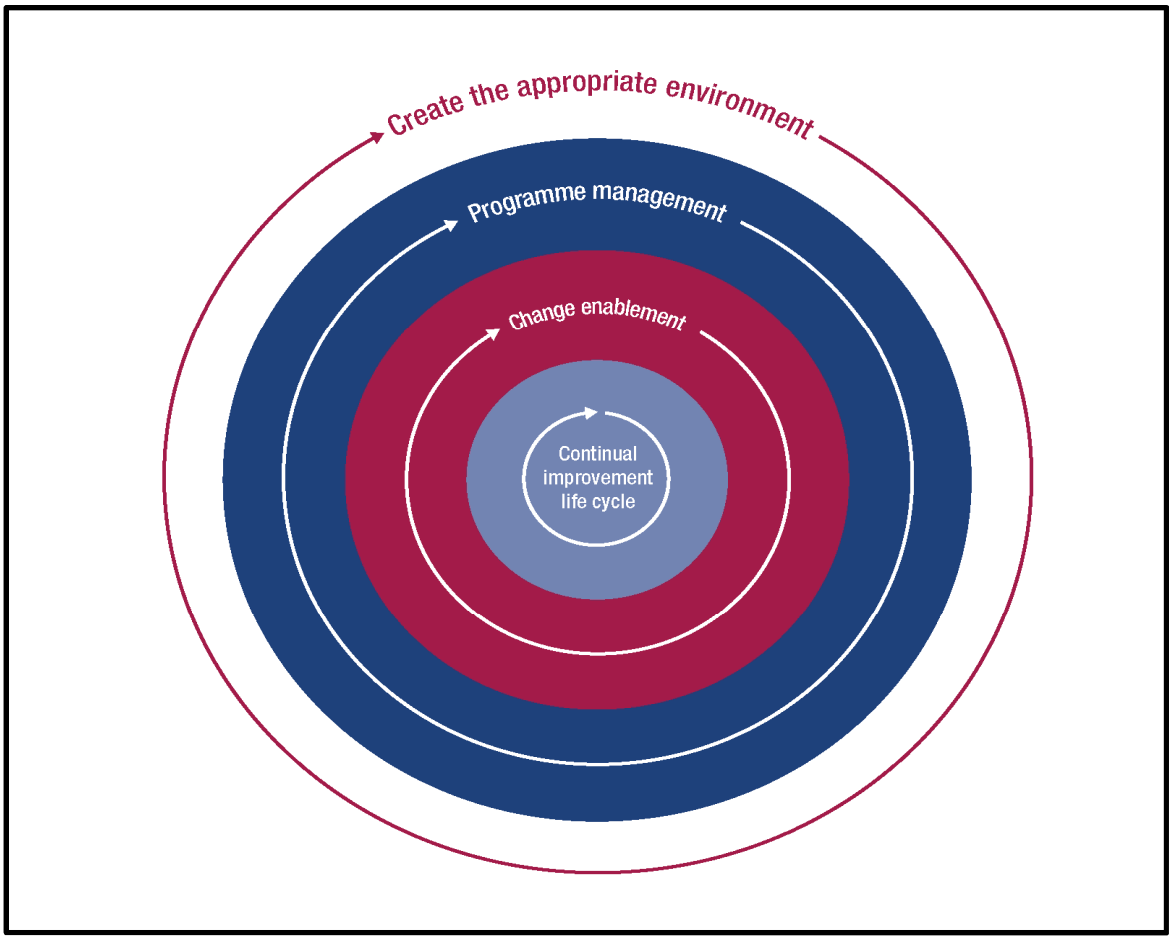
One of the best ways to formalise IT Governance and provide a mechanism for executive and board oversight and direction of IT-related activities is to establish an IT executive strategy committee. This committee acts on behalf of the board (to which it is accountable) and is responsible for how IT is used within the enterprise and for making key IT-related decisions affecting the enterprise. It should have a clearly defined mandate, and is best chaired by a business executive (ideally a board member) and staffed by senior business executives representing the major business units, as well as the chief information officer (CIO) and, if required, other senior IT managers. Internal audit and risk functions should provide an advisory role. Executives need to make decisions based on diverse opinions from business and IT managers, auditors and others. The COBIT 5 framework facilitates this by providing a common language for executives to communicate goals, objectives and expected results[59].

[59] Derek J. Oliver et al. 2012. COBIT 5 IMPLEMENTATION. ISACA Publications. 1st Edition. USA. Page : 17

3-1-2- Applying a Continual Improvement Life Cycle Approach:

Applying a continual improvement life cycle approach provides a method for enterprises to address the complexity and challenges typically encountered during IT Governance implementation. There are three interrelated components to the life cycle, as illustrated in **figure 2-12**: the core IT Governance continual improvement life cycle, the enablement of change (addressing the behavioural and cultural aspects of the implementation or improvement), and the management of the programme. In **figure 2-13**, the initiatives are depicted as continual life cycles to emphasise the fact that these are not one-off activities, but part of an ongoing process of implementation and improvement that in time become 'business as usual', at which time the programme can be retired.

Figure 2-13: Components of the Implementation Life Cycle

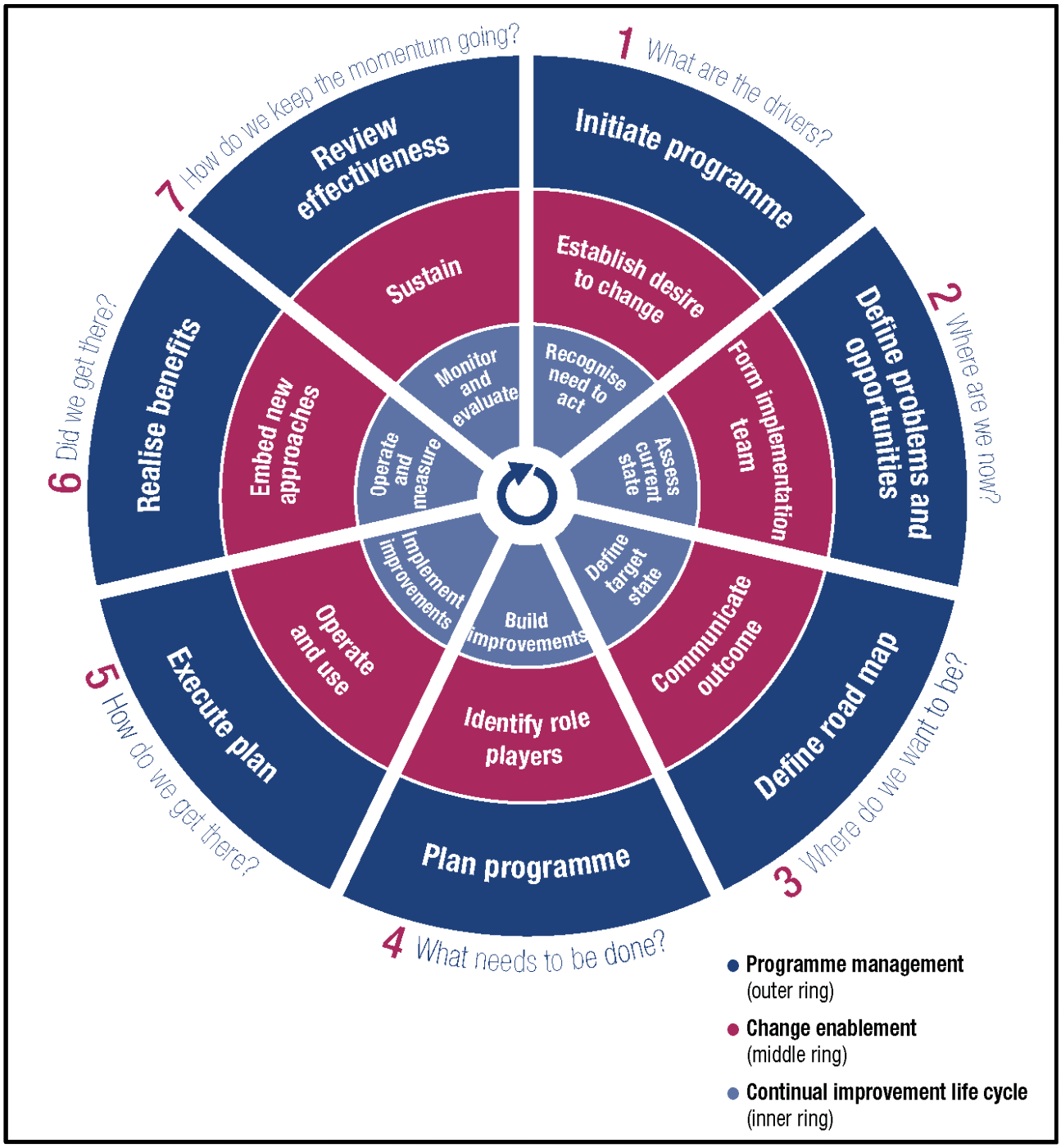


Source: Derek J. Oliver et al. 2012. COBIT 5 IMPLEMENTATION. ISACA Publications. 1st Edition. USA.

The seven phases of the implementation life cycle are illustrated in **figure 2-14**. The implementation and improvement programme is typically a continual and iterative one.

During the last phase, new objectives and requirements will be identified and a new cycle will be initiated.

Figure 2-14: Seven Phases of the Implementation Life Cycle



Source : Derek J. Oliver et al. 2012. COBIT 5 IMPLEMENTATION. ISACA Publications. 1st Edition. USA.

Phase1—What Are the Drivers?

Phase 1 identifies current change drivers and creates at executive management levels a desire to change that is then expressed in an outline of a business case. A change driver is an internal or external event, condition or key issue that serves as a stimulus for change. Events, trends (industry, market or technical), performance shortfalls, software implementations and even the goals of the enterprise can act as change drivers. Risk associated with implementation of the programme itself will be described in the business case and managed throughout the life cycle. Preparing, maintaining and monitoring a business case are fundamental and important disciplines for justifying, supporting and then ensuring successful outcomes of any initiative, including the improvement of IT Governance. They ensure a continuous focus on the benefits of the programme and their realisation.

Phase 2—Where Are We Now?

Phase 2 aligns IT-related objectives with enterprise strategies and risk, and prioritises the most important enterprise goals, IT-related goals and processes. COBIT 5 provides a generic mapping of enterprise goals to IT-related goals to IT processes to help with the selection. Given the selected enterprise and IT-related goals, critical processes are identified that need to be of sufficient capability to ensure successful outcomes. Management needs to know its current capability and where deficiencies may exist. This is achieved by a process capability assessment of the as-is status of the selected processes.

Phase 3—Where Do We Want To Be?

Phase 3 sets a target for improvement followed by a gap analysis to identify potential solutions. Some solutions will be quick wins and others more challenging, long-term tasks. Priority should be given to projects that are easier to achieve and likely to give the greatest benefit. Longer-term tasks should be broken down into manageable pieces.

Phase 4—What Needs To Be Done?

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

Phase 5—How Do We Get There?

Phase 5 provides for the implementation of the proposed solutions into day-to-day practices and the establishment of measures and monitoring systems to ensure that business alignment is achieved and performance can be measured. Success requires engagement, awareness and communication, understanding and commitment of top management, and ownership by the affected business and IT process owners[60].

[60] Derek J. Oliver et al. The previous reference, Page : 20

Phase 6—Did We Get There?

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

Phase 7—How Do We Keep the Momentum Going?

Phase 7 reviews the overall success of the initiative, identifies further governance or management requirements and reinforces the need for continual improvement. It also prioritises further opportunities to improve IT Governance. Programme and project management is based on good practices and provides for checkpoints at each of the seven phases to ensure that the programme performance is on track, the business case and risk are updated, and planning for the next phase is adjusted as appropriate. It is assumed that the enterprise's standard approach would be followed. Further guidance on programme and project management can also be found in COBIT 5 process BAI01. Although reporting is not mentioned explicitly in any of the phases, it is a continual thread through all of the phases and iterations.

The time spent per phase will differ greatly depending on (amongst other factors) the specific enterprise environment, its maturity, and the scope of the implementation or improvement initiative. However, the overall time spent on each iteration of the full life cycle ideally should not exceed six months, with improvements applied progressively; otherwise, there is a risk of losing momentum, focus and buy-in from stakeholders. The goal is to get into a rhythm of regular improvements. Larger-scale initiatives should be structured as multiple iterations of the life cycle. Over time, the life cycle will be followed iteratively while building a sustainable approach. This becomes a normal business practice when the phases in the life cycle are everyday activities and continual improvement occurs naturally.[61]

3-1-3- ENABLING CHANGE:

Successful implementation or improvement depends on implementing the appropriate change (the good practices) in the correct way. In many enterprises, there is a significant focus on the first aspect, but not enough emphasis on managing the human, behavioural and cultural aspects of the change and motivating stakeholders to buy into the change. Change enablement is one of the biggest challenges to IT Governance implementation. COBIT 5 defines change enablement as: "A systematic process of ensuring that all stakeholders are prepared and committed to the changes involved in moving from a current state to a desired future state"[62].

Various approaches to enabling change have been defined over the years and they provide valuable input that could be utilised during the implementation life cycle. One of the

[61] Derek J. Oliver et al. The previous reference, Page : 20
[62] John W. Lainhart et al., The previous reference, Page : 37

most widely accepted approaches to change enablement has been developed by John Kotter:

1. Establish a sense of urgency.
2. Form a powerful guiding coalition.
3. Create a clear vision that is expressed simply.
4. Communicate the vision.
5. Empower others to act on the vision.
6. Plan for and create short-term wins.
7. Consolidate improvements and produce more change.
8. Institutionalise new approaches[63].

The Kotter approach has been chosen as an adapted model for the specific requirements of an IT Governance implementation or improvement. This is illustrated by the change enablement life cycle in **figure 2-14**.

Phase 1—Establish the Desire to Change:

The purpose of this phase is to understand the breadth and depth of the envisioned change, the various stakeholders that are affected, the nature of the impact on and involvement required from each stakeholder group, as well as the current readiness and ability to adopt the change. Current pain points and trigger events can provide a good foundation for establishing the desire to change. The 'wake-up call', an initial communication on the programme, can be related to real-world issues that the enterprise may be experiencing. Also, initial benefits can be linked to areas that are highly visible to the enterprise, creating a platform for further changes and more widespread commitment and buy-in. While communication is a common thread throughout the implementation or improvement initiative, the initial communication or wake-up call is one of the most important and should demonstrate the commitment of senior management. Therefore, it should ideally be communicated by the executive committee or CEO.[64]

Phase 2—Form an Effective Implementation Team:

Dimensions to consider in assembling an effective core implementation team include involving the appropriate areas from business and IT as well as the knowledge and expertise, experience, credibility, and authority of team members. Obtaining an independent, objective view, as provided by external parties such as consultants and a change agent, could also be highly beneficial by aiding the implementation process or addressing skill gaps that may exist within the enterprise. Therefore, another dimension to consider is the appropriate mix of internal and external resources. The essence of the team should be a commitment to:

- A clear vision of success and ambitious goals;
- Engaging the best in all team members, all time;
- Clarity and transparency of team processes, accountabilities and communications;

[63] Kotter, John; 1996, Leading Change, Harvard Business School Press, USA, Page: 99
[64] Derek J. Oliver et al. The previous reference, Page : 37

- Integrity, mutual support and commitment to each other's success;
- Mutual accountability and collective responsibility;
- Ongoing measurement of its own performance and the way it behaves as a team;
- Living out of its comfort zone, always looking for ways to improve, uncovering new possibilities and embracing change.

Phase 3—Communicate Desired Vision :

A high-level change enablement plan should be developed in conjunction with the overall programme plan. A key component of the change enablement plan is the communication strategy, which should address who the core audience groups are, their behavioural profiles and information requirements, communication channels, and principles. The desired vision for the implementation or improvement programme should be communicated in the language of those affected by it. The communication should include the rationale for and benefits of the change as well as the impacts of not making the change (purpose), the vision (picture), the road map to achieving the vision (plan) and the involvement required of the various stakeholders (part). Senior management should deliver key messages (such as the desired vision). It should be noted in the communication that both behavioural/cultural and logical aspects should be addressed, and that the emphasis is on two-way communication. Reactions, suggestions and other feedback should be acted upon and captured.

Phase 4—Empower Role Players and Identify Quick Wins:

As core improvements are designed and built, change response plans are developed to empower various role players. The scope of these may include:

- Organisational design changes such as job content or team structures;
- Operational changes such as process flows or logistics;
- People management changes such as required training and/or changes to performance management and reward systems.[65]

Phase 5—Enable Operation and Use:

As initiatives are implemented within the core implementation life cycle, the change response plans also are implemented. Quick wins that have been realised are built on, and the behavioural and cultural aspects of the broader transition are addressed (issues such as dealing with fears of loss of responsibility, new expectations and unknown tasks). It is important to balance group and individual interventions to increase buy-in and engagement and to ensure that all stakeholders obtain a holistic view of the change. Solutions will be rolled out, and during this process, mentoring and coaching will be critical to ensure uptake in the user environment. The change requirements and objectives that had been set during the start of the initiative should be revisited to ensure that they were adequately addressed. Success measures should be defined and should include both hard business measures and perception measures that track how people feel about a change.[66]

[65] Derek J. Oliver et al. The previous reference, Page : 37
[66] Derek J. Oliver et al. The previous reference, Page : 38

Phase 6—Embed New Approaches :

As concrete results are achieved, new ways of working should become part of the enterprise's culture and be rooted in its norms and values. The implemented changes should be tracked, and the effectiveness of the change response plans should be assessed and corrective measures taken as appropriate. This might include enforcing compliance where still required. The communication strategy should be maintained to sustain ongoing awareness.

Phase 7—Sustain:

Changes are sustained through conscious reinforcement and an ongoing communication campaign, and they are maintained and demonstrated by continued top management commitment. Corrective action plans are implemented, lessons learned are captured and knowledge is shared with the broader enterprise.[67]

[67] Derek J. Oliver et al. The previous reference, Page : 38

3-2- Implementation Life cycle Tasks, Roles and Responsibilities:

Continual improvement of IT Governance is accomplished using the seven-phase implementation life cycle. Each phase is described with:

- Objective;
- Description;
- A brief about responsibilities of each group of role players in the phase. Note that these roles are generic and not every role necessarily must exist as a specific function.
- Change enablement tasks;

Phase 1—What Are the Drivers?

This phase aims at obtaining an understanding of the programme background and objectives and current governance approach. It articulates the compelling reasons to act within the organisational context. In this context the programme background, objectives and current governance culture are defined. The initial programme concept business case is defined. The buy-in and commitment of all key stakeholders is obtained.

Board and executive Provide guidance regarding stakeholder needs, business strategy, priorities, objectives, and guiding principles with respect to governance and management of enterprise IT. Business management and IT together ensure that stakeholder needs and business objectives have been stated with sufficient clarity to enable translation into business goals for IT, and provide input to understanding of risk and priorities. IT management gathers requirements and objectives from all stakeholders, gaining consensus on approach and scope. It provides expert advice and guidance regarding IT matters. Internal audit provides advice and challenge proposed activities and actions, ensuring that objective and balanced decisions are made. It provides input on current issues. Provide advice regarding controls and risk management practices and approaches. Risk, compliance and legal provide advice and guidance regarding risk, compliance and legal matters. They ensure that the management-proposed approach is likely to meet risk, compliance and legal requirements.[68]

In order to enable change, the phase contains the following tasks:

- Ensure integration with enterprise-level change enablement approaches or programmes, if any exist.
- Analyse the general organisational environment in which the change needs to be enabled, including organisation structure, management style(s), culture, ways of working, formal and informal relationships, and attitudes.
- Determine other ongoing or planned enterprise initiatives to determine change dependencies or impacts.
- Understand the breadth and depth of the change.

[68] Derek J. Oliver et al. The previous reference, Page : 40

• Identify stakeholders involved in the initiative from different areas of the enterprise as well as different levels and consider their needs.

• Determine the level of support and involvement required from each stakeholder group or individual, their influence and the impact of the change initiative on them.

• Determine the readiness and ability to implement the change for each stakeholder group or individual.

• Establish a wake-up call, using the pain points and trigger events as a starting point, and communicated by the IT executive strategy or steering committee (or an equivalent governance structure) to create awareness of the programme, its drivers and its objectives amongst all stakeholders.

• Eliminate any false signs of security or complacency.

• Instill the appropriate level of urgency, depending on the priority and impact of the change.

Phase 02—Where Are We Now?

The second phase identifies the enterprise and IT-related goals, i.e., how IT contributes to the enterprise goals identified via solutions and services. The focus is on identifying and analysing how IT creates value for the enterprise in enabling business transformation in an agile way, in making the current business processes more efficient, in making the enterprise more effective, and in meeting governance-related requirements such as managing risk, ensuring security, and complying with legal and regulatory requirements.

Based on the enterprise risk profile and its risk history and appetite, and actual benefit/value enablement risk, define benefit/value enablement risk, programme/project delivery and service delivery/IT operations risk to the enterprise and IT-related goals. The understanding of business and governance drivers and a risk assessment are used to focus on the processes critical to ensuring that IT goals are met. Then, it is necessary to establish how mature, well managed and executed these processes are, based on process descriptions, policies, standards, procedures and technical specifications, to determine whether they are likely to support the business and IT requirements.

Board and executive try to verify and interpret the results/conclusions of assessments. Business management assists IT with reasonableness of current assessments by providing the customer view. IT management ensures open and fair assessment of IT activities. It guides assessment of current practice. It obtains consensus. The internal audit role is to provide advice, provide input to and assist with current-state assessments. And if required, independently verify assessment results. Finally, risk, compliance and legal Review

assessment to ensure that risk, compliance and legal issues have been considered adequately.[69]

As it is mentioned previously, the enablement change part of this phase is about forming an effective implementation team. This includes:

- Assemble a core team from the business and IT with the appropriate knowledge, expertise, profile, experience, credibility and authority to drive the initiative. Identify the most desirable person (effective leader and credible to the stakeholders) to lead this team. Consider the use of external parties, such as consultants, as part of the team to provide an independent and objective view or to address any skill gaps that may exist.
- Identify and manage any potential vested interests that may exist within the team to create the required level of trust.
- Create the appropriate environment for optimal teamwork. This includes ensuring that the necessary time and involvement can be given.
- Hold a workshop to create consensus (shared vision) within the team and adopt a mandate for the change initiative.

Phase 03—Where Do We Want To Be?

It is based on the assessed current-state process capability levels, and using the results of the enterprise goals to IT-related goals analysis and identification of process importance performed earlier, an appropriate target capability level should be determined for each process. The chosen level should take into account available external and internal benchmarks. It is important to ensure the appropriateness to the business of the level chosen After the current capability of the process has been determined and the target capability planned, the gaps between as-is and to-be states should be evaluated and opportunities for improvement identified. After the gaps have been defined, the root causes, common issues, residual risk, existing strengths and best practices to close those gaps need to be determined. This phase may identify some relatively easy-to-achieve improvements such as improved training, the sharing of good practices and standardising procedures; however, the gap analysis is likely to require considerable experience in business and IT management techniques to develop practical solutions. Experience in undertaking behavioural and organisational change will also be needed.

Board and executive role is to set priorities, time scales and expectations regarding the future capability required from IT. Business management assists IT with the setting of capability targets. Ensure that the envisaged solutions are aligned to enterprise goals. IT

[69] Derek J. Oliver et al. The previous reference, Page : 42

management applies professional judgment in formulating improvement priority plans and initiatives. Obtain consensus on a required capability target. Ensure that the envisaged solution is aligned to IT-related goals. Internal audit provides advice and assist with target-state positioning and gap priorities. If required, independently verify assessment results. Risk, compliance and legal review plans to ensure that risk, compliance and legal issues have been addressed adequately.[70]

In order to describe and communicate desired outcome, the following tasks need to be accomplished:

- Describe the high-level change enablement plan and objectives, which will include the following tasks and components.
- Develop a communication strategy (including core audience groups, behavioural profile and information requirements per group, core messages, optimal communication channels, and communication principles) to optimise awareness and buy-in.
- Secure willingness to participate (picture of the change).
- Articulate the rationale for, and benefits of, the change to support the vision and describe the impact(s) of not making the change (purpose of the change).
- Link back to objectives for the initiative in the communications and demonstrate how the change will realise the benefit.
- Describe the high-level road map to achieving the vision (plan for the change) as well as the involvement required of various stakeholders (role within the change).
- Use senior management to deliver key messages to 'set the tone at the top'.
- Use change agents to communicate informally in addition to formal communications.
- Communicate through action—the guiding team should set an example.
- Appeal to their emotions where required to get people to change behaviours.

[70] Derek J. Oliver et al. The previous reference, Page : 45

Phase 04—What Needs To Be Done?

This phase aims to translate improvement opportunities into justifiable contributing projects. When all of the potential initiatives for improvement have been identified, these initiatives should be prioritised into formal and justifiable projects. The projects with high benefit and that are relatively easy to implement should be selected first and translated into formal and justifiable projects, each with a project plan that includes the project's contribution to the programme objectives. It is important to check whether the objectives still conform to the original value and risk drivers. The projects will be included in an updated business case for the programme. Details of any unapproved improvement project proposals should be recorded in a register for potential future consideration and opportunities presented for sponsors to reappraise and, when appropriate, resubmit their recommendations at a later date.

Board and executive support justified actions, provide budgets, and set priorities as appropriate. Business management Together with IT, ensure that the proposed improvement actions are aligned with agreed-on enterprise and IT-related goals and that any activities requiring business input or action are supported. Ensure that required business resources are allocated and available. Agree with IT on the metrics for measuring the outcomes of the improvement programme. IT management ensures viability and reasonableness of the programme plan. Ensure that the plan is achievable and that there are resources available to execute the plan. Consider the plan together with priorities of the enterprise's portfolio of IT-enabled investments to decide a basis for investment funding. Internal audit provides independent assurance that issues identified are valid, business cases are objectively and accurately presented, and plans appear achievable. It provides expert advice and guidance where appropriate. Risk, compliance and legal ensure that any identified risk, compliance and legal issues are being addressed, and proposals conform with any relevant policies or regulations.[71]

The change enablement tasks for this phase are:

- Obtain buy-in by engaging those affected by the change in the design through mechanisms such as workshops or review processes and giving them responsibility to accept the quality of results.

- Design change response plans to proactively manage change impacts and maximise engagement throughout the implementation process (could include organisational changes such as job content or organisational structure; people management changes such as training; performance management systems; or incentives/remuneration and reward systems).

[71] Derek J. Oliver et al. The previous reference, Page : 47

• Identify quick wins that prove the concept of the improvement programme. These should be visible and unambiguous, build momentum, and provide positive reinforcement of the process.

- Where possible, build on any existing strengths identified in phase 2 to realise quick wins. Identify strengths in existing enterprise processes that could be leveraged.

Phase 05—How Do We Get There?

This phase involves the most effort and longest elapsed time of all the life cycle phases. It is recommended, however, that the size and overall time taken not be excessive to ensure that it is manageable and that benefits are delivered in a reasonable time frame. This is especially true for the first few iterations when it will also be a learning experience for all involved. Monitor performance of each project to ensure that goals are being achieved. Report back to stakeholders at regular intervals to ensure that progress is understood and on track.

The role of board and executive is to monitor implementation and provide support and direction as required. Business management takes ownership for business participation in the implementation, especially where business processes are affected and IT processes require user/customer involvement. IT management makes sure that the implementation includes the full scope of activities required and that they are practical and achievable and likely to be adopted and used. It makes sure that process owners are involved, buy into the new approach and own the resulting processes. It resolves issues and manages risk as encountered during the implementation. Internal audit reviews and provide input during implementation to avoid identification of missing enablers and especially key controls after the fact. It provides guidance on implementation of control aspects. If required, provide a project/implementation risk review service, monitoring risk that could jeopardise implementation and providing independent feedback to the programme and project teams. Finally, Risk, compliance and legal Provide guidance as required on risk, compliance and legal aspects during implementation.[72]

As it is mentioned previously the main focus of this phase is to enable operation and use. This may be realised if the IT Governance entities execute the following tasks:

- Build on the momentum and credibility that can be created by quick wins, then introduce more widespread and challenging change aspects.
- Communicate quick-win successes and recognise and reward those involved in them.
- Implement the change response plans.

[72] Derek J. Oliver et al. The previous reference, Page : 50

- Ensure that the broader base of role players has the skills, resources and knowledge, as well as buy-in and commitment to the change.
- Balance group and individual interventions to ensure that a holistic view of the change is obtained by key stakeholders.
- Communicate roles and responsibilities for use.
- Define measures of success, including those from a business viewpoint and perception measures.
- Set in place mentoring and coaching to ensure uptake and buy-in.
- Close the loop and ensure that all change requirements have been addressed.

Phase 06—Did We Get There?

In this phase, IT Governance entities try to report positive and negative results from the performance measurements to all stakeholders, which will build confidence and enable any corrective actions to be taken on time. Projects should be monitored as they are developing, using both programme management and project management techniques, and preparation should be made to change the plan and/or cancel the project if early indications are that a project is off track and may not meet critical milestones.

Board and executive try to assess performance in meeting the original objectives and confirm realisation of desired outcomes. They consider the need to redirect future activities and take corrective action. They assist in the resolution of significant issues, if required. Business management provides feedback and considers the effectiveness of the business contribution to the initiative. It uses positive results to improve current business-related activities. It uses else lessons learned to adapt and improve the business approach to future initiatives. IT management provides feedback and considers the effectiveness of IT contribution to the initiative. It uses positive results to improve current IT-related activities. IT monitors projects based on project criticality as they are developing, using both programme management and project management techniques, and be prepared to change the plan and/or cancel one or more projects or take other corrective action if early indications are that a project is off track and may not meet critical milestones. It uses lessons learned to adapt and improve IT approach to future initiatives. Internal audit provides independent assessment of the overall efficiency and effectiveness of the initiative. Provide feedback and consider the effectiveness of audit contribution to the initiative. It uses positive results to improve current audit-related activities. It uses lessons learned to adapt and improve audit approach to future initiatives. Finally, Risk, compliance and legal assess whether the initiative has improved the ability of the enterprise to identify and manage risk

and legal, regulatory and contractual requirements. They provide feedback and make any necessary recommendations for improvements.[73]

To be successful in enabling the change for this phase, it is necessary to realise these tasks:

- Ensure that new ways of working become part of the enterprise culture (the way we do things around here), i.e., rooted in the enterprise norms and values. This is important for concrete results to be achieved.
- In transitioning from project mode to business as usual, behaviours need to be shaped by revised job descriptions, remuneration and reward systems, and operating procedures as implemented through the change response plans.
- Monitor whether assigned roles and responsibilities have been assumed.
- Track the change and assess the effectiveness of the change response plans, linking the results back to the original change objectives and goals. This should include both hard business measures and perception measures.
- Leverage pockets of excellence to provide a source of inspiration.
- Maintain the communication strategy to achieve ongoing awareness and highlight successes.
- Ensure that there is open communication amongst all role players to resolve issues.
- Where issues cannot be resolved, escalate to sponsors.
- Document change enablement lessons learned for future implementation initiatives/

[73] Derek J. Oliver et al. The previous reference, Page : 52

Phase 07-How Do We Keep the Momentum Going?

The goal of this phase is to enable the team to determine whether the programme delivered against expectations. This can be done by comparing the results to the original success criteria and gathering feedback from the implementation team and stakeholders via interviews, workshops and satisfaction surveys. The lessons learned can contain valuable information for team members and project stakeholders for use in ongoing initiatives and improvement projects. It involves continual monitoring, regular and transparent reporting, and confirmation of accountabilities. Further improvements are identified and used as input to the next iteration of the life cycle.

In this phase, the enterprise should build on the successes and lessons learned from the governance implementation project(s) to build and reinforce commitment amongst all IT and business stakeholders for continually improved governance of IT. Policies, organisational structures, roles and responsibilities, and governance processes should be developed and optimised so that IT Governance operates effectively as part of normal business practice, and there is a culture supporting this, demonstrated by top management.

Board and executive provide direction, set objectives, and allocate roles and responsibilities for the enterprise for the improvement of IT Governance. They continue to 'set the tone at the top', develop organisational structures, and encourage a culture of good governance and accountability for IT amongst business and IT executives. They ensure else that IT is aware of, and, as appropriate, involved in, new business objectives and requirements in as timely a manner as possible. Business management provides support and commitment by continuing to work positively with IT to improve IT Governance and make it business as usual. It verifies that new IT Governance objectives are aligned with current enterprise objectives. IT management drives and provides strong leadership to sustain the momentum of the improvement programme. It engages in governance activities as part of normal business practice. It creates policies, standards and processes to ensure that governance becomes business as usual. Internal audit provides objective and constructive input, encourage self-assessment, and provide assurance to management that governance is working effectively, thus building confidence in IT. It provides ongoing audits based on an integrated governance approach using criteria shared with IT and the business based on the COBIT framework. Risk, compliance and legal Work with IT and the business to anticipate legal and regulatory requirements, and identify and respond to IT-related risk as a normal activity in IT Governance.[74]

As it is mentioned previously, the enablement change main focus in this phase is about the sustaining. This may be possible if the organisation carries out the following tasks:

- Provide conscious reinforcement and an ongoing communication campaign, as well as demonstrated continual top management commitment.

[74] Derek J. Oliver et al. The previous reference, Page : 54

- Confirm conformance to objectives and requirements.
- Continually monitor the effectiveness of the change itself, change enablement activities and buy-in of stakeholders.
- Implement corrective action plans where required.
- Provide feedback on performance, reward achievers and publicise successes.
- Share knowledge from the initiative to the broader enterprise.

3-3-Impact of COBIT 5 on IT Governance:

This research sets two assessment levels for COBIT 5 impact on IT Governance. The first level concerns IT Governance Implementation, it is about the produced output by using COBIT 5 as a framework for IT Governance. The second level is submitted as the final impact; it deals with its exact contributions in IT Governance Focus Areas (Life cycle).

Table 2-4: COBIT 5 components used in IT Governance Implementation

Phase	COBIT 5 Resource used in IT Governance
Phase 01	• COBIT 5 (enterprise goals, enablers) • COBIT 5: Enabling Processes (EDM01; AP001; MEA01) • COBIT 5 Implementation • The Business Case Guide: Using Val IT 2.0
Phase 02	• COBIT 5 (enterprise goals—IT-related goals cascade and mapping of stakeholder needs to goals), www.isaca.org/cobit • COBIT 5: Enabling Processes AP001; AP002; AP005; AP012; BAI01; MEA01; MEA02; MEA03 (used for process selection as well as implementation and programme planning) • COBIT 5 Implementation • COBIT 5 self-assessment guide
Phase 03	• COBIT 5 (enterprise goals) • COBIT 5: Enabling Processes (management practices and activities for the target-state definition and gap analysis; AP001, AP002) • COBIT 5 self-assessment guide.
Phase 04	• COBIT 5 (enabler models), www.isaca.org/cobit • COBIT5: Enabling Processes (AP05.AP012, BAI01;goals and metrics)
Phase 05	• COBIT5: Enabling Processes(as best practice input and BAI01)
Phase 06	• COBIT5: Enabling Processes(as best practice input and EDM05, AP005, BAI01, MEA01)
Phase 07	• COBIT 5: Enabling Processes (EDM01, AP001, BAI08, MEA01)

Source:

1- Derek J. Oliver et al. 2012. COBIT 5 IMPLEMENTATION. ISACA Publications. 1st Edition. USA

2- Gary Hardy et al. 2012. IT Governance Implementation Guide. IT Governance Institute. USA. Published on www.itgi.org.

Table 2-5: COBIT 5 Output in each IT Governance implementation phase	
Phase	**COBIT 5 Output**
Phase 01	✓ Business case outline; ✓ High-level roles and responsibilities; ✓ Identified stakeholder map, including support and involvement required, influence and impact, and agreed-on understanding of the efforts required to manage human change; ✓ Programme wake-up call (all stakeholders); ✓ Programme kick-off communication (key stakeholders).
Phase 02	✓ Agreed-on enterprise goals for IT and impact on IT; ✓ An agreed-on understanding of the risk and impacts resulting from misaligned IT-related goals and service and project delivery failures; ✓ Selected processes and goals; ✓ Current capability rating for selected processes; ✓ Risk acceptance position and risk profile; ✓ Benefit/value enablement risk, programme/project delivery and service delivery/IT operations risk assessments; ✓ Strengths on which to build; ✓ Change agents in different parts and at different levels in the enterprise. ✓ Core team and assigned roles and responsibilities; ✓ Evaluated outline business case; ✓ An agreed-on understanding of the issues and challenges (including process capability levels).
Phase 03	✓ Target capability rating for selected processes; ✓ Description of improvement opportunities; ✓ Risk response document including risk not mitigated; ✓ Change enablement plan and objectives; ✓ Communication strategy and communication of the change vision covering the four Ps (picture, purpose, plan, part); ✓ Detailed business case; ✓ High-level programme plan; ✓ Key metrics that will be used to track programme and operational performance.
Table 2-5 (Cont.)	
Phase 04	✓ Implemented improvements; ✓ Implemented change response plans; ✓ Realised quick wins and visibility of change success; ✓ Success communications; ✓ Defined and communicated roles and responsibilities in the business-as-usual

	environment; ✓ Project change logs and issue/risk logs; ✓ Defined business and perception success measures; ✓ Benefits tracked to monitor realisation.
Phase 05	✓ Implemented improvements; ✓ Implemented change response plans; ✓ Realised quick wins and visibility of change success; ✓ Success communications; ✓ Defined and communicated roles and responsibilities in the business-as-usual environment; ✓ Project change logs and issue/risk logs; ✓ Defined business and perception success measures; ✓ Benefits tracked to monitor realisation.
Phase 06	✓ Updated project and programme scorecards; ✓ Change effectiveness measures (both business and perception measures); ✓ Report explaining scorecard results; ✓ Improvements entrenched in operations; ✓ Key metrics added into ongoing IT performance measurement approach.
Phase 07	✓ Recommendations for further IT Governance activities; ✓ Stakeholder satisfaction survey; ✓ Documented success stories and lessons learned; ✓ Ongoing communication plan; ✓ Performance reward scheme.

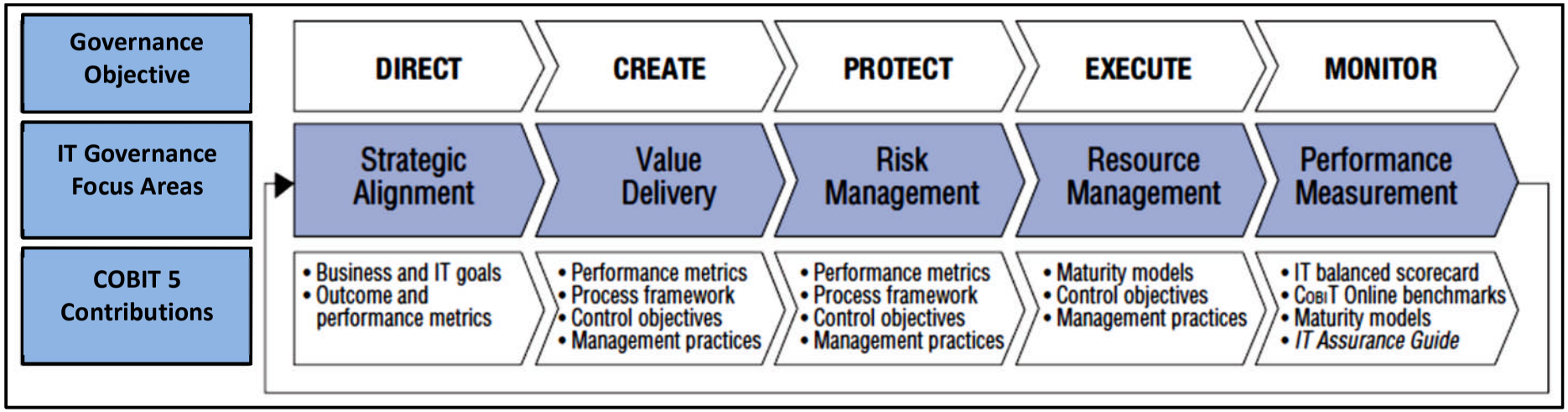
Source:

1- Derek J. Oliver et al. 2012. COBIT 5 IMPLEMENTATION. ISACA Publications. 1st Edition. USA

2- Gary Hardy et al. 2012. IT Governance Implementation Guide. IT Governance Institute. USA. Published on www.itgi.org.

As it has been mentioned in CHAPTER 01, IT governance is a life cycle that, for a specific objective, can be entered at any point but is best started from the point of aligned business and IT strategy. Then, the implementation will be focused on delivering the value that the strategy promises and addressing the risks that need to be managed. COBIT 5 plays a critical role in these areas through its contributions; those are formed by the previous phases' outputs. COBIT 5 contributions include Business and IT goals, Outcome and performance metrics, Process framework, Control objectives, Management practices, Maturity models, IT balanced scorecard, COBIT Online benchmarks, IT Assurance Guide (**Figure 2-13**).

Figure 2-15 : IT Governance Lifecycle



Source : Gary Hardy et al. 2012. IT Governance Implementation Guide. IT Governance Institute. USA. Published on www.itgi.org.

CHAPTER 03

A Case study of Statoil Company

Introduction:

All what has been instituted in the theoretical part is good and interesting, but the better is to support it with empirical investigation, because each company has its own characteristics. The third chapter tries to investigate practically the impact of Cobit 5 on IT Governance Stages, and the impact of these stages on IT Governance effectiveness, using Statoil Company as a model to kill such ambiguities about practical area.

As Statoil is a large company with an extensive governance system and many governing and strategic documents most of the work done in this study has been to classify and analyze data. The data relevant to the study was somewhat unordered and unstructured described in Statoil's systems. Understanding the Statoil IT governance was vital to the success of this thesis, and most of time has been spent studying Statoil implementations.

The main aim of this chapter is to test the theoretical model using an adequate model. The first element treated in this chapter is methodology; it is about the study used population; the reason behind choosing Statoil Company as a target case; methods and tools of data collection and sampling; and the method of data analysis. After the methodology the study moves to analysing Statoil management system, targeting the elements associated with its subject such as values, organisational principles, company arenas, and Business Process Modal. The third element referred to is Corporate Governance; it is about governing bodies and governing documentation. The fourth element is an analysis of IT Service, focusing on the existing compatibility between Statoil IT Processes and COBIT 5 Processes during the realisation of COBIT 5 project; and externalizing its influence on IT Governance effectiveness, passing by its impact on ITG stages accomplishment levels. Finally, the study moves to statistical data analysis and discussion, externalizing practical knowledge about the relationship between COBIT 5 and IT Governance.

1-Methodology:

This study tries to investigate practically if and how does COBIT 5 enables IT Governance Stages, and to determine the influence of these components on IT Governance effectiveness.

1-1- Study Population:

This study is a field study, where Statoil Company represents the study's unit of analysis. Here the study justifies the use of Statoil Company as a study's unit.

Why Statoil Company??

Statoil has grown up along with the emergence of the Norwegian oil and gas industry, dating back to the late 1960s. In 1972, the Norwegian State Oil Company, Statoil, was formed, and two years later the Statfjord field was discovered in the North Sea. In 1979, the Statfjord field commenced production, and in 1981 Statoil was the first Norwegian company to be given operator responsibility for a field, at Gullfaks in the North Sea.

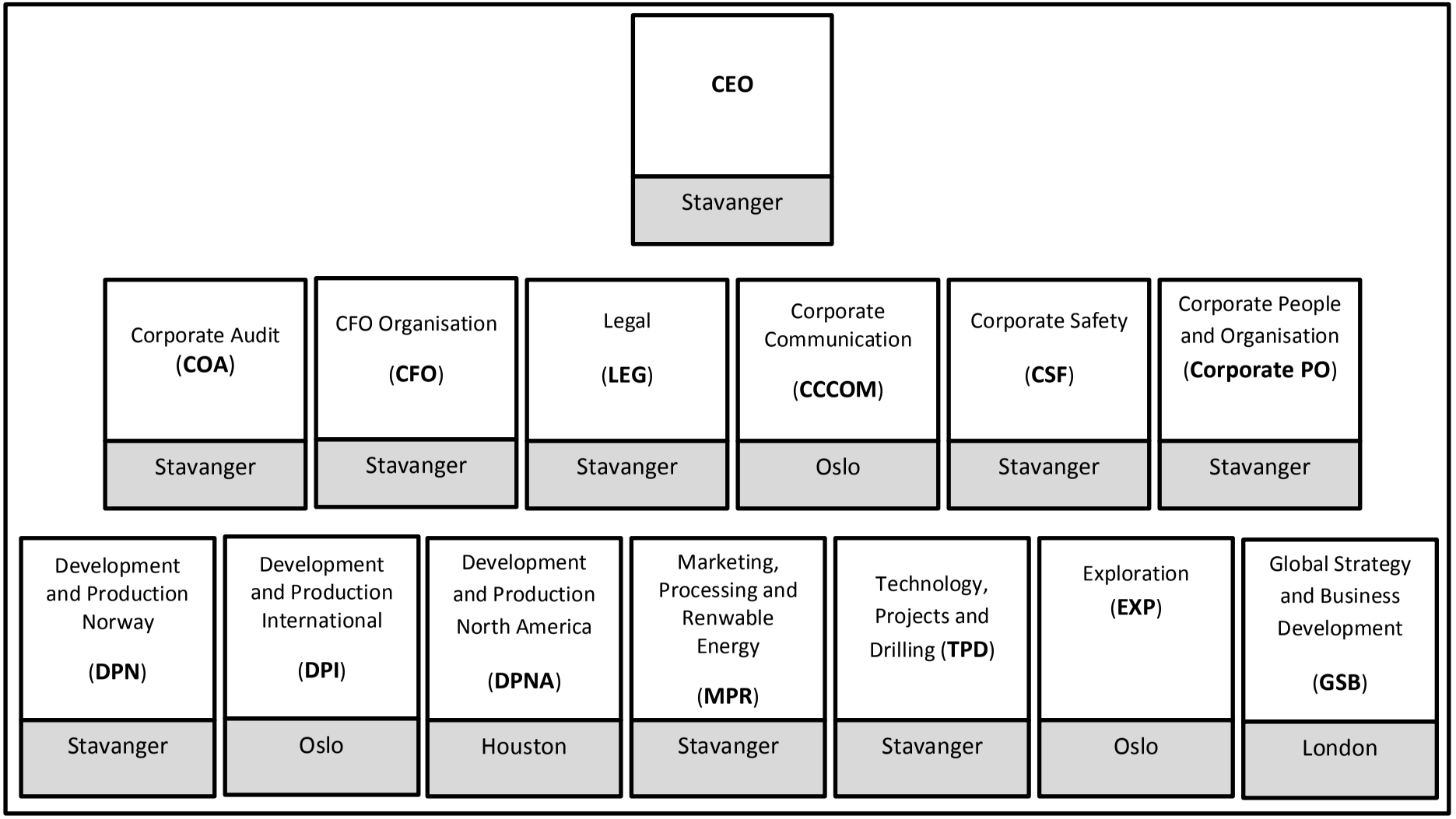
Statoil merged with Norsk Hydro's oil and gas division on 1 October 2007. The new company was given the temporary name of StatoilHydro, and the new company reached a size and strength for considerable international expansion. The company changed its name back to Statoil on 1 November 2009. Norsk Hydro's oil history stretches back to the late 1960's, when the company was a license holder in the giant Ekofisk discovery in the North Sea in 1969.

Statoil has been one of the most important players in the Norwegian oil industry, and has contributed strongly to make Norway into a modern industrial nation. Today, Norway is one of the world's most productive petroleum provinces and a test lab for technology development, and this company is one of the world's largest suppliers of oil and gas.

Statoil has become an international energy company with operations in 34 countries; Algeria, Angola, Azerbaijan, Australia, Bahamas, Belgium, Brazil, China, Cuba, Denmark, Faroe Islands, Germany, Greenland, India, Indonesia, Ireland, Kazakhstan, Libya, Mozambique, Netherlands, Nigeria, Norway, North America, Russia, Singapore, Suriname, Tanzania, Turkey, Turkmenistan, United Arab Emirates, United Kingdom, Venezuela. Building on 40 years of experience from oil and gas production on the Norwegian continental shelf, it is committed to accommodating the world's energy needs in a responsible manner, applying technology and creating innovative business solutions. It is headquartered in Stavanger, Norway with approx. 23,000 employees worldwide, and is listed on the New York and Oslo stock exchanges.

It is by far the largest Norwegian company and it has its own IT Department which, among other activities, works with development and maintenance of software systems used in the oil- and gas industry all around the world. To be competitive in the oil- and gas market, Statoil continuously explores and takes advantage of new technologies and updates strategies and governance policies.

Figure 3-1 : Statoil Organisational Chart



Source : The Statoil Book. 2013. Version 3.1

1-2- Data Collection and sampling:

The study data will be collected using primary and secondary sources. Secondary sources are articles, journals, books and theses, while primary data will be gathered from three sources. The first primary source is field study Statoil Company by visiting In Salah Gas Group, and making electronic correspondence with the company executives. The second primary source is Statoil professional documents such as the company status; Governing documentations; annual reports; IT Service reports, IT Projects' schedules, and balanced scorecards, Business Process Programme.

In order to collect data, the researcher will use content analysis and questionnaire, and he will conduct some interviews.

1-3- Data Analysis:

Data will be analyzed using COBIT 5 to analyse Statoil Business Process Model and COBIT5 assessors to assess maturity of IT Governance components and IT Governance effectiveness for different Statoil IT processes.

MINITAB16. It will be used to compute the reliability of the instruments and data sources. The level of significance will be set at 0.05 for all relationships. To test the study's hypotheses, the following data analysis methods will be used:

- Descriptive statics to describe the characteristics of the sample of study;
- Regression Analysis will be used to test the validity of the study model as well as the impact of independent variables on the dependent variable.

2- Corporate Governance:

It is a public limited company with a governance structure based on Norwegian law. Its main share listing is on the Oslo Stock Exchange, and its share is also listed on the New York Stock Exchange. According to its articles of association, its object is to engage in exploration, production, transportation, refining and marketing of petroleum and petroleum-derived products, and other forms of energy, as well as other business. This company is responsible for marketing and selling the Norwegian government's petroleum, derived from the state's direct financial interest (SDFI) or paid as royalty in kind. Statoil's objective is to ensure long-term value creation for its shareholders through engaging in exploration for and production, transportation, processing and marketing of petroleum and petroleum-derived products. The following principles underline its approach to corporate governance:

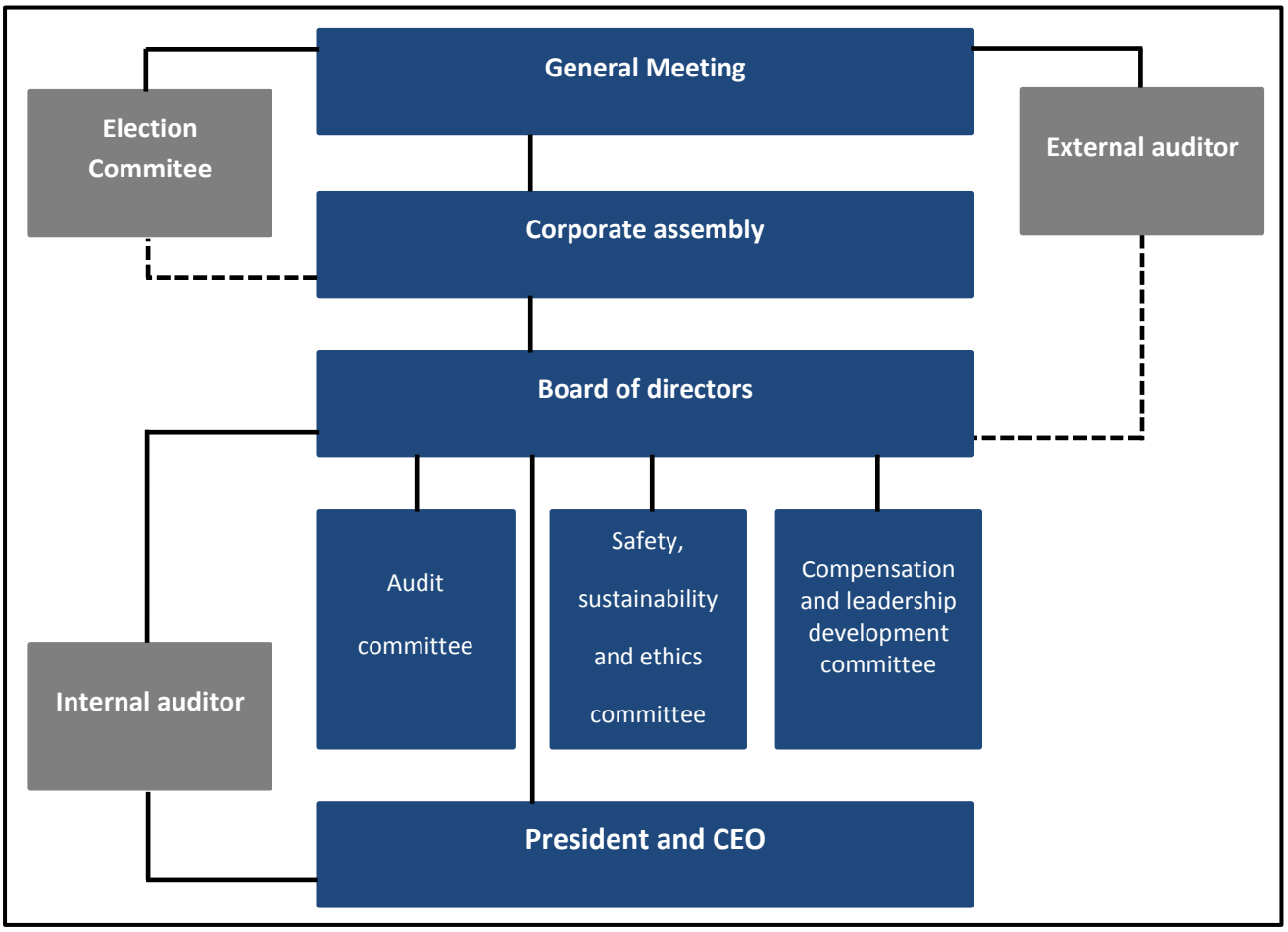
- All shareholders will be treated equally;
- Statoil will ensure that all shareholders have access to up-to-date, reliable and relevant information about the company's activities;
- Statoil will have a board of directors that is independent of the group's management. In accordance with its ethical guidelines, the board focuses on there not being any conflicts of interest between owners, the board of directors and the company management;
- The board of directors will base its practical work on the principles for good corporate governance applicable at all times.[1]

2-1-Governing bodies :

Governing bodies in Statoil includes the board of directors, the general meeting and the corporate assembly. The board of directors is responsible for the overall management of the Statoil group, and for supervising the group activities in general. They handle matters of major importance, and they appoint the president and chief executive officer (CEO). They also establish the working instructions, power of attorney, and terms and conditions of employment for the president and CEO.[2]

[1] The Statoil Book. 2013. version 3.1
[2] The Statoil Book. 2013. version 3.1

Figure 3-2: Statoil Governing Bodies



Source: The Statoil Book. 2013. Version 3.1

●The board of directors:

The board of directors of Statoil is responsible for the overall management of its group, and for supervising its activities in general as further defined in the board rules of procedure. The board handles matters of major importance or of an extraordinary nature. However, it may require that any matter be referred to it. The board appoints the president and chief executive officer (CEO), and establishes the working instructions, powers of attorney, and terms and conditions of employment for the chief executive.

The board has three sub-committees. The audit committee role is to support the board in exercising its management and monitoring responsibilities, particularly in respect of accounting and financial reporting, and to ensure that this group has an independent and effective external and internal audit system. The safety, sustainability and ethics committee role is to assist the board in its supervision of the company safety, sustainability and ethics policies, systems and principles with the exception of aspects related to financial matters.

The role of the compensation and leadership development committee is to assist the board of directors in its work relating to the terms of employment for Statoil CEO and the main principles and strategy for the remuneration and leadership development of senior executives in Statoil.[3]

●The general meeting:

The general meeting tasks include approving the company accounts and the allocation of net income, electing the members of the corporate assembly, and electing the members of the election committee.

External auditor is independent of the company and elected by the general meeting. The same firm of auditors should, as a general rule, be appointed for all the subsidiaries. If an auditor is appointed for joint ventures the company operates, its external auditor must be used. Any deviation from this rule must be approved by the chief financial officer (CFO).

●The corporate assembly:

The corporate assembly has a duty to supervise the board and chief executive in their management of the company. It takes decisions based on proposals from the board on matters related to substantial investments, measured against the total resources of Statoil group, and in matters concerning the rationalization and restructuring of operations which would result in a major change in the workforce. The corporate assembly is responsible for electing the board.

●Governance of subsidiaries:

Control and management of all organisational entities is based on the same governance principles, whether the entity is organisationally a part of parent company or an independent legal entity in the form of a wholly-owned subsidiary (wholly-owned limited liability company). In the case of partly-owned subsidiaries, the same principle applies concerning control and management of the business. Statoil representatives on the boards of such companies must coordinate their points of view and vote in accordance with decisions made in the line.

3-2-Governing Documentation:

Governing documentation ensures standardisation and the deployment of best practice across the group. Function requirements for the function and process areas describe what the company wants to achieve. Process models, work flow diagrams and requirements describe how to execute activities. The owners of governing documentation handle proposals for improvements and, where relevant, provide recommendations on dispensations. Owners of governing documentation are appointed in subsidiaries which have their own management system.[4]

[3] The Statoil Book. 2013. version 3.1
[4] The Statoil Book. 2013. version 3.1

It is the corporate parent obligation acting through the line to ensure that its subsidiaries implement Statoil global governing documentation. It is the subsidiary obligation to assess and implement such governance, to the extent possible based on legal advice.

Table 3-1: Governing Documentation

Process owners	Function owners
Exploration (EXPL)	Management system (MS)
Petroleum technology and IOR (PETEC)	Safety (SF)
Drilling and well (D&W)	Information technology (IT)
Project development (PD)	Legal (LEG)
Operation and maintenance (OM)	People and organisation (PO)
Marketing and supply (M&S)	Finance and control (F&C)
Supply chain management (SCM)	Sustainability (SU)
Technology development and implementation (TDI)*	Communication (COM)
Business development (BD)*	Risk management (RM)**
	Ethics and compliance (EC)**
	Facility Management (FM)**

* Owners of TDI and BD governing documentation are not formally defined as process owners, but have the same responsibility for governing documentation, simplification, improvement and monitoring as described for the process owner.

**These areas are not defined as corporate functions, but holds the role as function owners with ownership to corresponding functional requirements.

3-Statoil Management System:

Statoil has a management system which defines how it works and describes how it leads and performs its activities. This system has three main objectives:

1. Contribute to safe, reliable and efficient operations and enable the company to comply with external and internal requirements;
2. Help this company to incorporate its values, its people and its leadership principles in everything Statoil does;
3. Support the business performance through high-quality decision- making, fast and precise execution, and continuous learning.

3-1-Statoil Values:

Statoil values embody its spirit and energy. These values are essential if the company is to succeed over time in a competitive environment. They are at the core of its management system. Statoil values drive its performance and guide it in how it does business, and in how it works together and towards external stakeholders.

●**Courageous:** Be ambitious, identify opportunities and challenges, make demands and manage risk;

●**Open:** Be trustful, curious, promote value diversity, communicate well, be ethical;

●**Hands-on:** Deliver on promises, develop expertise, and strive for simplification and clarity, act loyal to decisions and show dedication and endurance;

●**Caring:** Cause zero harm to people and prevent accidents, save the environment, act within law, demonstrate social responsibility and respect the individual.

3-2-Statoil Organisational Principles:

Statoil organisational principles define a simple organisational design which has the flexibility to meet demands of a changing business environment. The Principles are:

1. Value and performance are created in company combined asset-based and function-based organisation;

2. The organisational entities have clear responsibilities and two distinctly defined roles; the line role and the support role;

3. Responsibilities and authorities are established through the process of delegation to the line role, and through the assignment of tasks to support roles in delivery entities;

4. A single point of accountability applies;

5. The line role has primacy, and acts in accordance with the management system.

3-3-Statoil Arenas:

The purpose of the arenas is to provide quality and consistency across the organisation before important decisions are made. Three arenas support quality in decision-making within their particular specialist skills:

- Information Technology arena
- technology arena
- investment arena

●**The information technology arena** ensures that the portfolio of major IT initiatives supports the company strategy and creates ownership across the group. The arena must consider the consequences and risks of the company by providing their comments to the IT portfolio and the financial targets set.

●**The technology arena** endorses the technology development and implementation portfolio on a continuous basis, including funding, for line management approval. The technology arena ensures that the portfolio is clear, founded in the corporate technology strategy, supported by management and that ownership exists across the group.

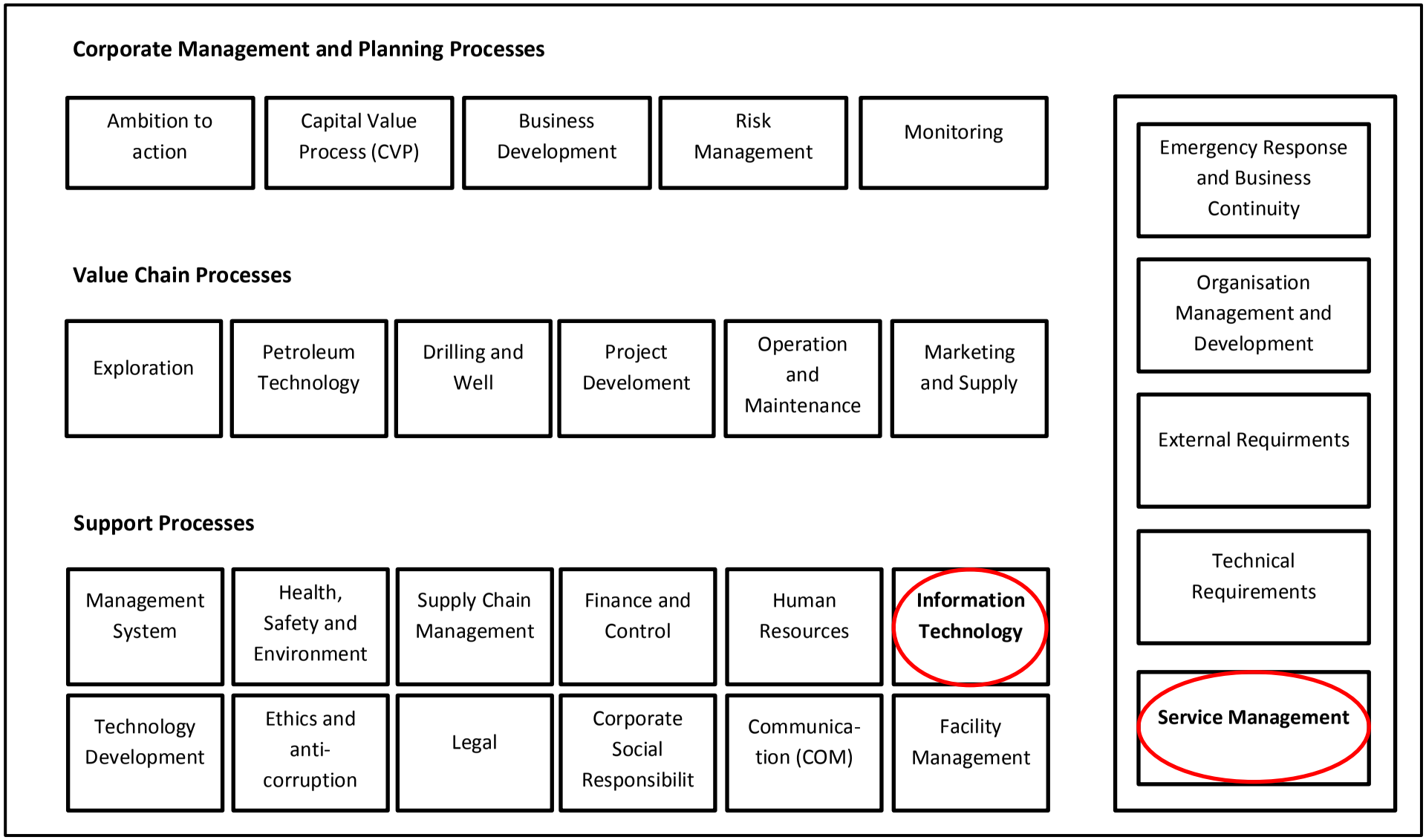
●**The investment arena** performs an independent technical and commercial review before passing decision gates on exploration projects, on acquisitions and divestments involving a major commitment, and where there is significant risk or exposure. Investment arena reviews are mandatory for investment decisions, for acquisitions and divestments requiring approval by the chief executive, and for exploration decisions requiring approval by the exploration executive. A copy of the conclusion of the investment arena review shall be included in the final decision document.[5]

3-4-Statoil Business Process Model:

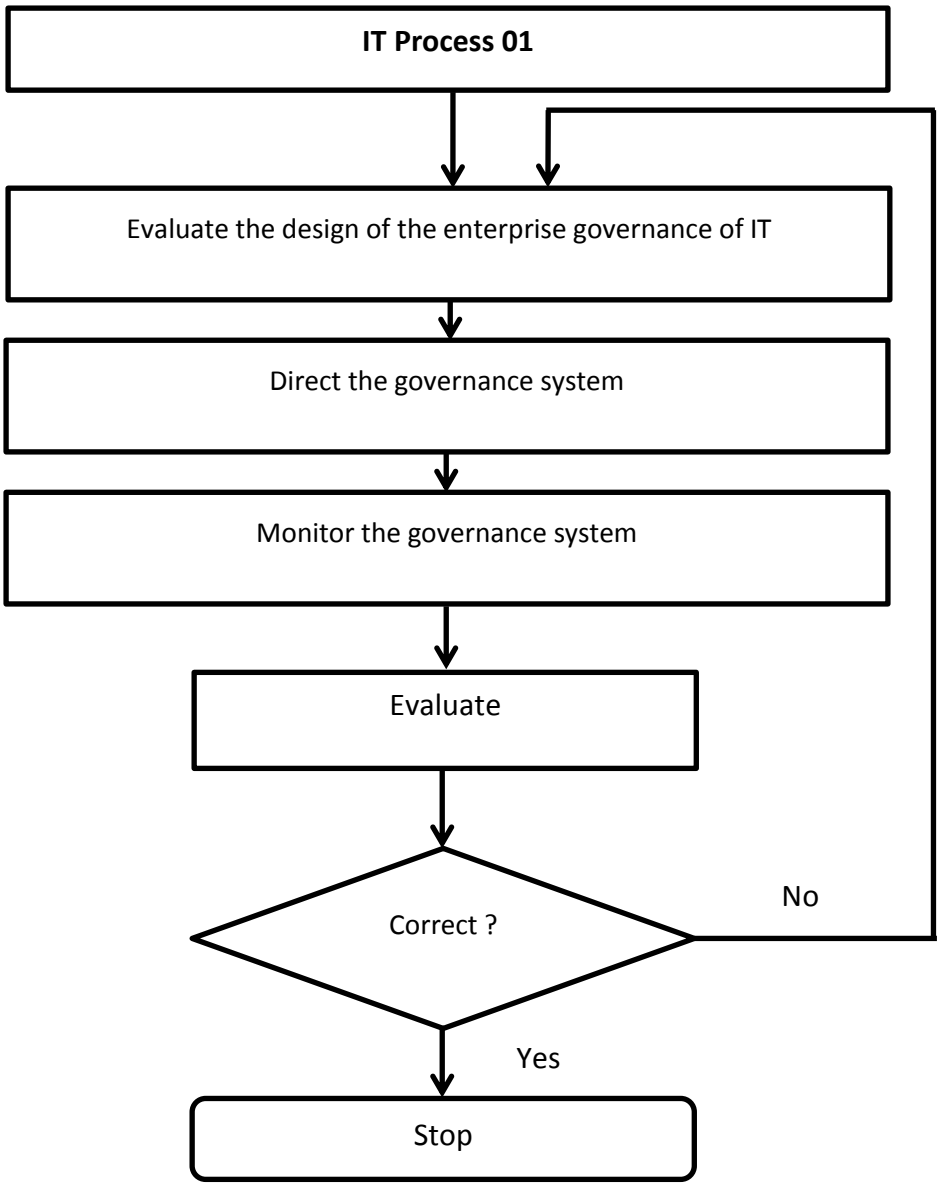
Statoil Business Process Model (BPM) consists of a set of core processes, and a set of support processes (**Figure 3-3**). The **core processes** include all processes regarding Statoil oil and gas. This chain embodies all processes regarding exploration, drilling, plant operation, marketing and supply of oil, including relating project management technology processes. It follows the oil from the ground to the gas stations. The **support processes** include all other functionalities of Statoil that help support and maintain the daily operation. the Information Technology process which contains business processes for how to operate IT within Statoil or the Legal process which deals with all legal sub-processes.

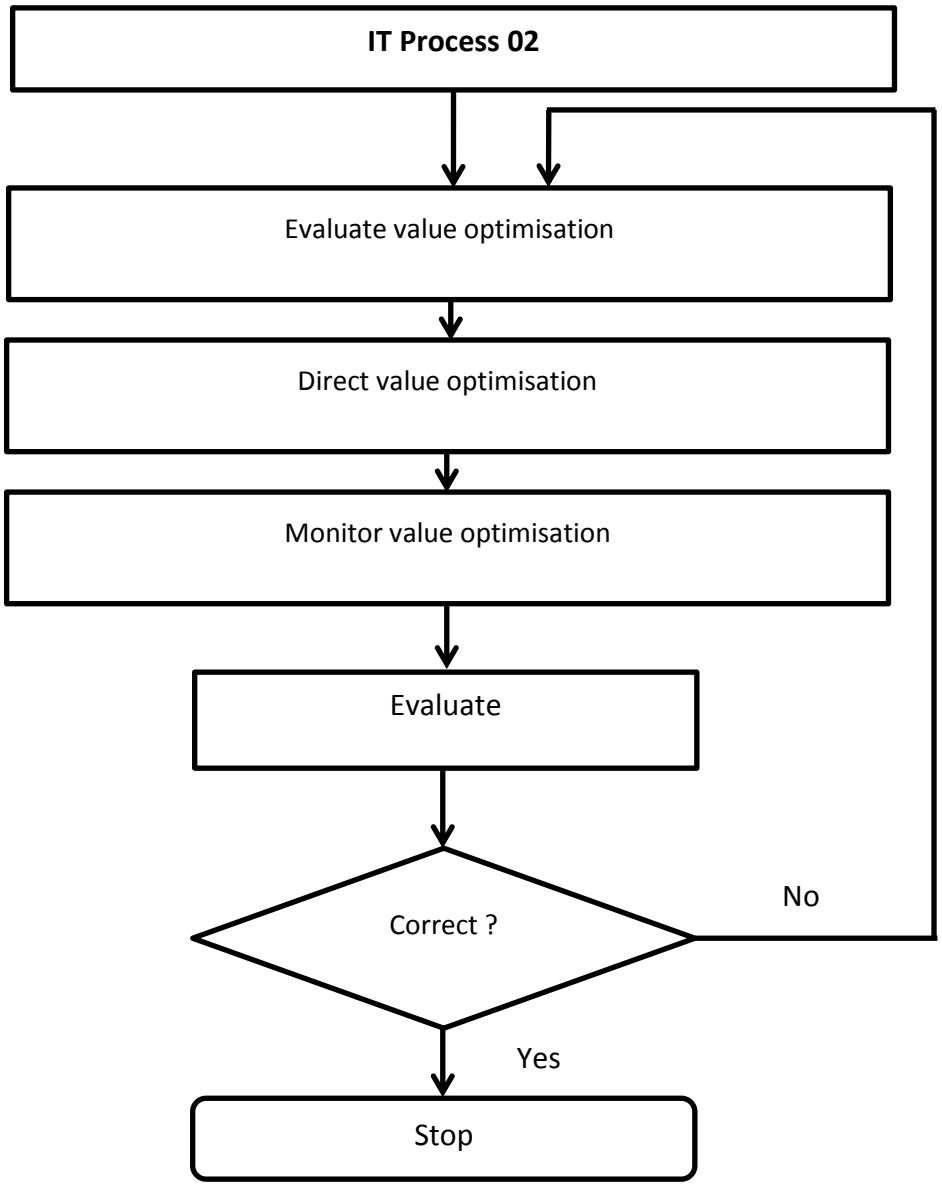
[5] The Statoil Book. 2013. version 3.1

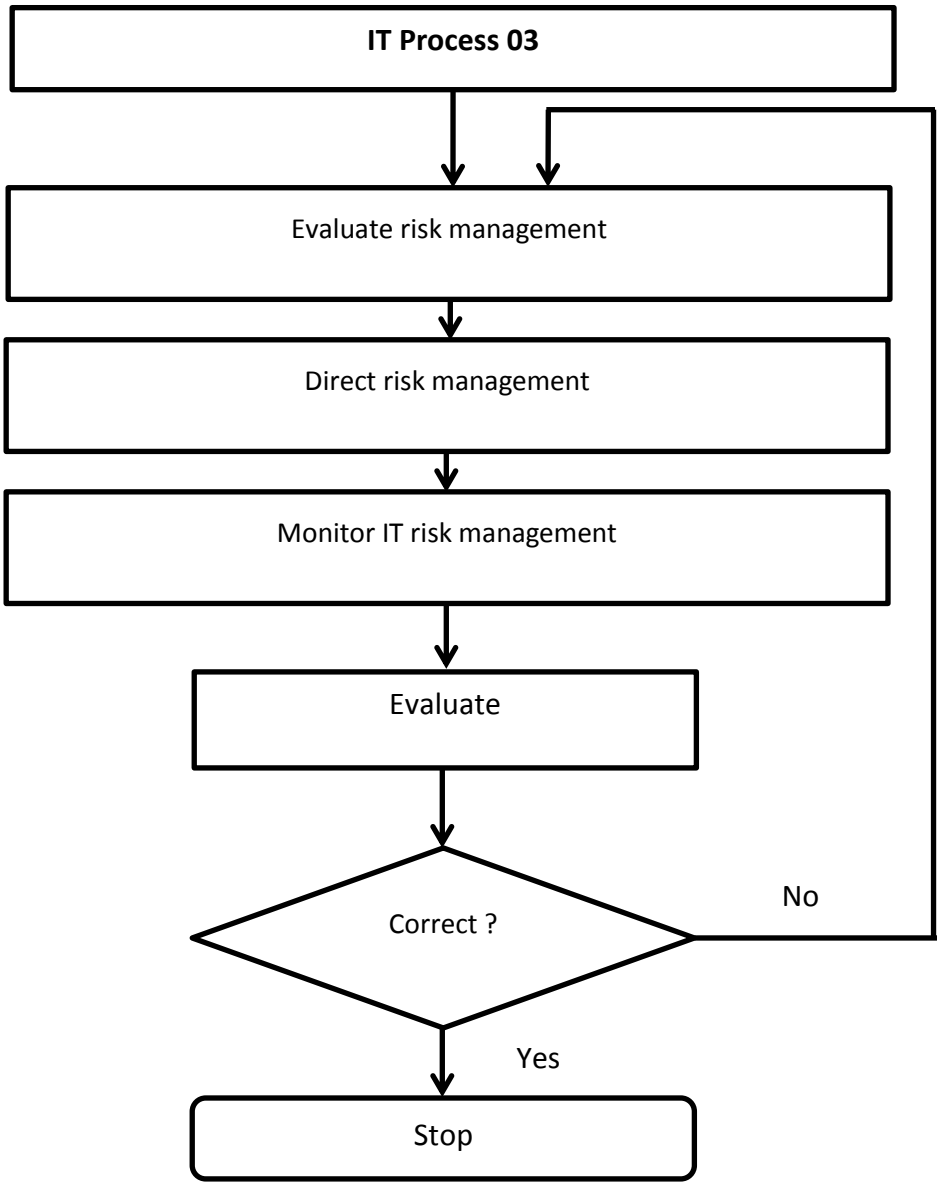
Figure 3-3 : Statoil Business Process Model

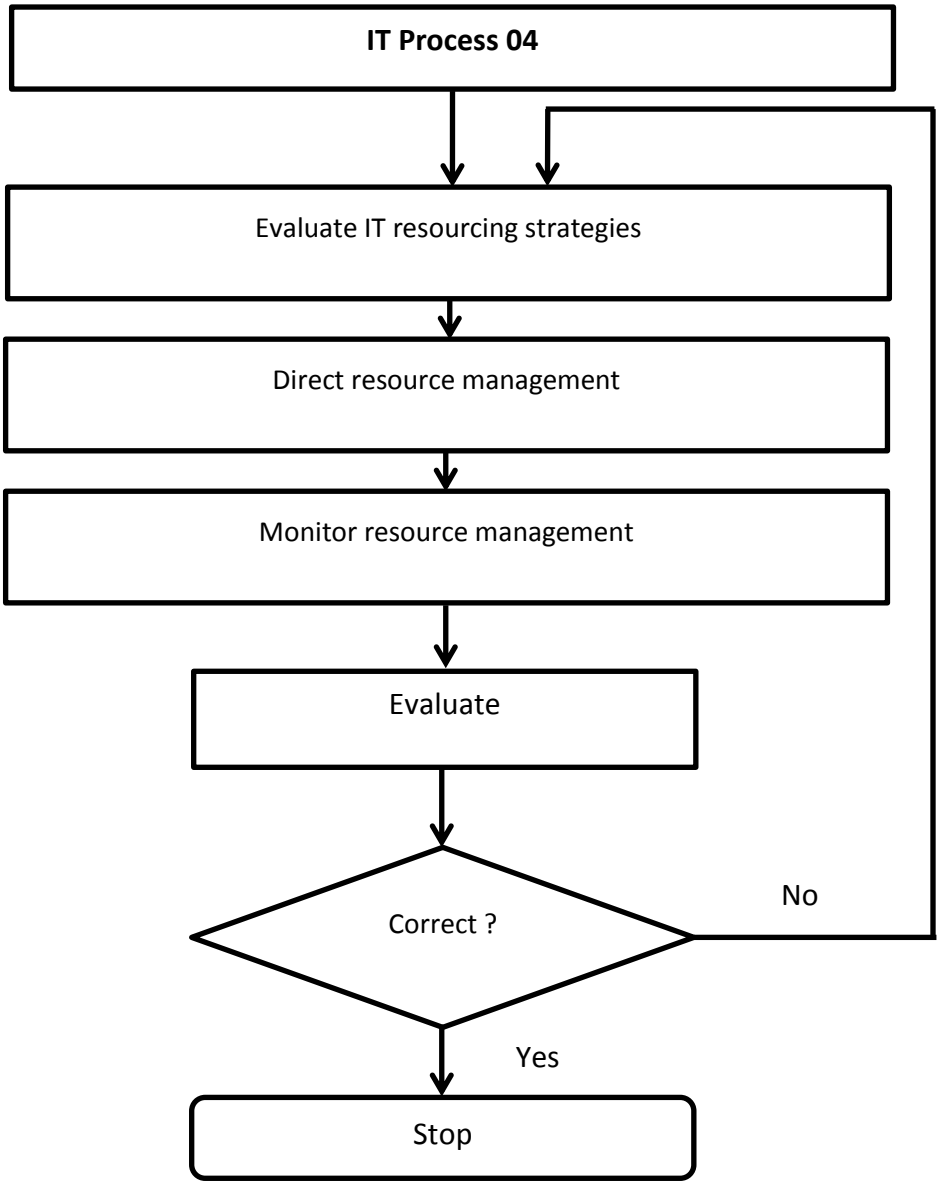


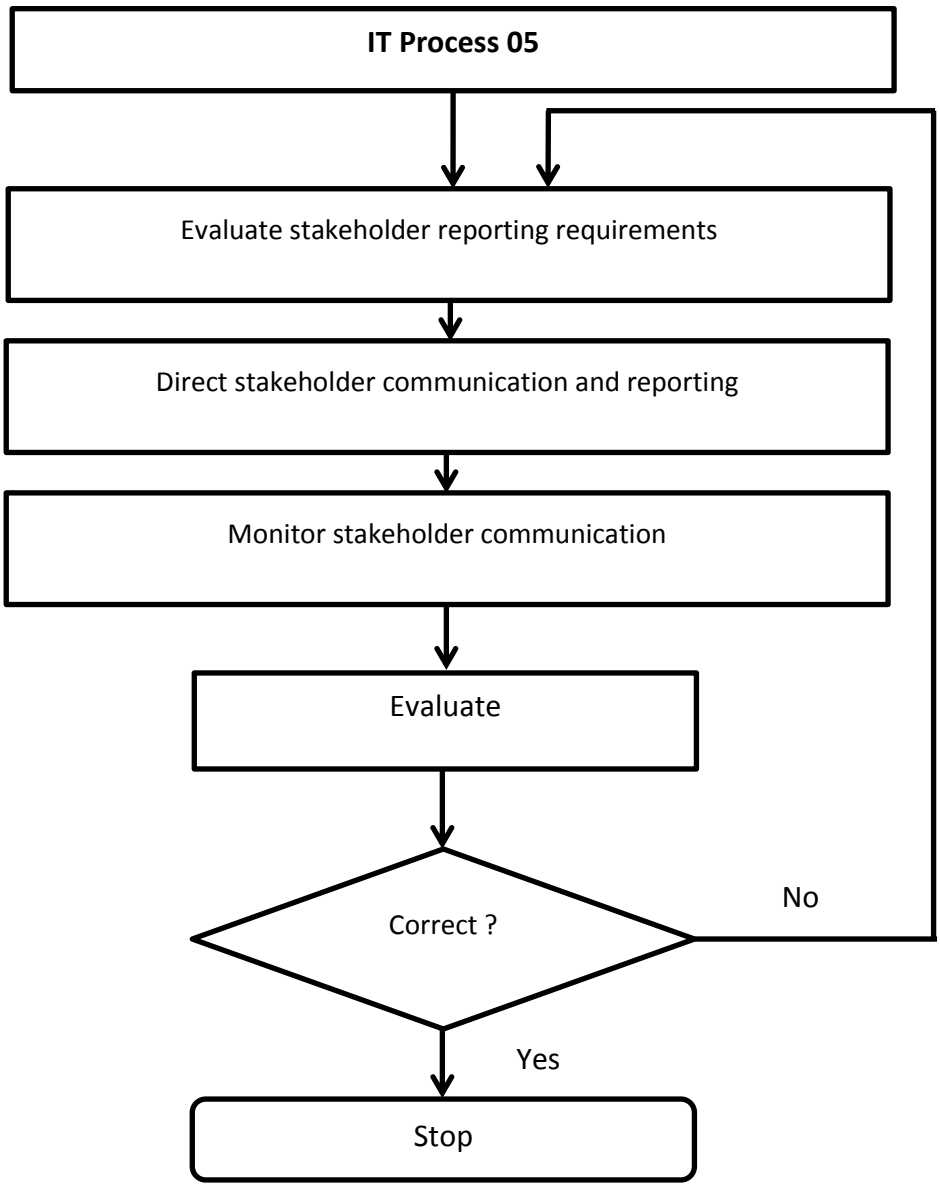
Each process is divided into a map of lower-level processes. This study will exemplify with the Information Technology process, as this is the most relevant. The following figures display the general logic discovered by the study for the lower level processes of the Information Technology support process displayed in **Figure 3-3**.

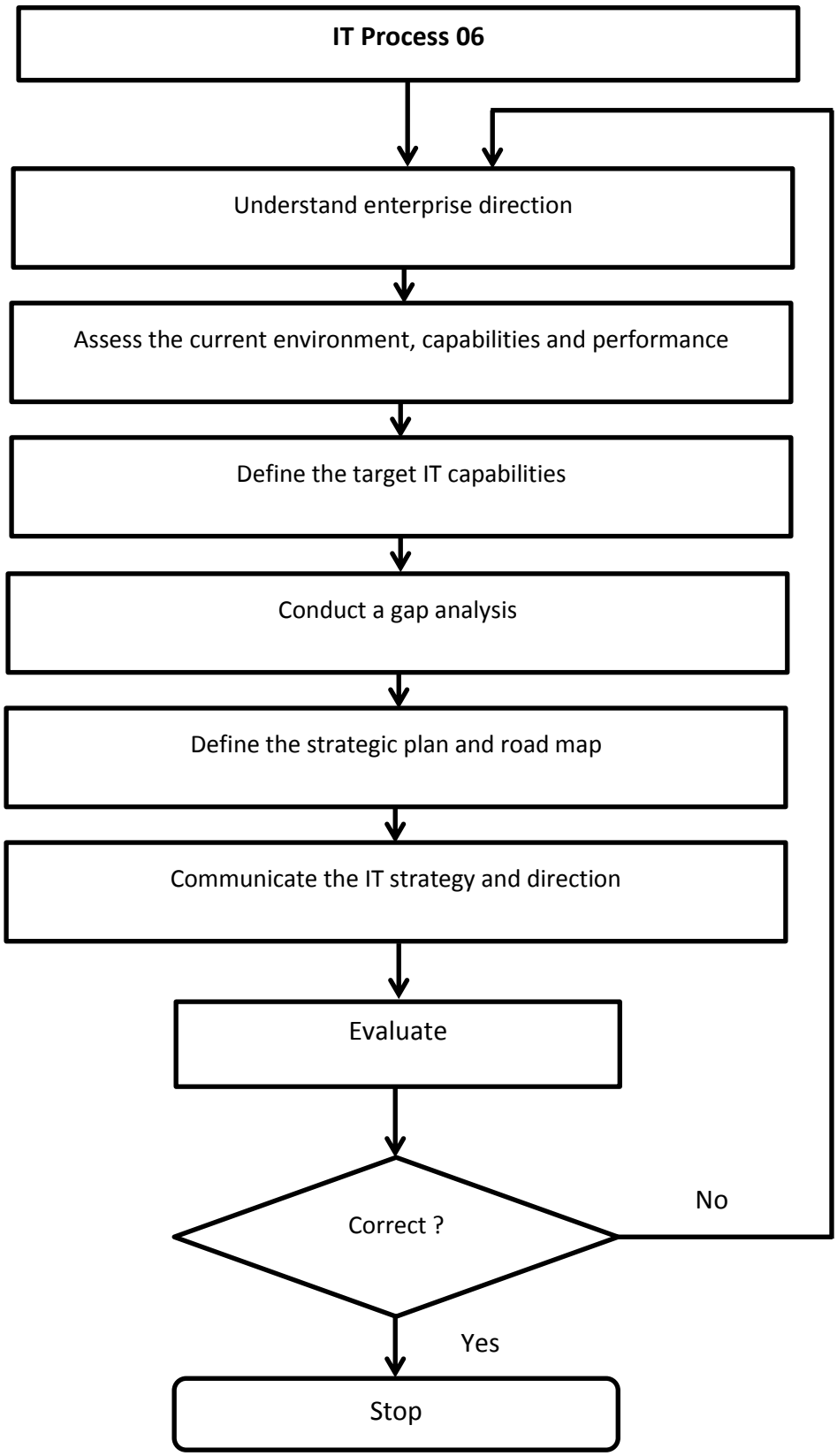


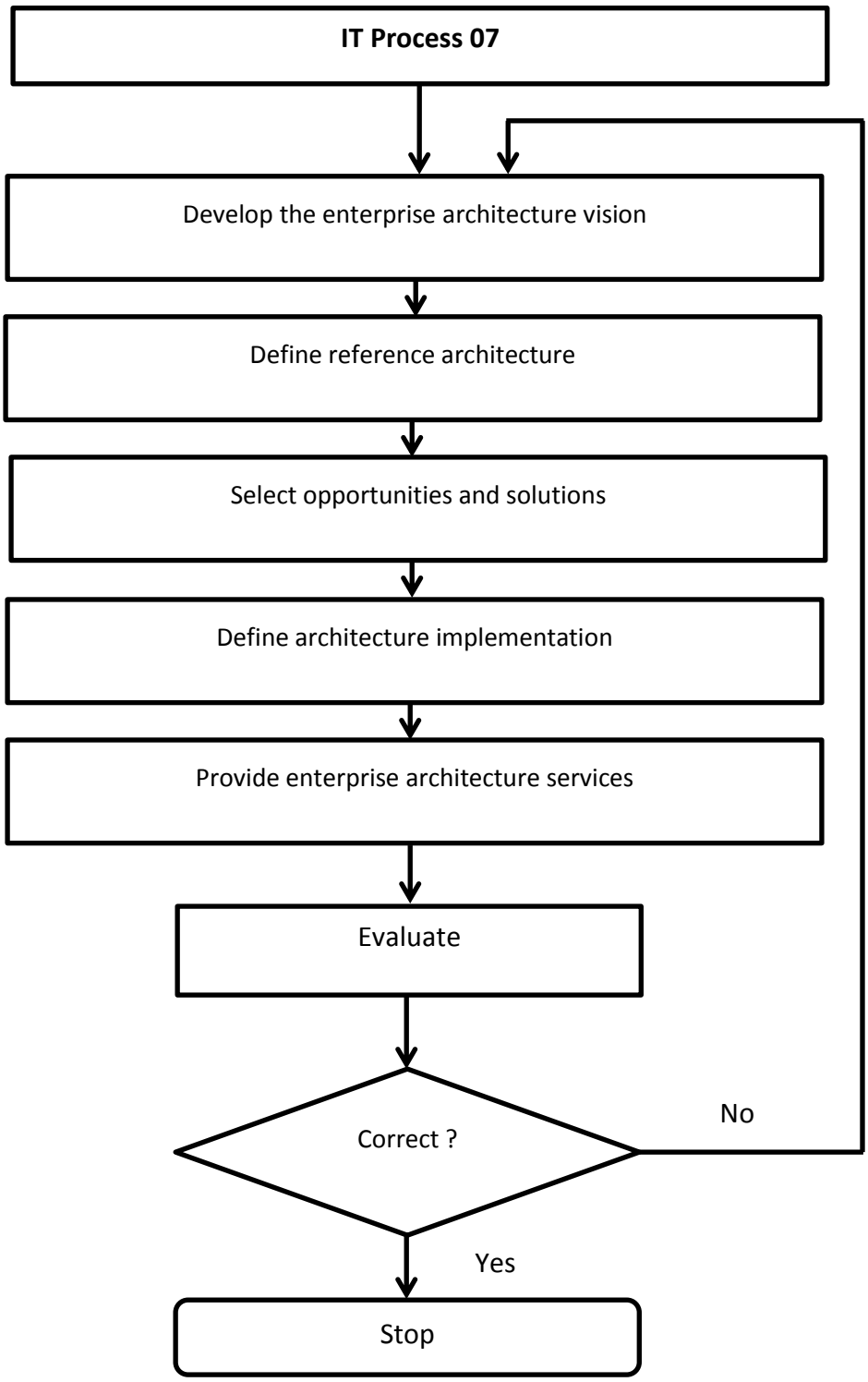

IT Process 02
Evaluate value optimisation
Direct value optimisation
Monitor value optimisation
Evaluate
Correct ?
No
Yes
Stop

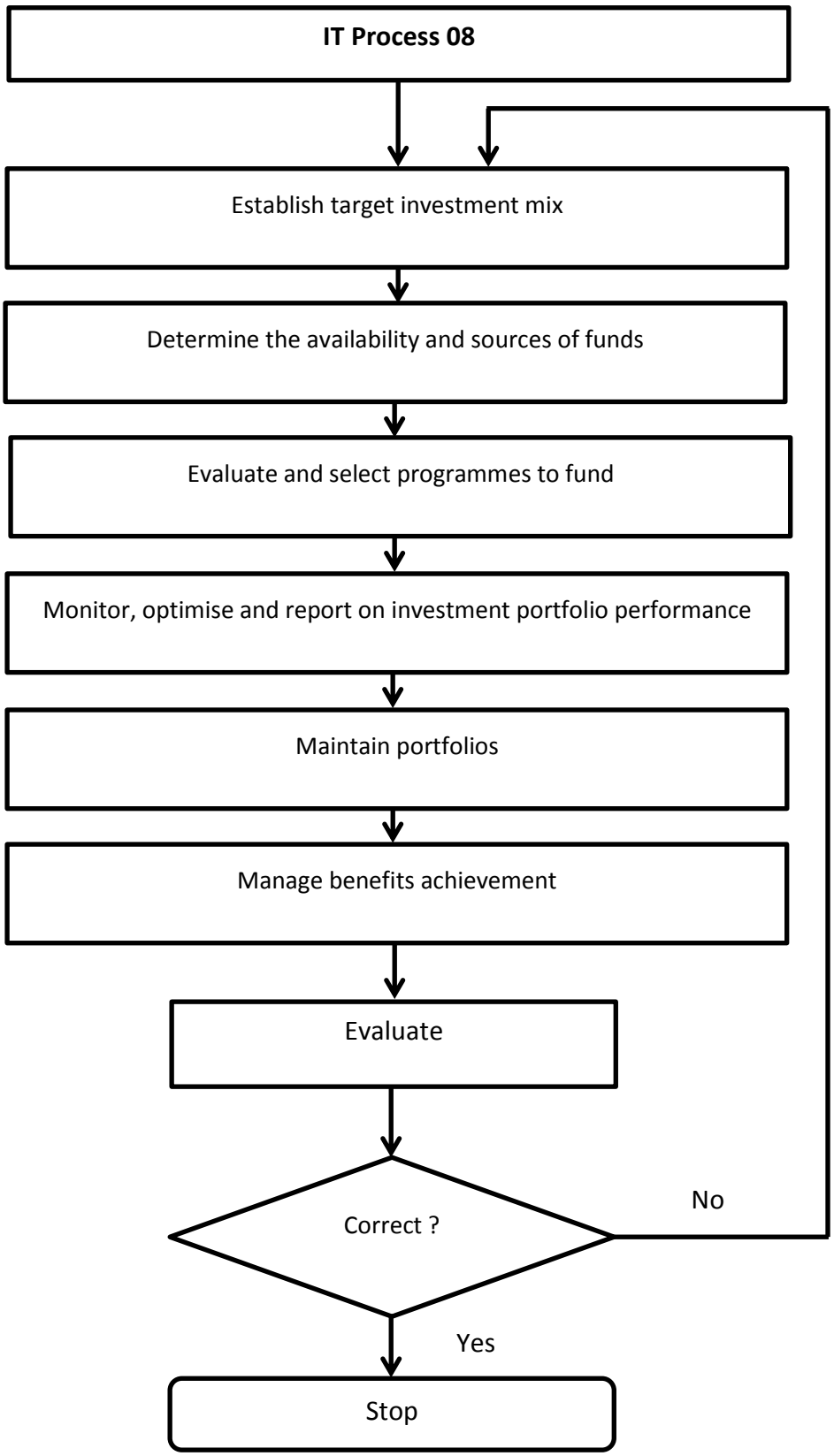

IT Process 03
Evaluate risk management
Direct risk management
Monitor IT risk management
Evaluate
Correct ?
No
Yes
Stop

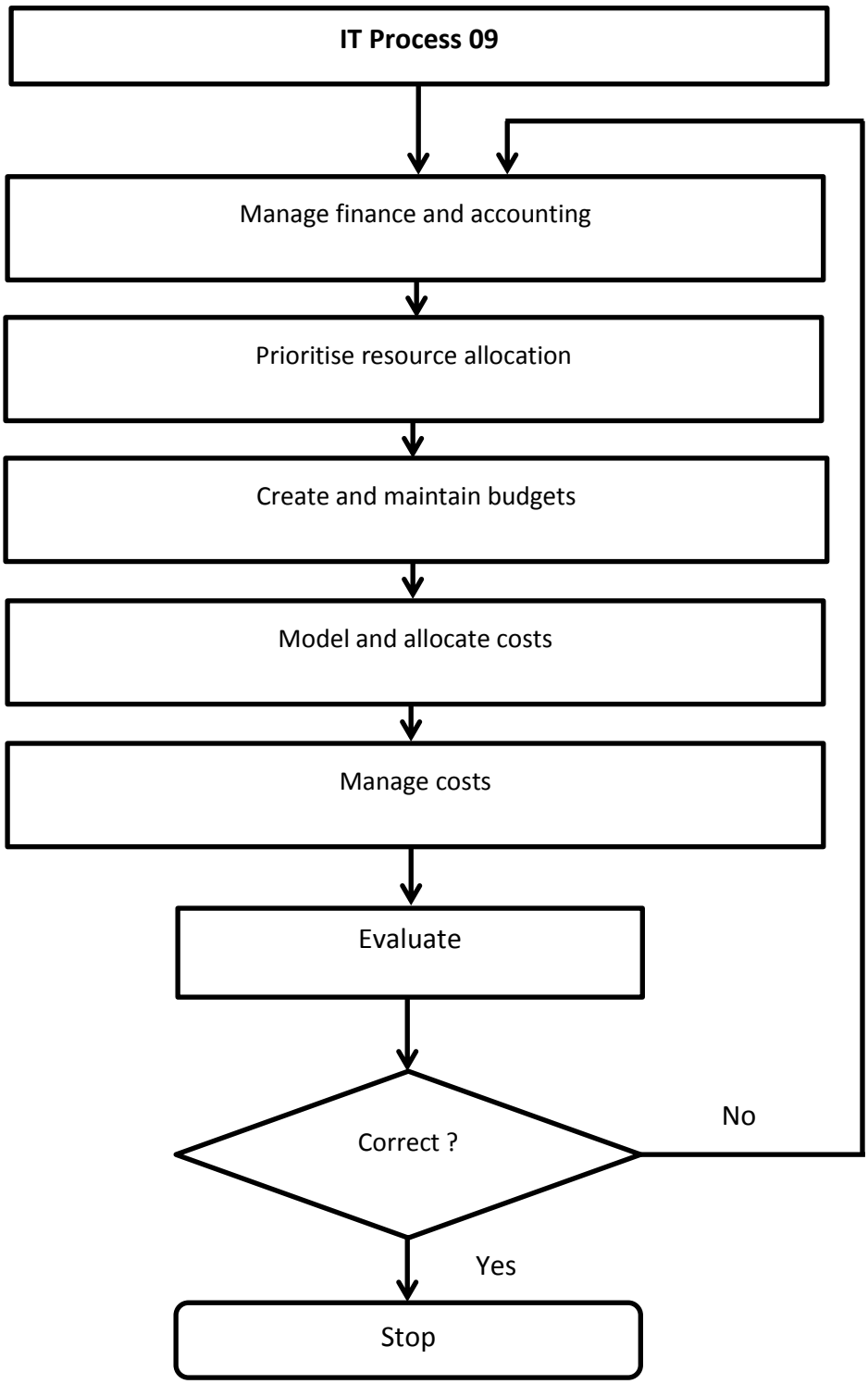

IT Process 04
Evaluate IT resourcing strategies
Direct resource management
Monitor resource management
Evaluate
Correct ?
No
Yes
Stop

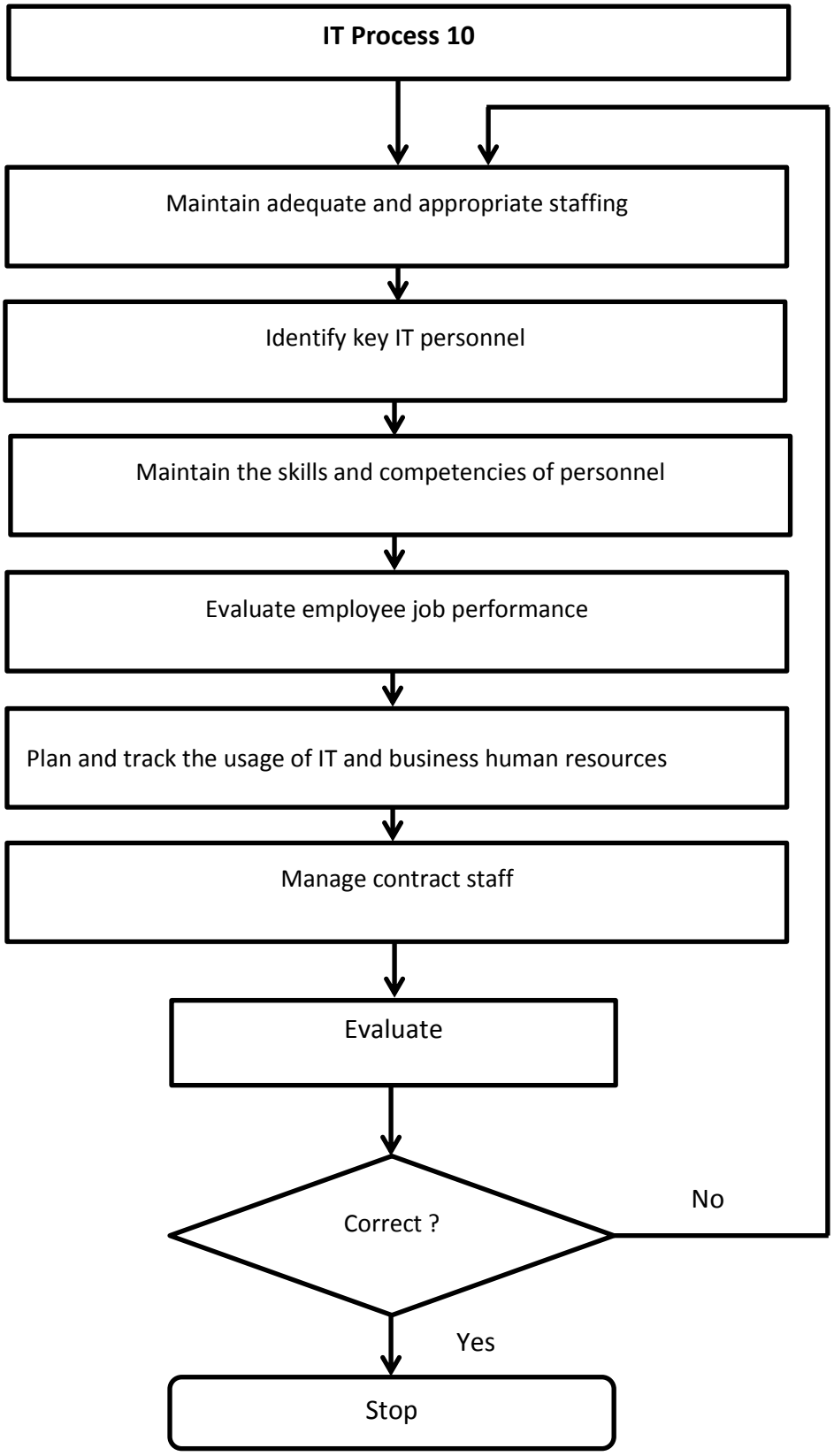

IT Process 05
Evaluate stakeholder reporting requirements
Direct stakeholder communication and reporting
Monitor stakeholder communication
Evaluate
Correct ?
No
Yes
Stop

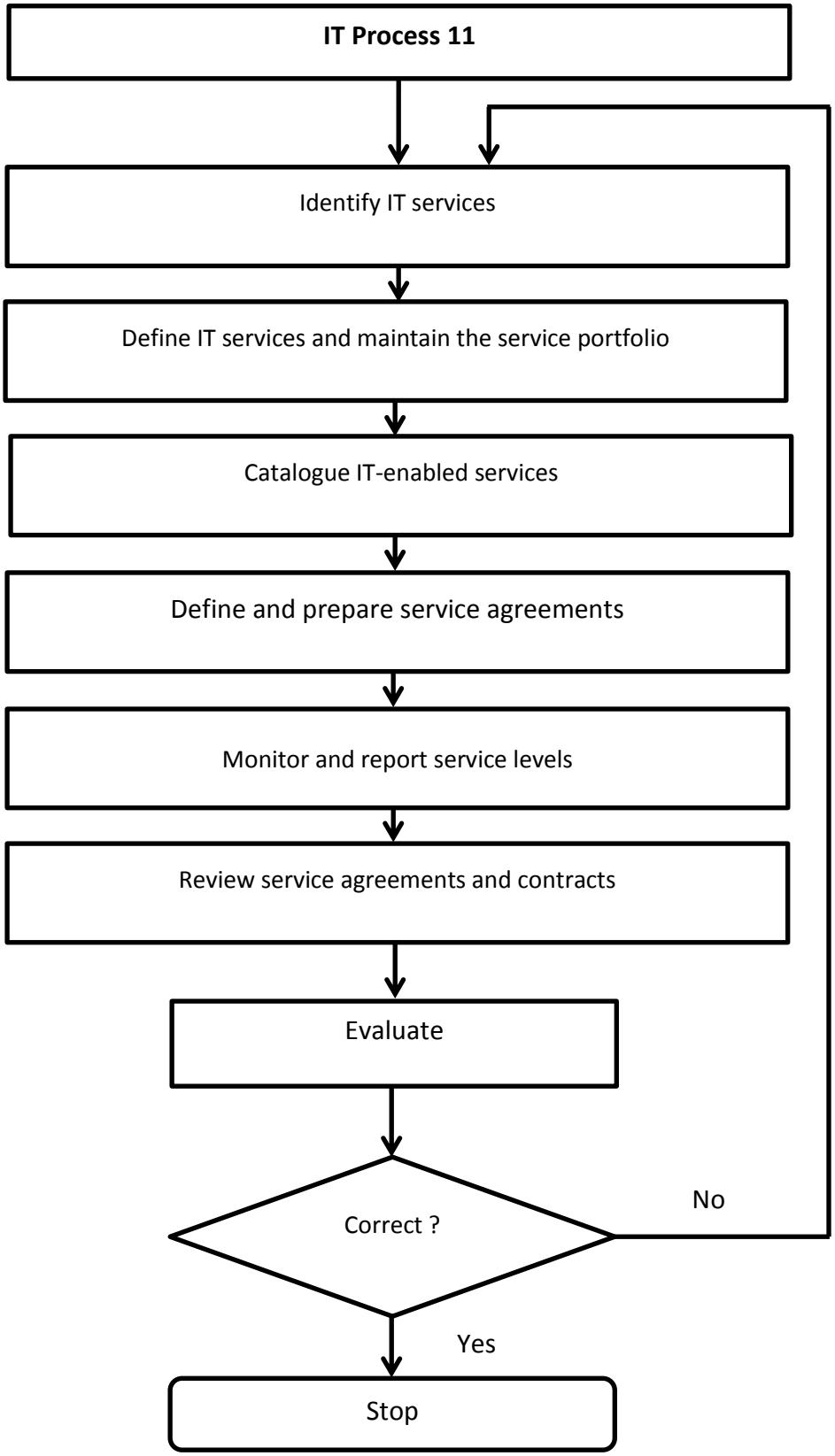

IT Process 06
Understand enterprise direction
Assess the current environment, capabilities and performance
Define the target IT capabilities
Conduct a gap analysis
Define the strategic plan and road map
Communicate the IT strategy and direction
Evaluate
Correct ?
No
Yes
Stop

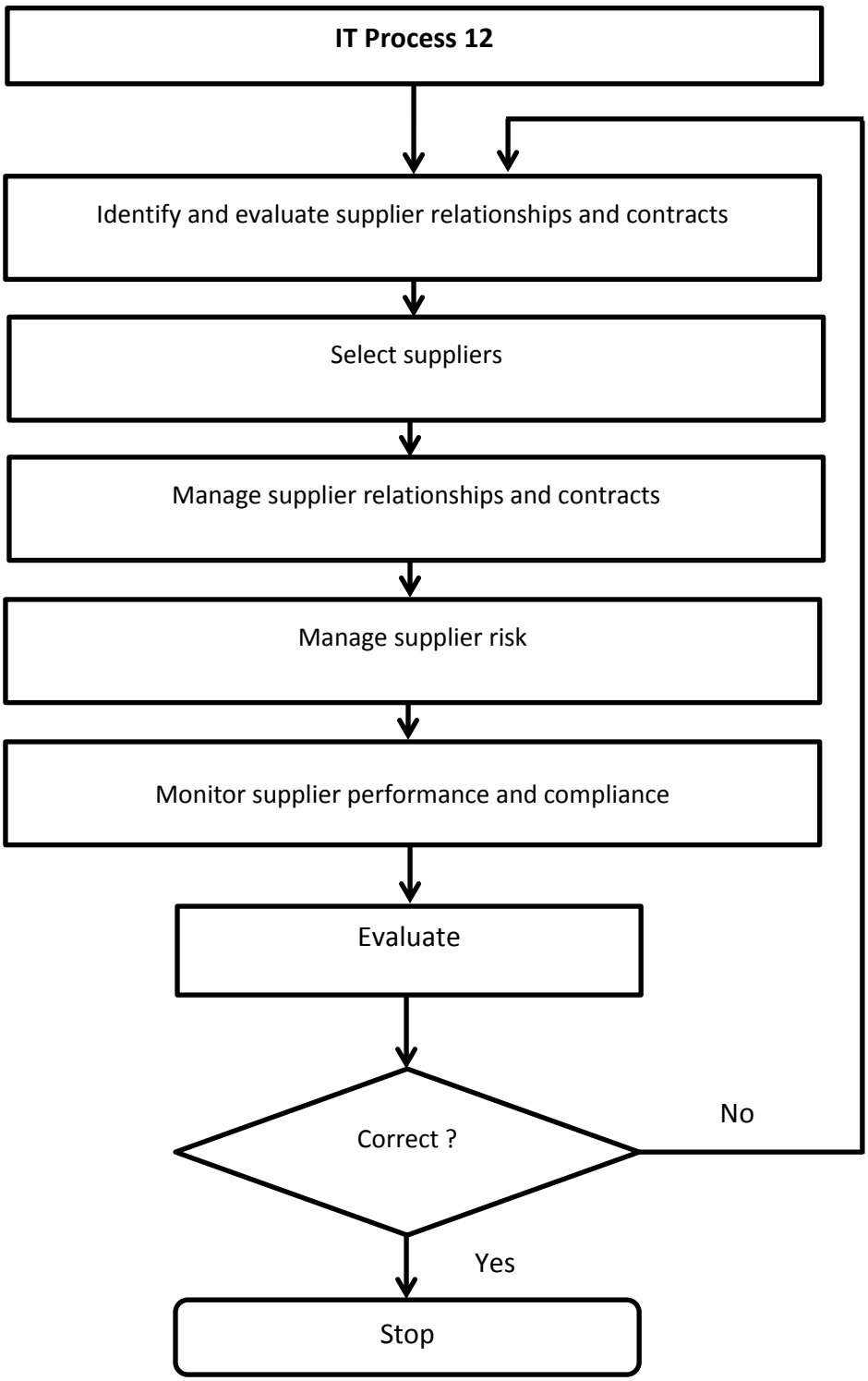

IT Process 07
Develop the enterprise architecture vision
Define reference architecture
Select opportunities and solutions
Define architecture implementation
Provide enterprise architecture services
Evaluate
Correct ?
No
Yes
Stop

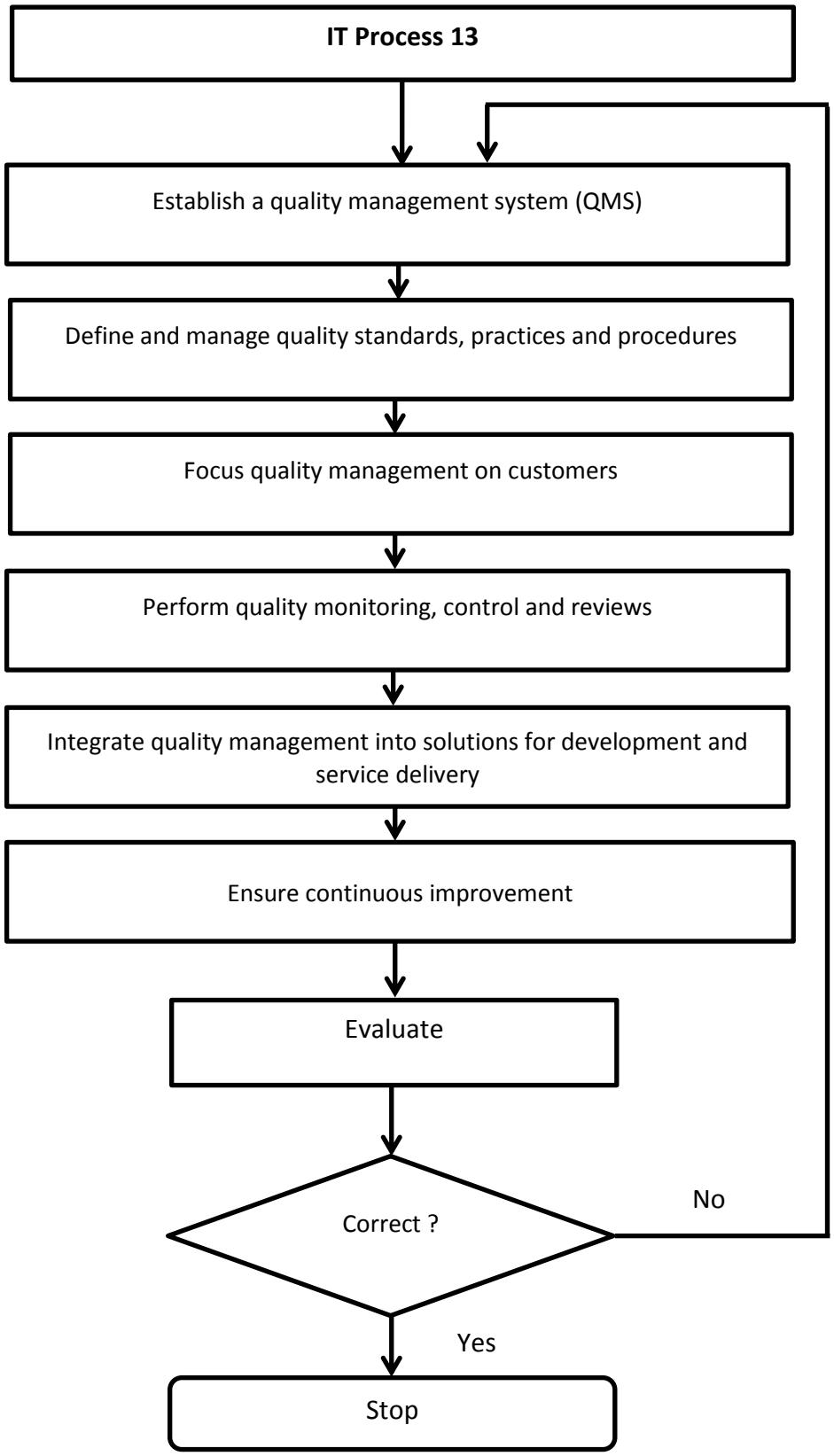

IT Process 08
Establish target investment mix
Determine the availability and sources of funds
Evaluate and select programmes to fund
Monitor, optimise and report on investment portfolio performance
Maintain portfolios
Manage benefits achievement
Evaluate
Correct ?
No
Yes
Stop

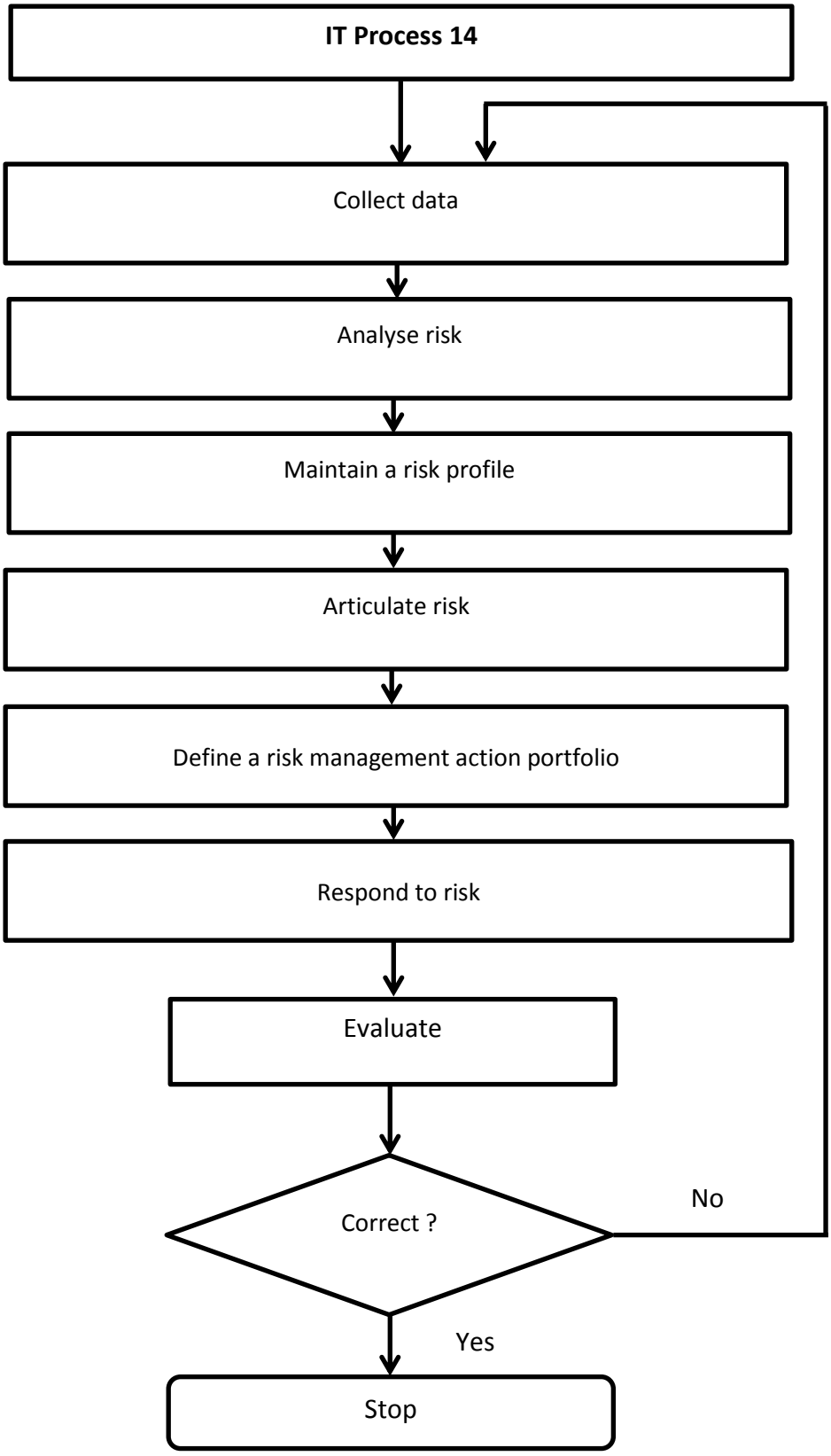

IT Process 09
Manage finance and accounting
Prioritise resource allocation
Create and maintain budgets
Model and allocate costs
Manage costs
Evaluate
Correct ?
No
Yes
Stop

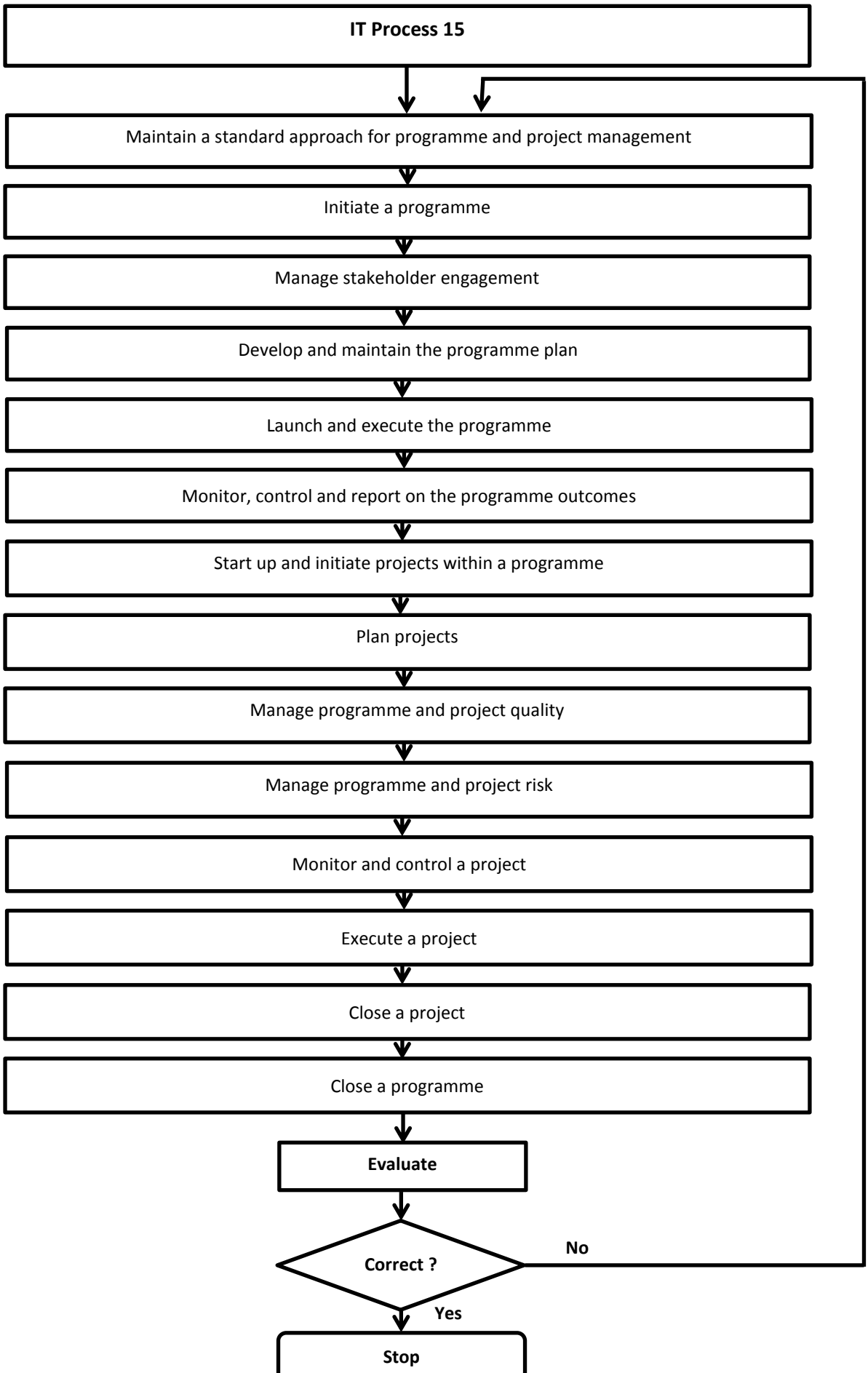

IT Process 10
Maintain adequate and appropriate staffing
Identify key IT personnel
Maintain the skills and competencies of personnel
Evaluate employee job performance
Plan and track the usage of IT and business human resources
Manage contract staff
Evaluate
Correct ?
No
Yes
Stop

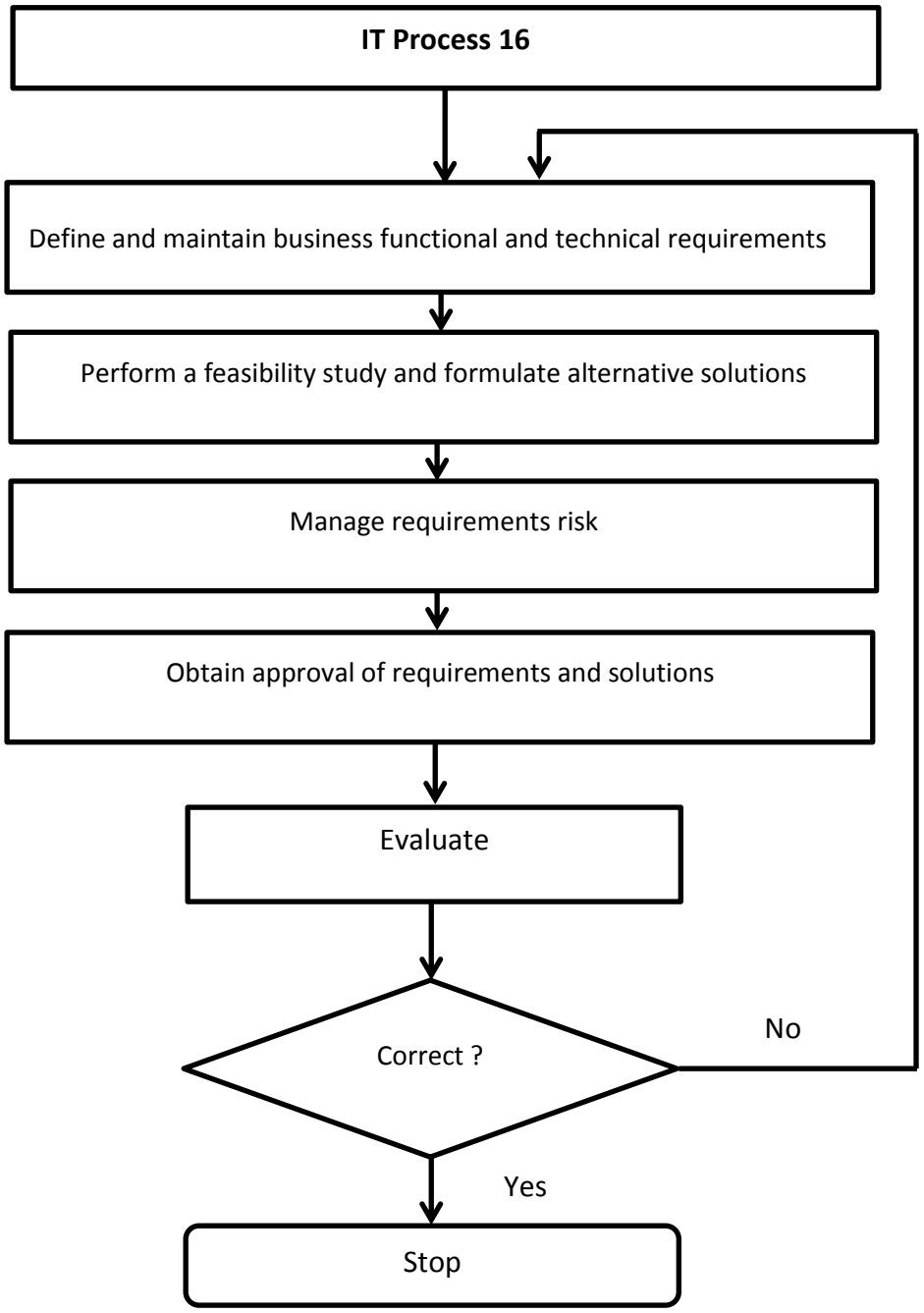

IT Process 11
Identify IT services
Define IT services and maintain the service portfolio
Catalogue IT-enabled services
Define and prepare service agreements
Monitor and report service levels
Review service agreements and contracts
Evaluate
Correct ?
No
Yes
Stop

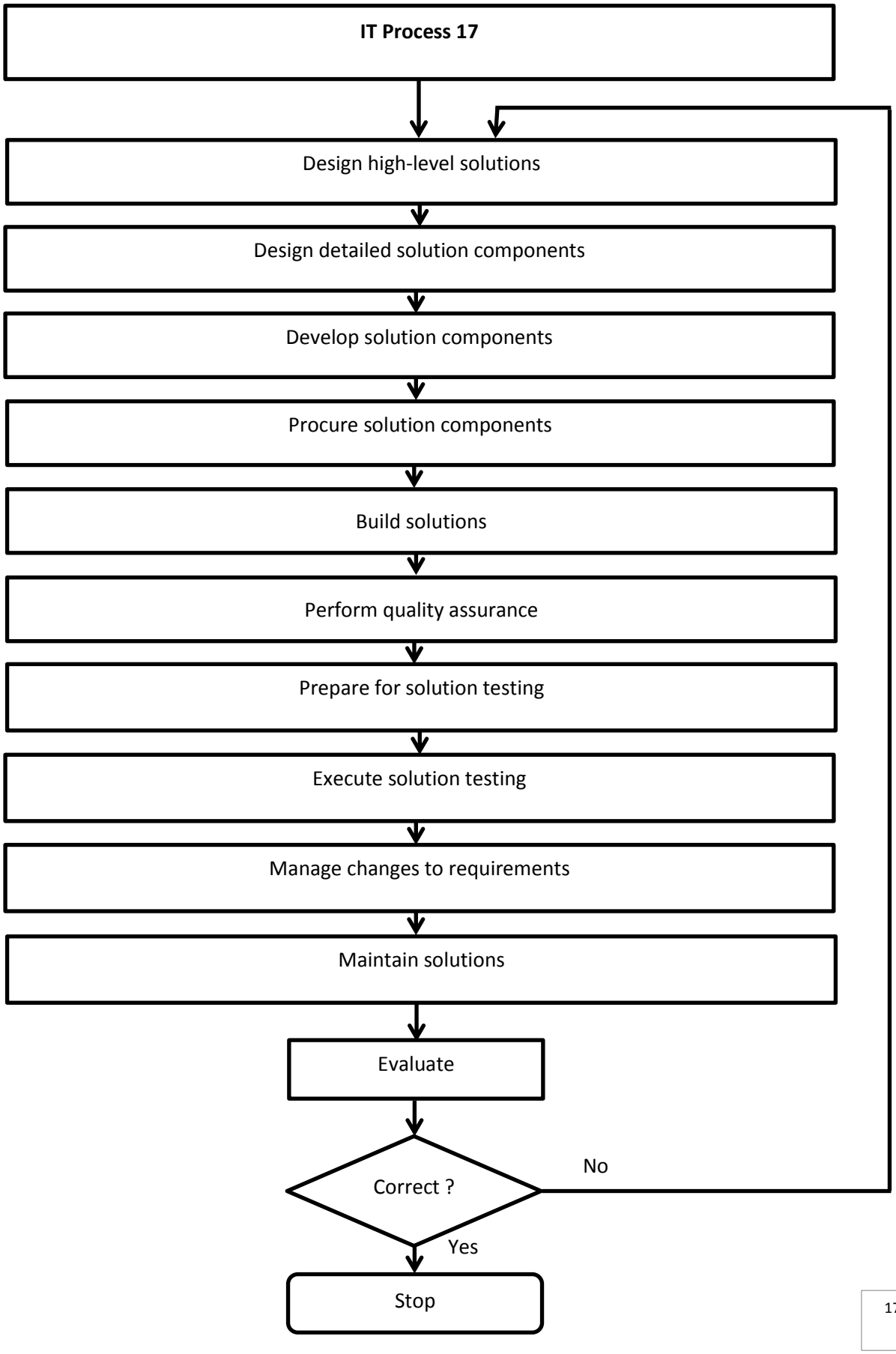

IT Process 12
Identify and evaluate supplier relationships and contracts
Select suppliers
Manage supplier relationships and contracts
Manage supplier risk
Monitor supplier performance and compliance
Evaluate
Correct ?
No
Yes
Stop

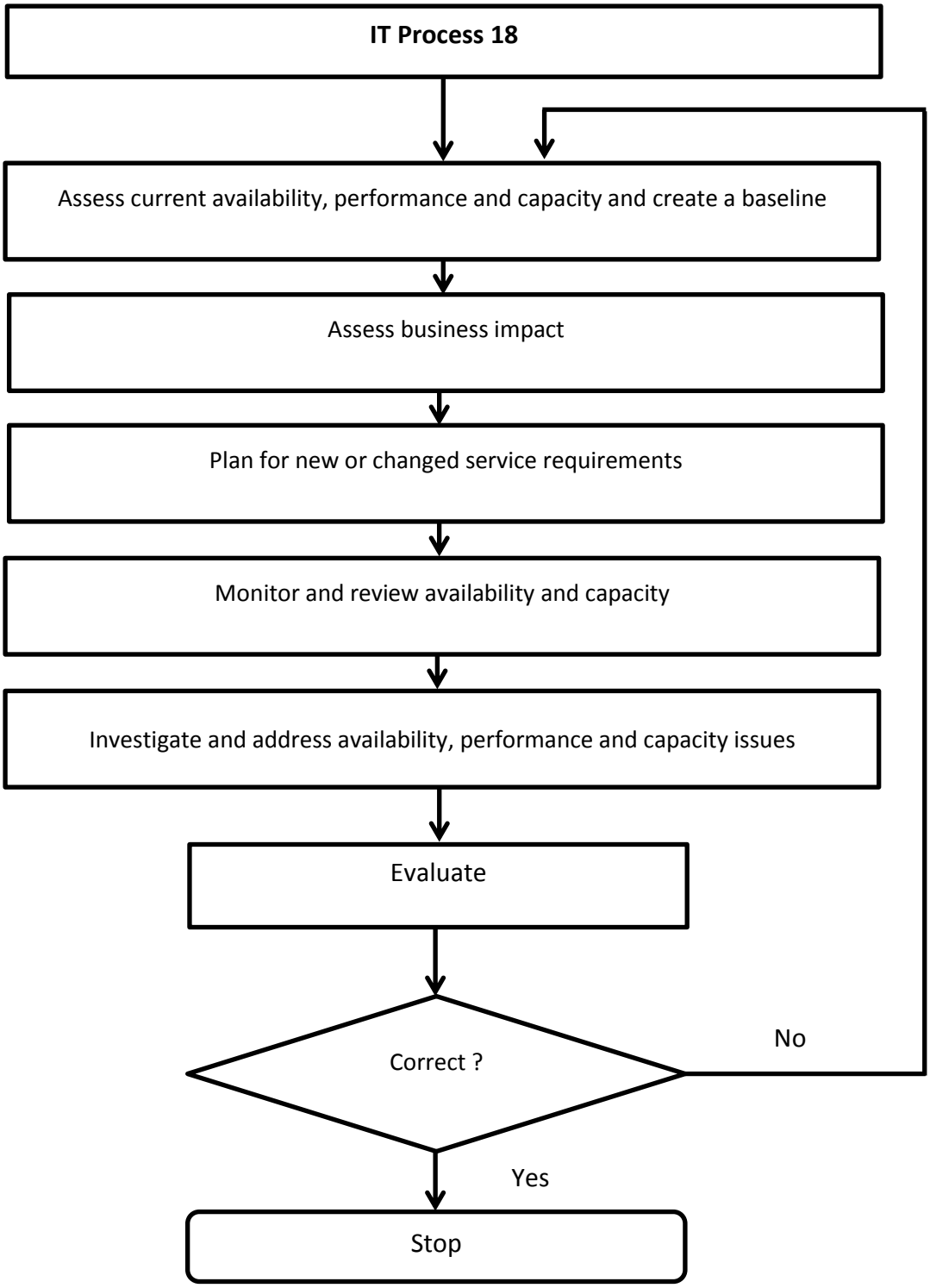

IT Process 13
Establish a quality management system (QMS)
Define and manage quality standards, practices and procedures
Focus quality management on customers
Perform quality monitoring, control and reviews
Integrate quality management into solutions for development and service delivery
Ensure continuous improvement
Evaluate
Correct ?
No
Yes
Stop

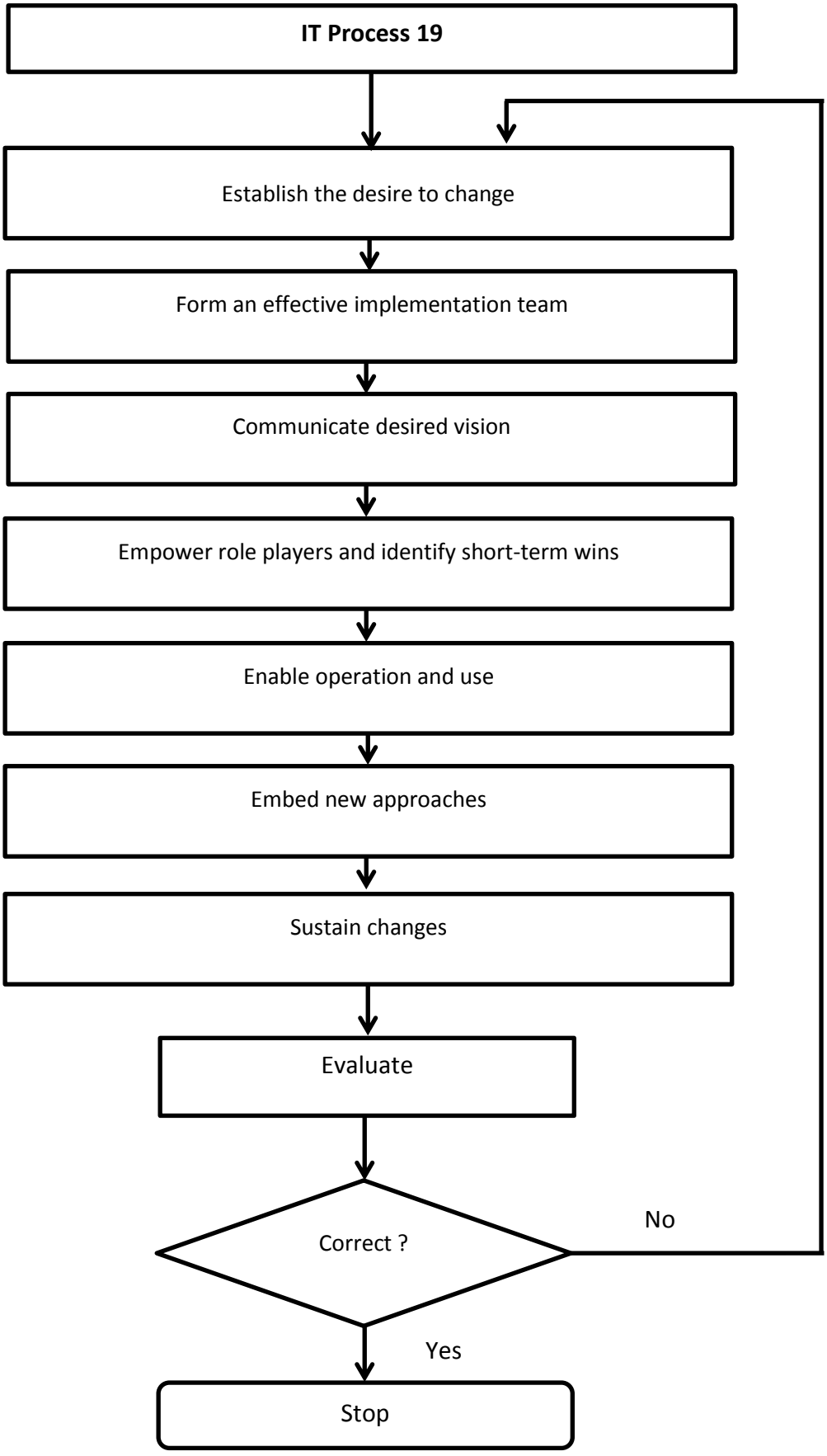

IT Process 14
Collect data
Analyse risk
Maintain a risk profile
Articulate risk
Define a risk management action portfolio
Respond to risk
Evaluate
Correct ?
No
Yes
Stop

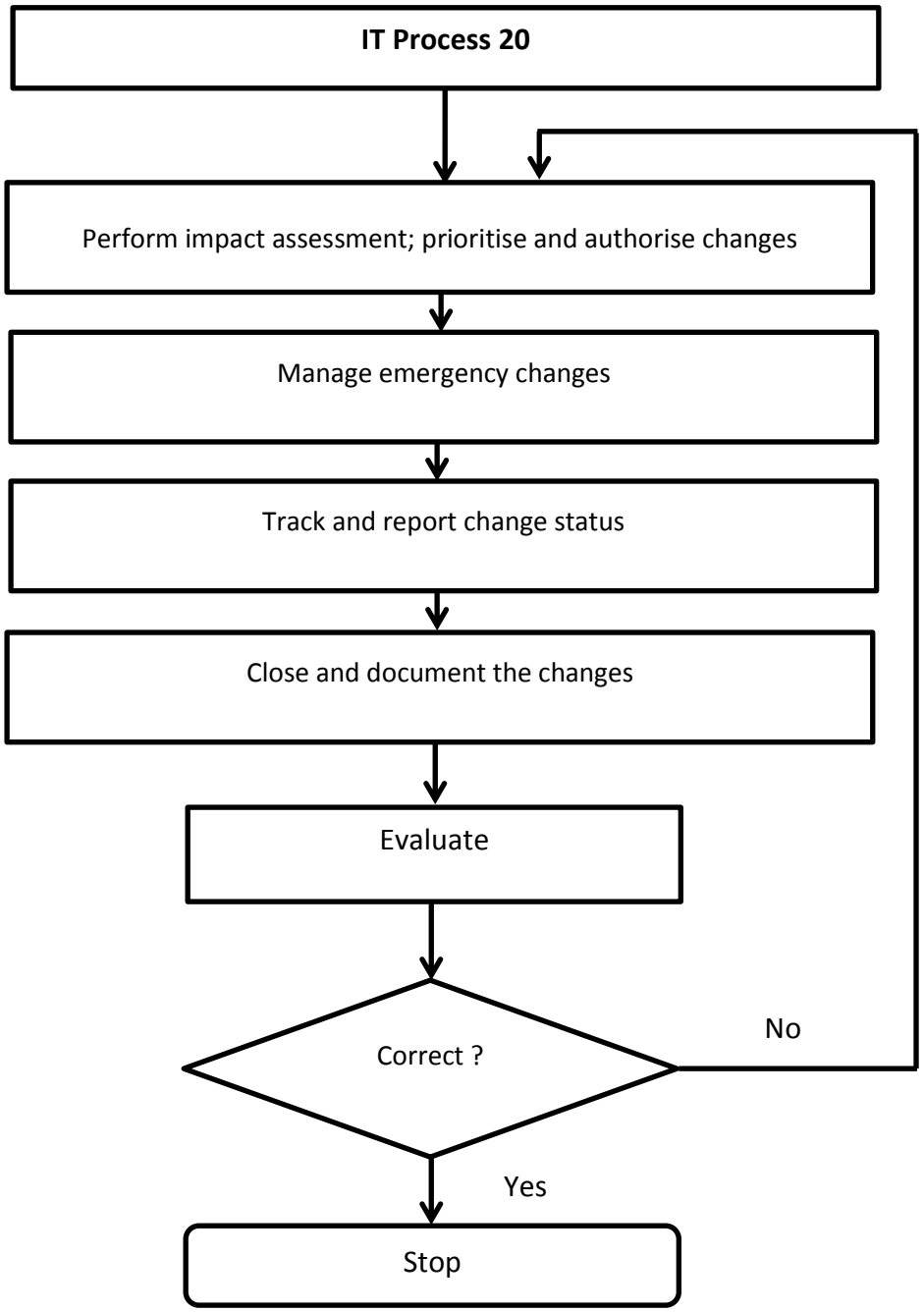

IT Process 15
Maintain a standard approach for programme and project management
Initiate a programme
Manage stakeholder engagement
Develop and maintain the programme plan
Launch and execute the programme
Monitor, control and report on the programme outcomes
Start up and initiate projects within a programme
Plan projects
Manage programme and project quality
Manage programme and project risk
Monitor and control a project
Execute a project
Close a project
Close a programme
Evaluate
Correct ?
No
Yes
Stop

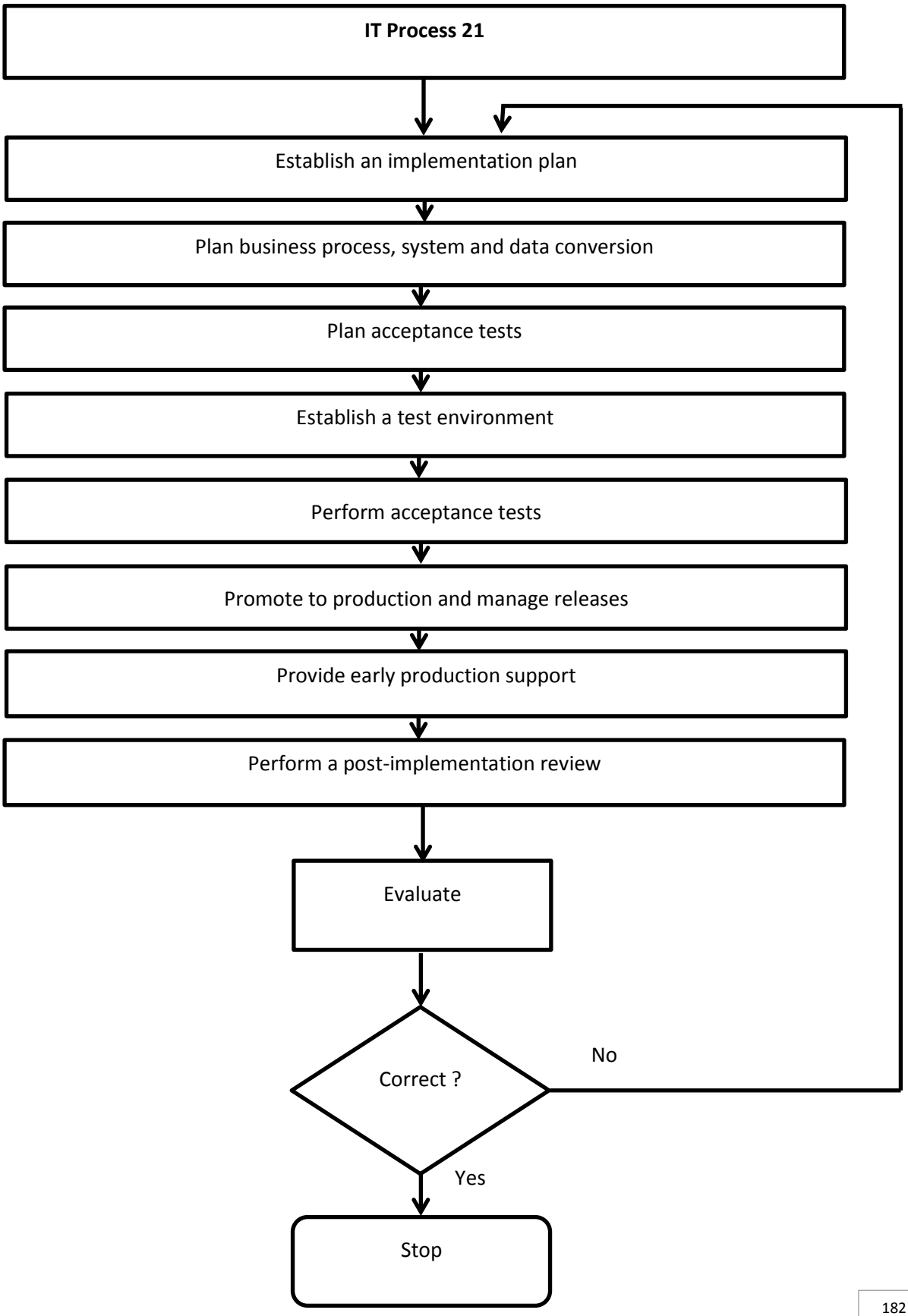

IT Process 16
Define and maintain business functional and technical requirements
Perform a feasibility study and formulate alternative solutions
Manage requirements risk
Obtain approval of requirements and solutions
Evaluate
Correct ?
No
Yes
Stop

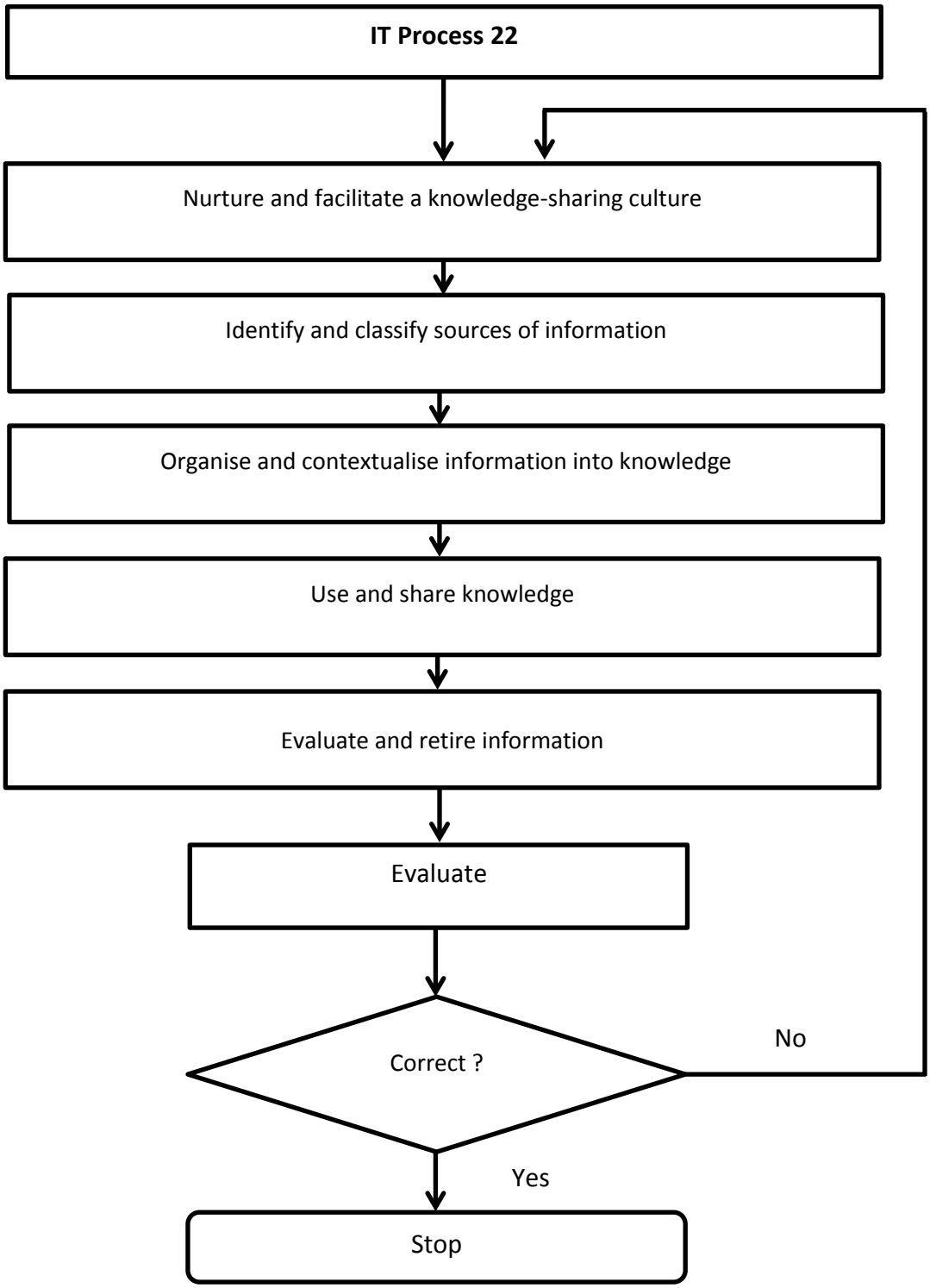

IT Process 17
Design high-level solutions
Design detailed solution components
Develop solution components
Procure solution components
Build solutions
Perform quality assurance
Prepare for solution testing
Execute solution testing
Manage changes to requirements
Maintain solutions
Evaluate
Correct ?
No
Yes
Stop

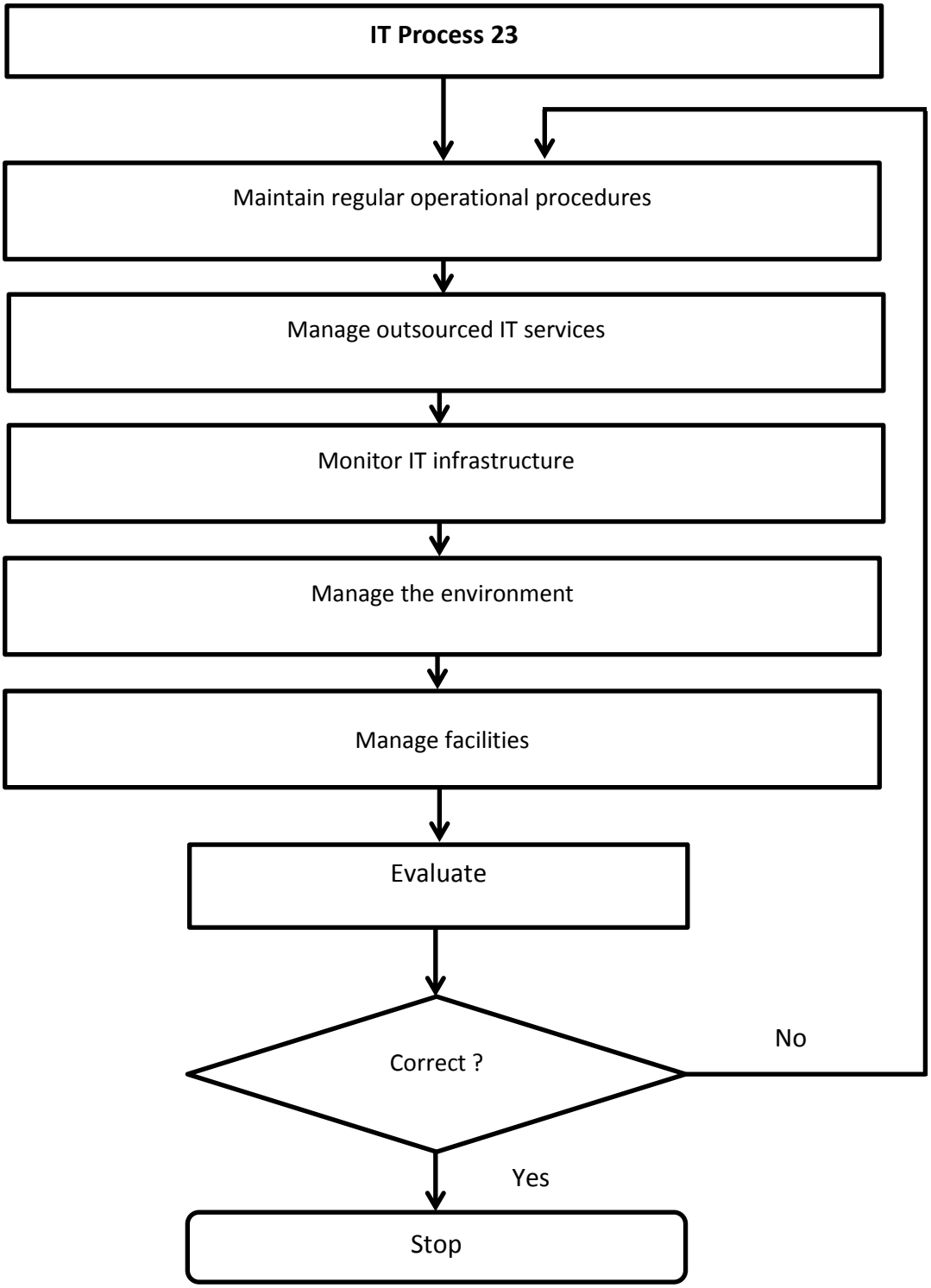

IT Process 18
Assess current availability, performance and capacity and create a baseline
Assess business impact
Plan for new or changed service requirements
Monitor and review availability and capacity
Investigate and address availability, performance and capacity issues
Evaluate
Correct ?
No
Yes
Stop

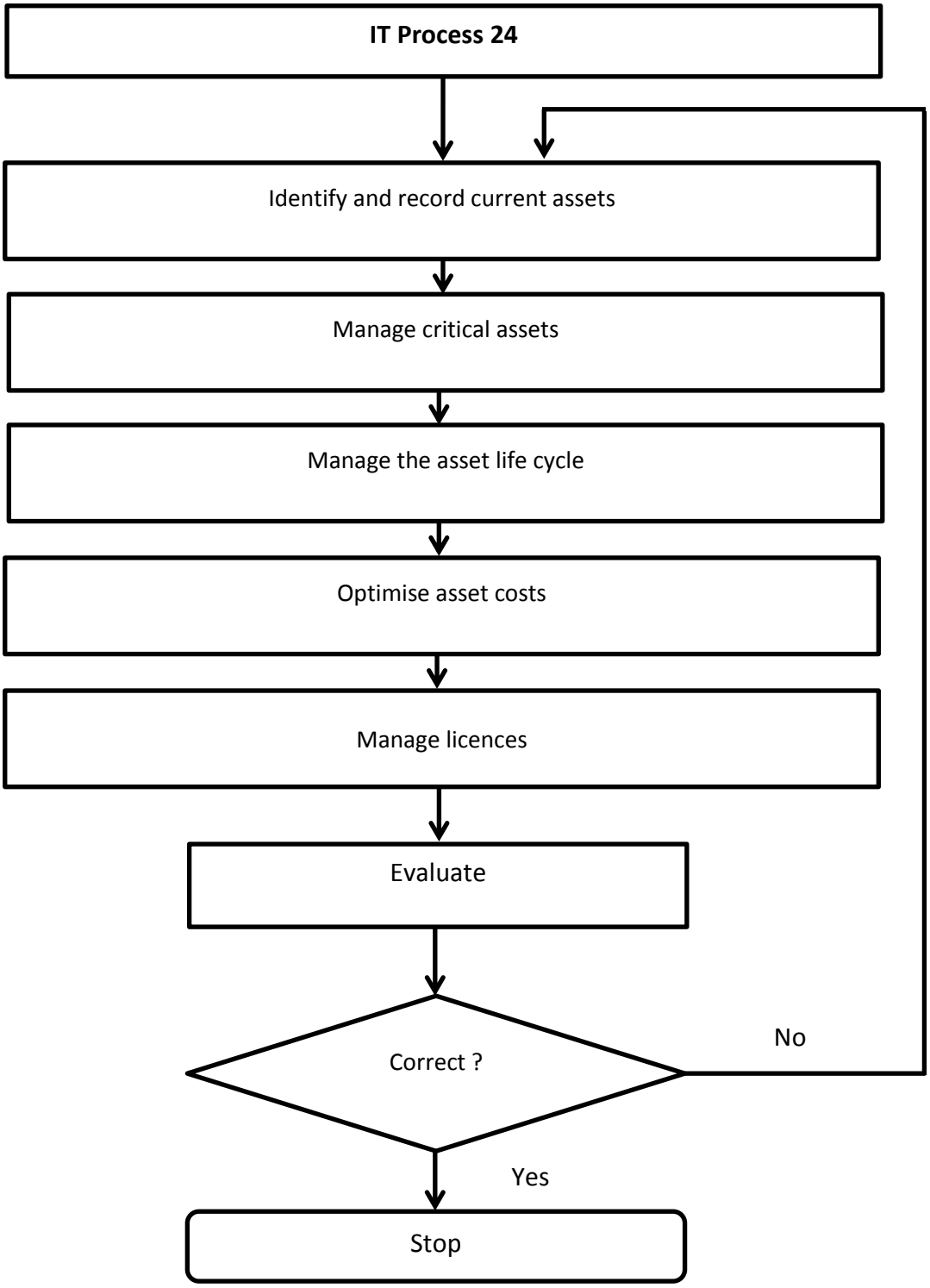

IT Process 19
Establish the desire to change
Form an effective implementation team
Communicate desired vision
Empower role players and identify short-term wins
Enable operation and use
Embed new approaches
Sustain changes
Evaluate
Correct ?
No
Yes
Stop

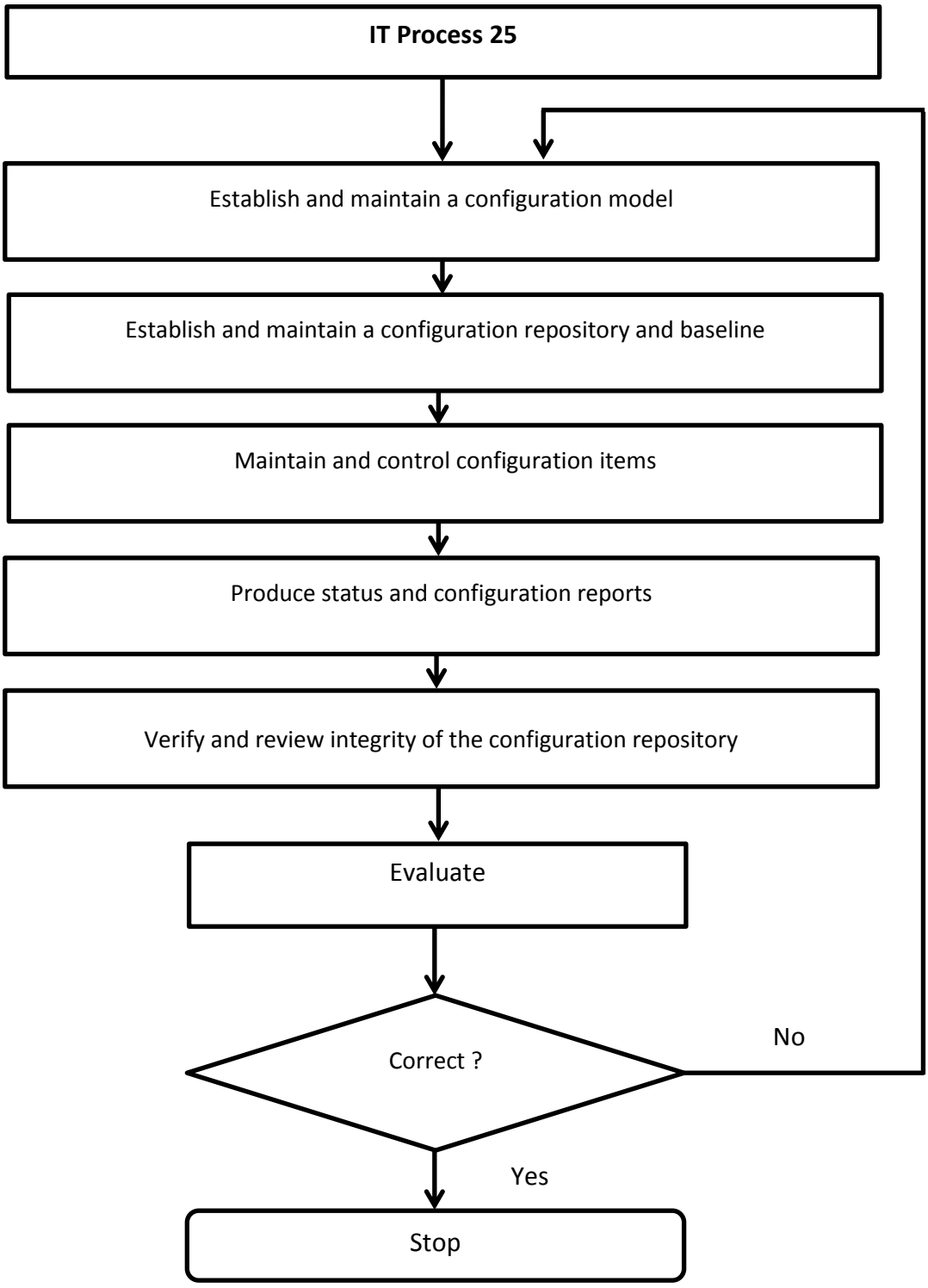

IT Process 20
Perform impact assessment; prioritise and authorise changes
Manage emergency changes
Track and report change status
Close and document the changes
Evaluate
Correct ?
No
Yes
Stop

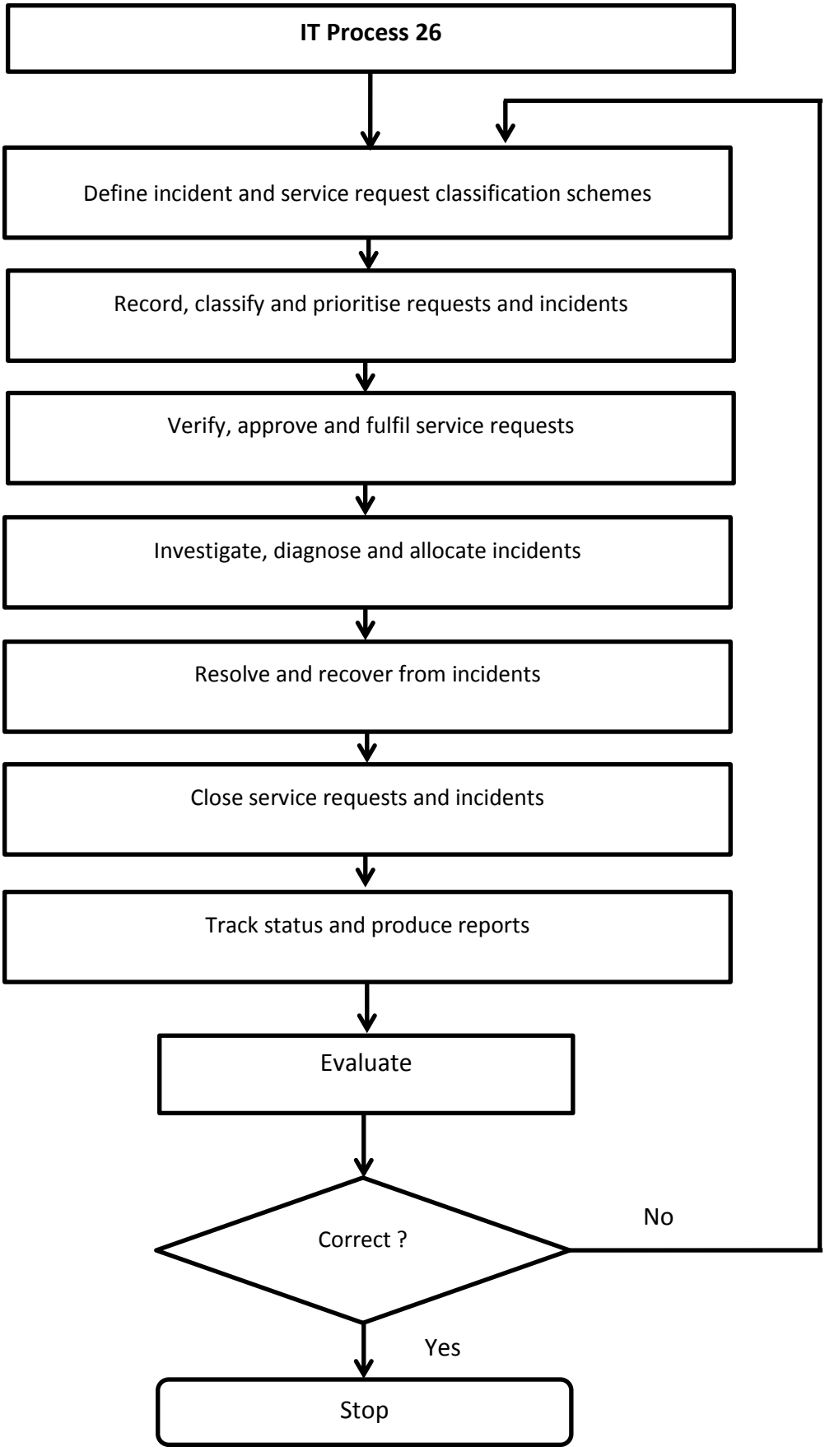

IT Process 21
Establish an implementation plan
Plan business process, system and data conversion
Plan acceptance tests
Establish a test environment
Perform acceptance tests
Promote to production and manage releases
Provide early production support
Perform a post-implementation review
Evaluate
Correct ?
No
Yes
Stop

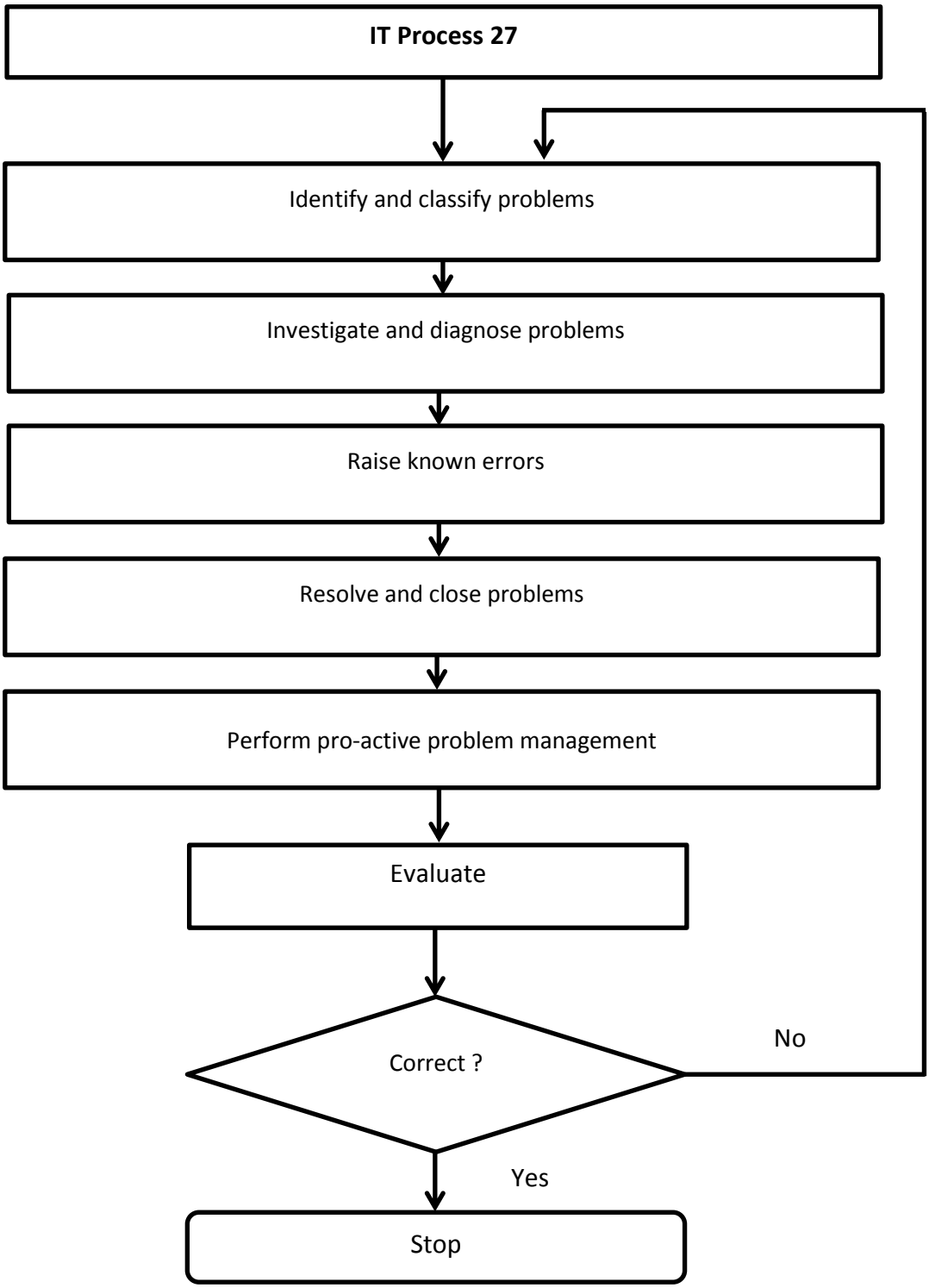

IT Process 22
Nurture and facilitate a knowledge-sharing culture
Identify and classify sources of information
Organise and contextualise information into knowledge
Use and share knowledge
Evaluate and retire information
Evaluate
Correct ?
No
Yes
Stop

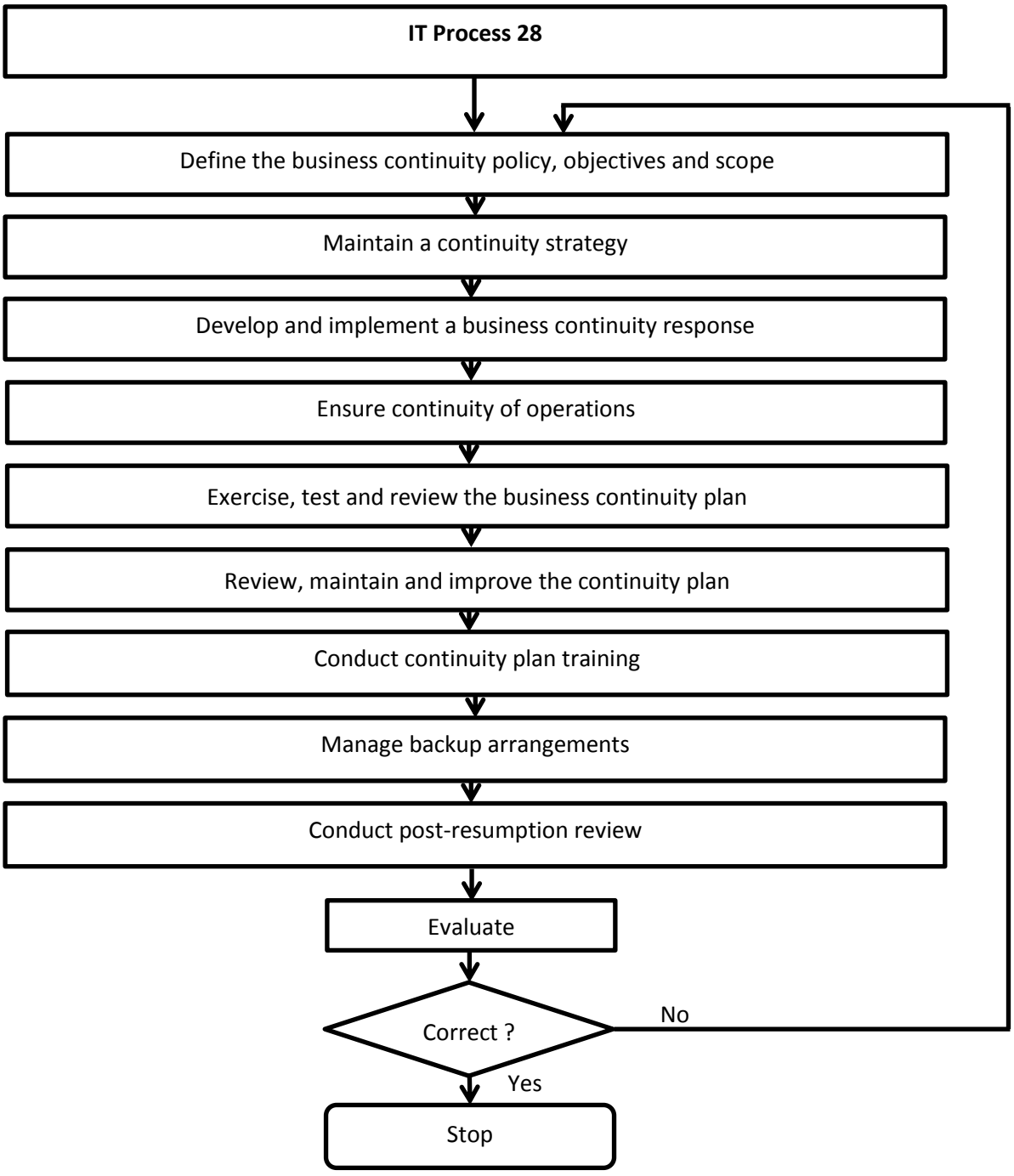

IT Process 23
Maintain regular operational procedures
Manage outsourced IT services
Monitor IT infrastructure
Manage the environment
Manage facilities
Evaluate
Correct ?
No
Yes
Stop

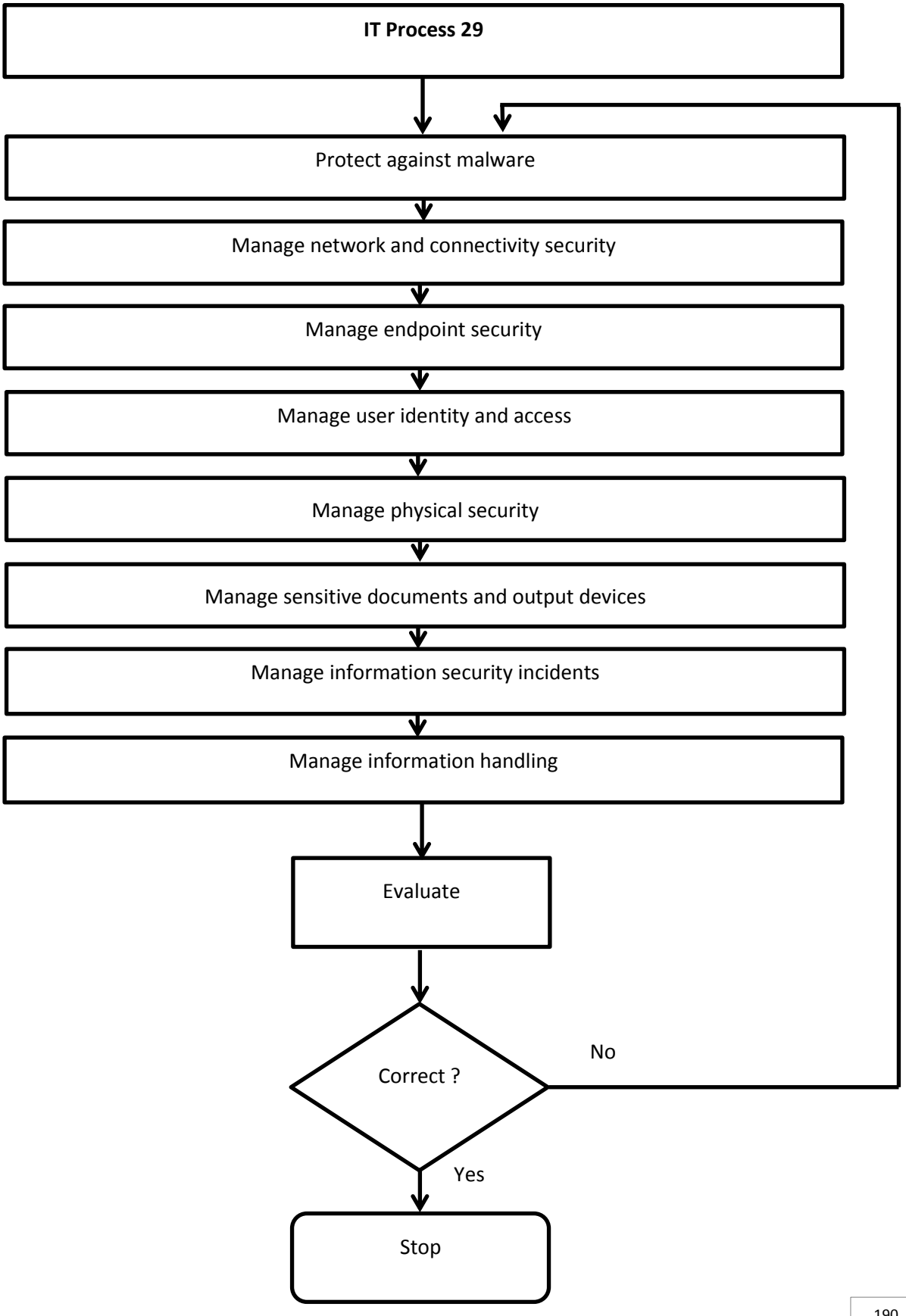

IT Process 24
Identify and record current assets
Manage critical assets
Manage the asset life cycle
Optimise asset costs
Manage licences
Evaluate
Correct ?
No
Yes
Stop

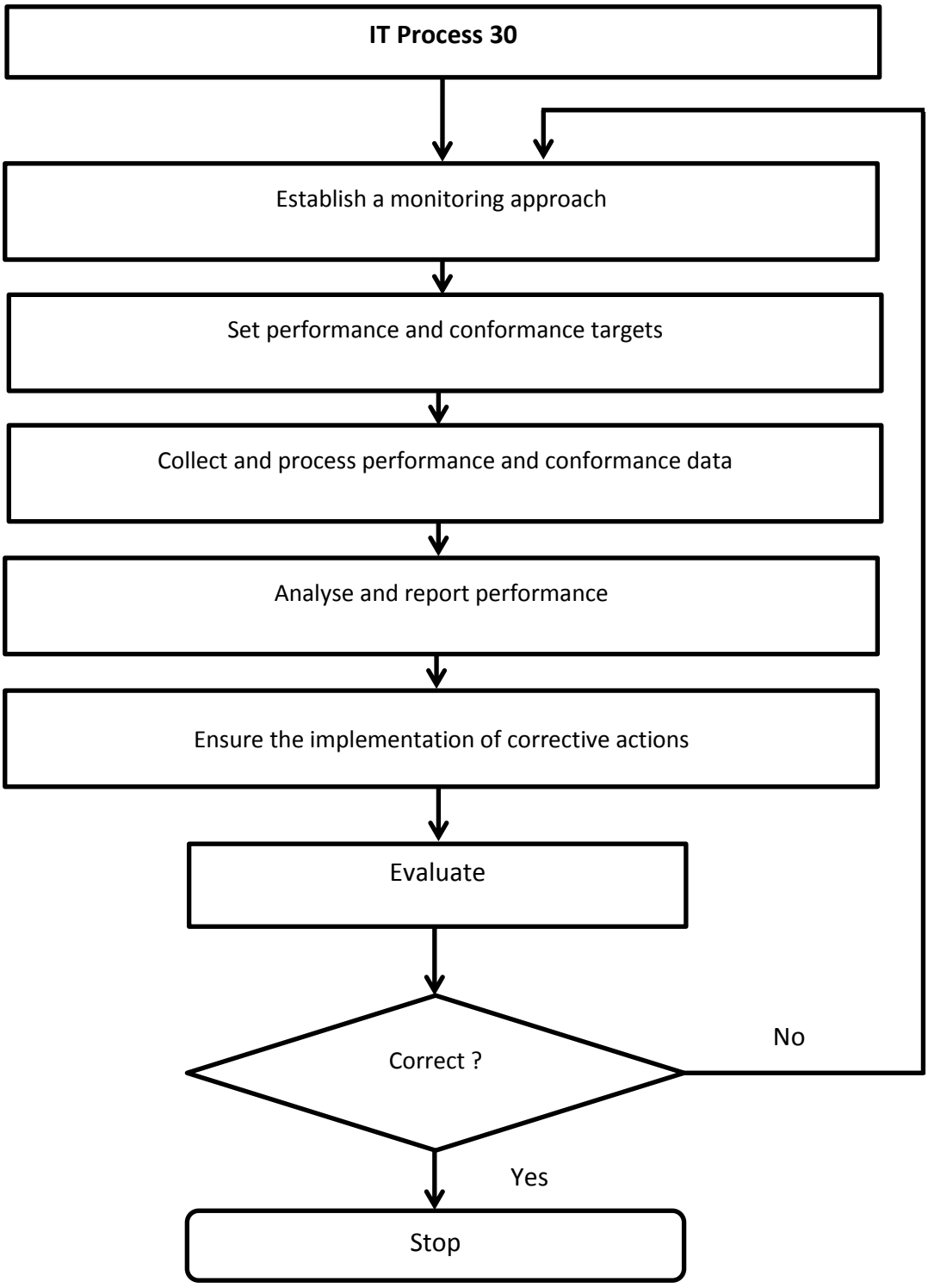

IT Process 25
Establish and maintain a configuration model
Establish and maintain a configuration repository and baseline
Maintain and control configuration items
Produce status and configuration reports
Verify and review integrity of the configuration repository
Evaluate
Correct ?
No
Yes
Stop

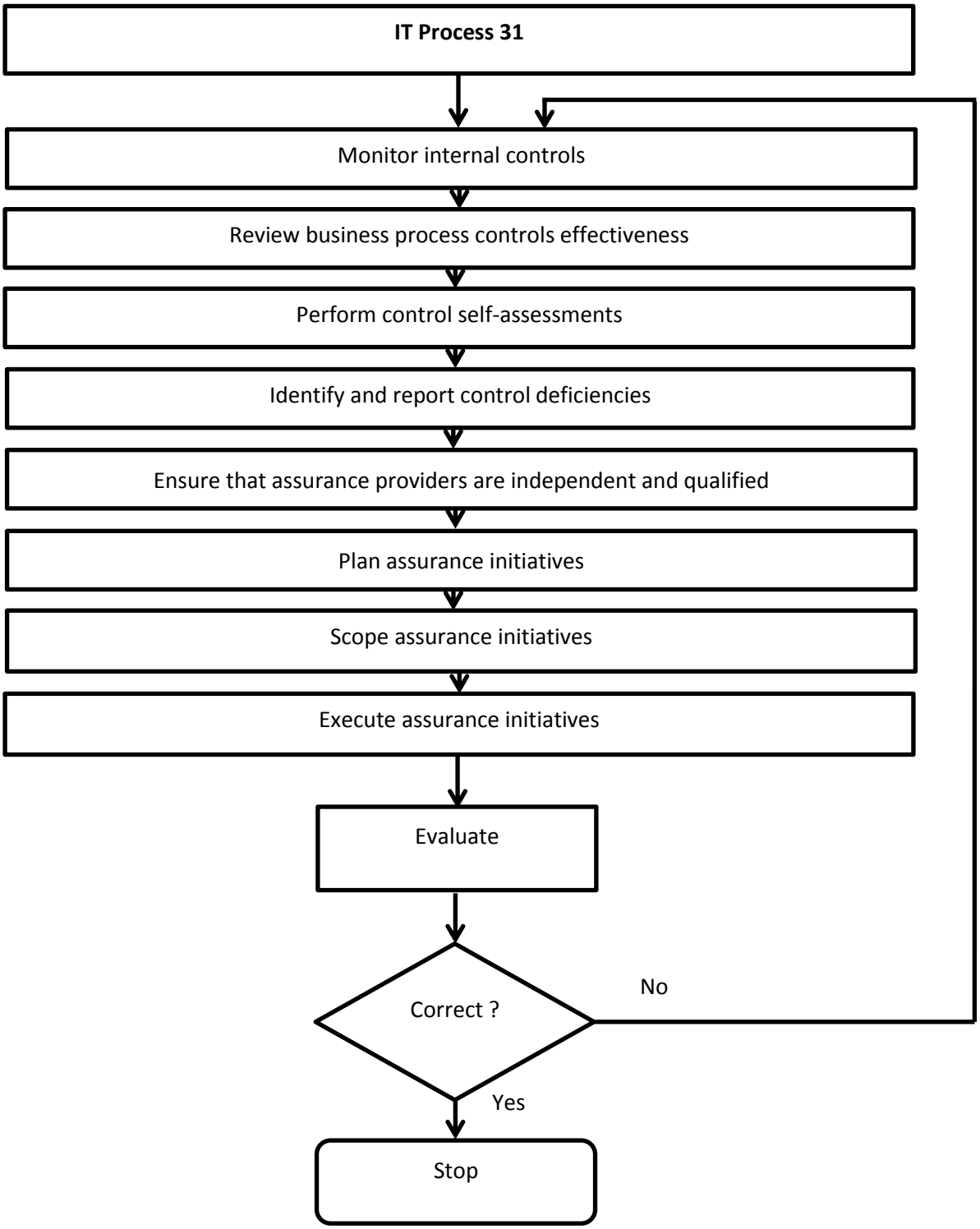

IT Process 26
Define incident and service request classification schemes
Record, classify and prioritise requests and incidents
Verify, approve and fulfil service requests
Investigate, diagnose and allocate incidents
Resolve and recover from incidents
Close service requests and incidents
Track status and produce reports
Evaluate
Correct ?
No
Yes
Stop

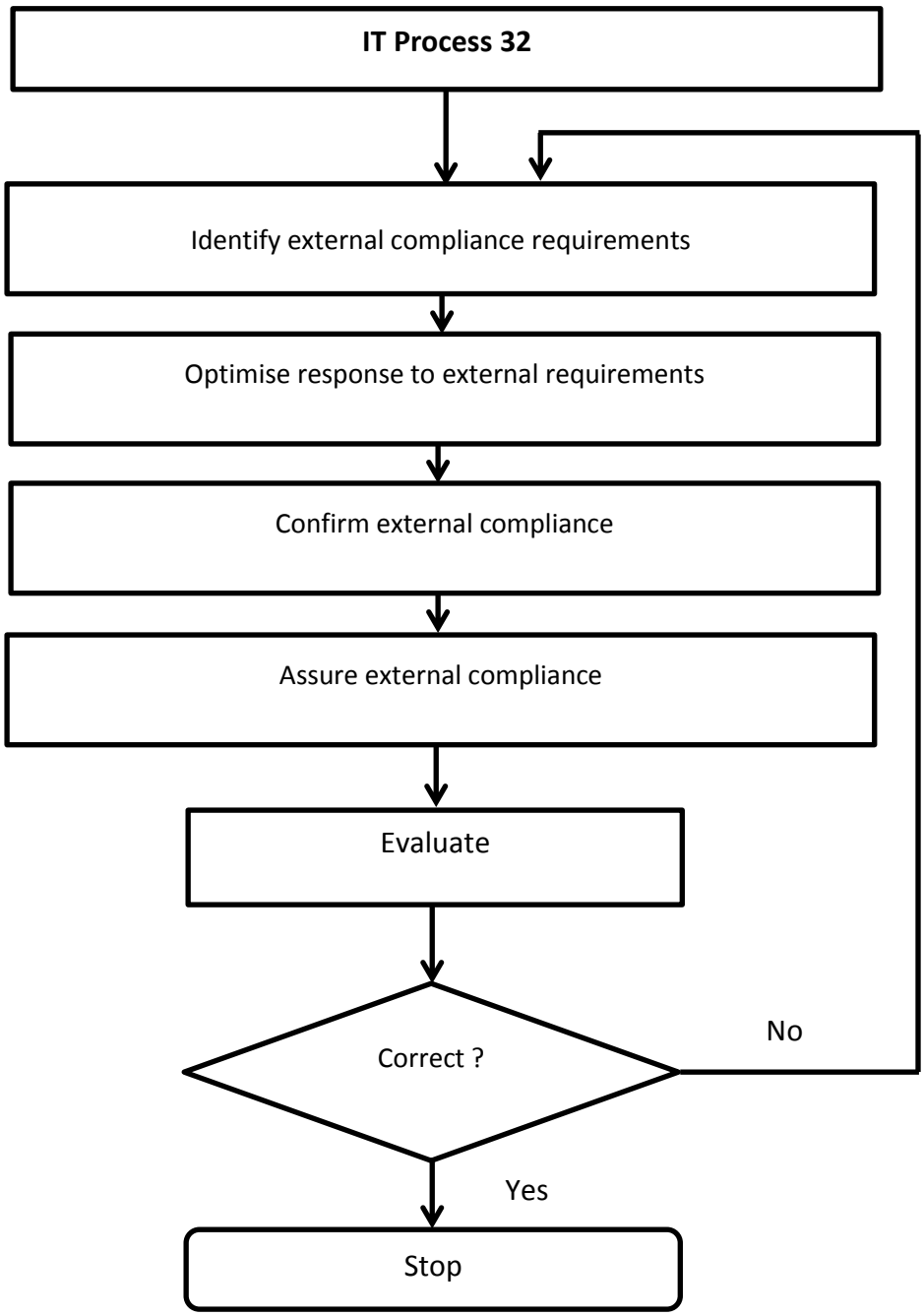

IT Process 27
Identify and classify problems
Investigate and diagnose problems
Raise known errors
Resolve and close problems
Perform pro-active problem management
Evaluate
Correct ?
No
Yes
Stop


IT Process 28
Define the business continuity policy, objectives and scope
Maintain a continuity strategy
Develop and implement a business continuity response
Ensure continuity of operations
Exercise, test and review the business continuity plan
Review, maintain and improve the continuity plan
Conduct continuity plan training
Manage backup arrangements
Conduct post-resumption review
Evaluate
Correct ?
No
Yes
Stop


IT Process 29
Protect against malware
Manage network and connectivity security
Manage endpoint security
Manage user identity and access
Manage physical security
Manage sensitive documents and output devices
Manage information security incidents
Manage information handling
Evaluate
Correct ?
No
Yes
Stop


IT Process 30
Establish a monitoring approach
Set performance and conformance targets
Collect and process performance and conformance data
Analyse and report performance
Ensure the implementation of corrective actions
Evaluate
Correct ?
No
Yes
Stop


IT Process 31
Monitor internal controls
Review business process controls effectiveness
Perform control self-assessments
Identify and report control deficiencies
Ensure that assurance providers are independent and qualified
Plan assurance initiatives
Scope assurance initiatives
Execute assurance initiatives
Evaluate
Correct ?
No
Yes
Stop


IT Process 32
Identify external compliance requirements
Optimise response to external requirements
Confirm external compliance
Assure external compliance
Evaluate
Correct ?
No
Yes
Stop

3-5- The correspondence between Statoil IT Processes and COBIT 5 Model:

Table 3-2: The correspondence between Statoil IT Process and COBIT 5 Processes

IT Process	Correspondent COBIT 5 IT Process
01	EDM01
02	EDM02
03	EDM03
04	EDM04
05	EDM05
06	APO02
07	APO03
08	APO05
09	APO06
10	APO07
11	APO09
12	APO10
13	APO11
14	APO12
15	BAI 01
16	BAI 02
17	BAI 03
18	BAI 04
19	BAI 05
20	BAI 06
21	BAI 07
22	BAI 08
23	DSS 01
24	DSS 02
25	DSS 03
26	DSS 04
27	DSS 05
28	DSS 06
29	DSS 07
30	MEA 01
31	MEA 02
32	MEA 03

3-6- Outputs of Statoil IT Process:

The following data represent the approximation of both of maturity of IT Governance components and IT Governance accumulated effectiveness during different COBIT5-based Statoil IT Processes. The statistical and explaining results are obtained after treating data concerning Statoil IT Management and responses of interview participants. The number of participants is 50, the study targets a set of members concerned and interested in IT Governance. This interview is based on the norms set by ISACA to assess maturity of IT Governance components and IT Governance effectiveness. Effectiveness = met objectives/planned objectives. These results are obtained through scorecard, using 32 combinations of IT Metrics and supported by the results of the interview in order to explain statistical results.

The main Scorecard is composed of the following metrics:

- ✓ Percent of enterprise strategic goals and requirements supported by IT strategic goals;
- ✓ Stakeholder satisfaction with scope of the planned portfolio of programmes and services;
- ✓ Percent of IT value drivers mapped to business value drivers;
- ✓ Cost of IT non-compliance, including settlements and fines;
- ✓ Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment
- ✓ Number of non-compliance issues relating to contractual agreements with IT service providers;
- ✓ Coverage of compliance assessments;
- ✓ Percent of executive management roles with clearly defined accountabilities for IT decisions;
- ✓ Number of times IT is on the board agenda in a proactive manner;
- ✓ Frequency of IT strategy (executive) committee meetings;
- ✓ Rate of execution of executive IT-related decisions;
- ✓ Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment;
- ✓ Number of significant IT-related incidents that were not identified in risk assessment;
- ✓ Percent of enterprise risk assessments including IT-related risks;
- ✓ Update frequency of risk profile ;
- ✓ Percent of IT-enabled investments where benefit realisation monitored through full economic life cycle;
- ✓ Percent of IT services where expected benefits realised;
- ✓ Percent of IT-enabled investments where claimed benefits met or exceeded;
- ✓ Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits;

- ✓ Percent of IT services with clearly defined and approved operational costs and expected benefits;
- ✓ Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information;
- ✓ Number of business disruptions due to IT service incidents;
- ✓ Percent of business stakeholders satisfied that IT service delivery meets agreed-upon service levels;
- ✓ Percent of users satisfied with quality of IT service delivery;
- ✓ Percent of business process owners satisfied with supporting IT products and services;
- ✓ Level of business user understanding of how technology solutions support their processes;
- ✓ Satisfaction level of business users with training and user manuals;
- ✓ Level of satisfaction of business executives with IT's responsiveness to new requirements;
- ✓ Number of critical business processes supported by up-to-date infrastructure and applications;
- ✓ Average time to turn strategic IT objectives into an agreed and approved initiative;
- ✓ Number of security incidents causing business disruption or public embarrassment;
- ✓ Number of IT services with outstanding security requirements;
- ✓ Time to grant, change and remove access privileges, compared to agreed service levels;
- ✓ Frequency of security assessment against latest standards and guidelines;
- ✓ Frequency of capability maturity and cost optimisation assessments;
- ✓ Trend of assessment results ;
- ✓ Satisfaction levels of business and IT executives with IT-related costs and capabilities;
- ✓ Number of business processing incidents caused by technology integration errors;
- ✓ Number of business process changes that need to be delayed or reworked because of technology integration issues;
- ✓ Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues;
- ✓ Number of applications or critical infrastructures operating in silos and not integrated Number of programmes/projects on time and within budget;
- ✓ Percent of stakeholders satisfied with programme/project quality;
- ✓ Number of programmes needing significant rework due to quality defects;
- ✓ Cost of application maintenance vs. overall IT cost;
- ✓ Level of business user satisfaction with quality of management information;
- ✓ Number of business process incidents caused by non-availability of information;
- ✓ Ratio and extent of erroneous business decisions where erroneous or unavailable information was key factor;
- ✓ Number of incidents related to non-compliance to policy;

- ✓ Percent of stakeholders who understand policies;
- ✓ Percent of policies supported by effective standards and working practices;
- ✓ Frequency of policies review and update;
- ✓ Percent of staff whose IT-related skills are sufficient for the competency required for their role;
- ✓ Percent of staff satisfied with their IT-related roles;
- ✓ Number of learning/training hours per staff;
- ✓ Level of business executive awareness and understanding of IT innovation possibilities;
- ✓ Stakeholder satisfaction with levels of IT innovation expertise and ideas;
- ✓ Number of approved initiatives resulting from innovative IT ideas.

Table 3-4: Maturity of IT Governance components					
IT Process (Statoil IT Service)	**Strategic Alignment Maturity** (%)	**Value Delivery Maturity** (%)	**Resource Management Maturity** (%)	**Risk Management Maturity** (%)	**Performance Measurement Maturity** (%)
01	5,13	4,76	4,55	4,88	8,70
02	10,26	9,52	9,10	9,76	17,40
03	15,39	14,28	13,65	14,64	26,10
04	20,52	19,04	18,20	19,52	34,80
05	25,65	23,80	22,75	24,40	43,50
06	30,78	23,80	27,30	26,84	43,50
07	33,34	23,80	31,85	31,72	43,50
08	35,90	26,18	34,12	31,72	47,85
09	35,90	26,18	38,67	31,72	52,20
10	41,03	26,18	43,22	34,16	56,55
11	46,16	30,94	47,77	34,16	65,25
12	46,16	35,70	50,04	39,04	69,60
13	51,29	38,08	50,04	41,48	69,60
14	56,42	38,08	50,04	43,92	69,60
15	61,55	40,46	52,31	46,36	73,95
16	66,68	45,22	54,58	48,80	73,95
17	71,81	49,98	56,85	51,24	73,95
18	74,37	52,36	61,40	53,68	78,30
19	74,37	57,12	63,67	53,68	78,30
20	74,37	61,88	65,94	53,68	78,30
21	76,93	66,64	68,21	56,12	82,65
22	79,49	71,40	68,21	58,56	82,65
23	79,49	71,40	72,76	58,56	82,65
24	79,49	73,78	77,31	58,56	82,65
25	79,49	78,54	77,31	61,00	82,65
26	82,05	83,30	77,31	61,00	87,00
27	82,05	88,06	77,31	63,44	87,00
28	84,61	92,82	81,86	68,32	91,30
29	84,61	92,82	81,86	73,20	91,30
30	84,61	92,82	81,86	73,20	100,00
31	84,61	97,58	81,86	78,08	100,00
32	89,74	97,58	81,86	82,96	100,00

Table 3-5: Accumulated effectiveness of IT Governance

IT Process (Statoil IT Management)	IT Governance Accumulated Effectiveness (%)
01	5,29
02	10,58
03	15,87
04	21,16
05	26,45
06	29,1
07	31,75
08	33,87
09	35,46
10	37,58
11	41,81
12	44,98
13	47,1
14	48,69
15	51,86
16	55,03
17	58,2
18	61,37
19	62,96
20	64,55
21	67,72
22	69,31
23	70,37
24	71,96
25	73,55
26	75,67
27	77,26
28	81,49
29	82,55
30	83,61
31	85,73
32	87,85

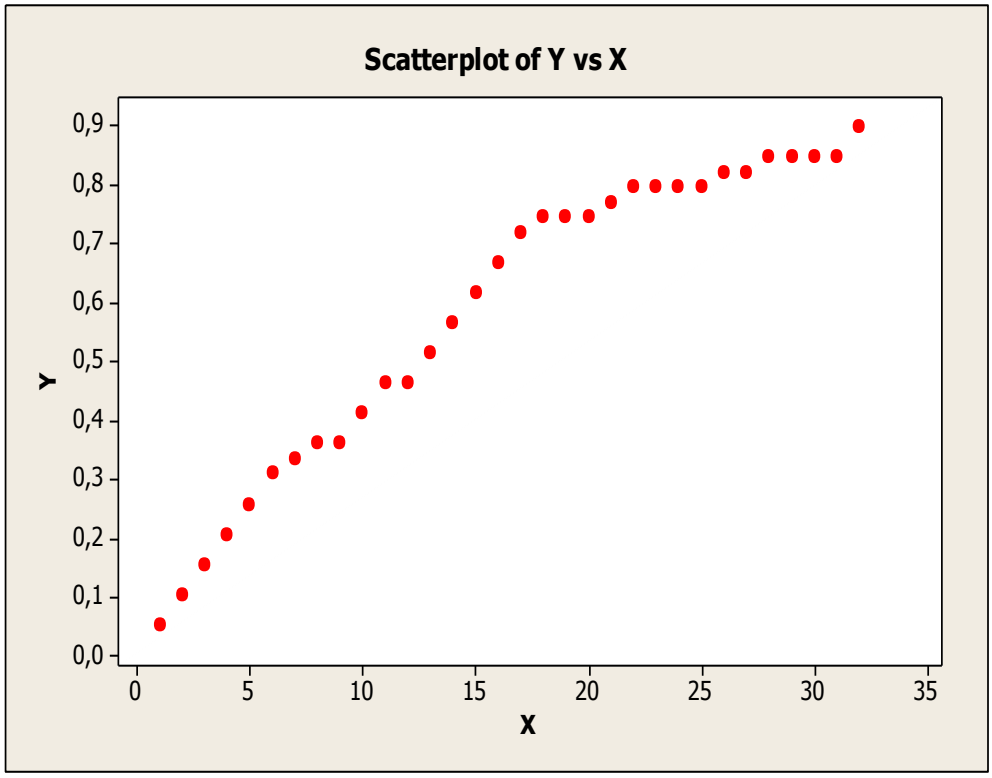
4- Data Analysis:

4-1-The relationship between COBIT 5 and Strategic Alignment Maturity:

Y: Strategic Alignment Maturity

X: COBIT 5 Process

X	Y
01	0,0513
02	0,1026
03	0,1539
04	0,2052
05	0,2565
06	0,3078
07	0,3334
08	0,359
09	0,359
10	0,4103
11	0,4616
12	0,4616
13	0,5129
14	0,5642
15	0,6155
16	0,6668
17	0,7181
18	0,7437
19	0,7437
20	0,7437
21	0,7693
22	0,7949
23	0,7949
24	0,7949
25	0,7949
26	0,8205
27	0,8205
28	0,8461
29	0,8461
30	0,8461
31	0,8461
32	0,8974



Regression for Y vs X
Summary Report

Y: Strategic Alignment Maturity
X: COBIT 5 Process

Is there a relationship between Y and X?

P = 0,000

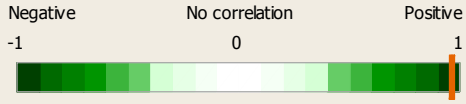
The relationship between Y and X is statistically significant (p < 0,05).

% of variation accounted for by model

R-sq (adj) = 92,70%

92,70% of the variation in Y can be accounted for by the regression model.

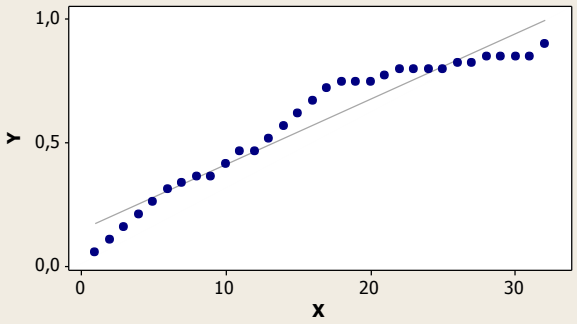
Correlation between Y and X



The positive correlation (r = 0,96) indicates that when X increases, Y also tends to increase.

Fitted Line Plot for Linear Model

Y = 0,1458 + 0,02647 X



Comments

The fitted equation for the linear model that describes the relationship between Y and X is:

Y = 0,1458 + 0,02647 X

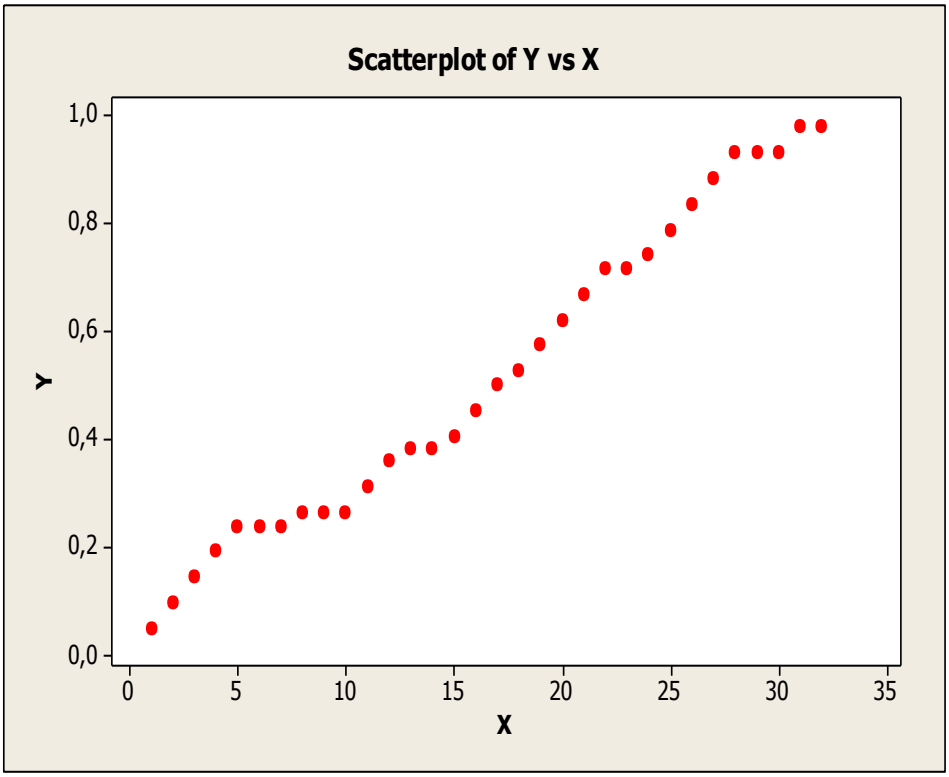
If the model fits the data well, this equation can be used to predict Y for a value of X, or find the settings for X that correspond to a desired value or range of values for Y.

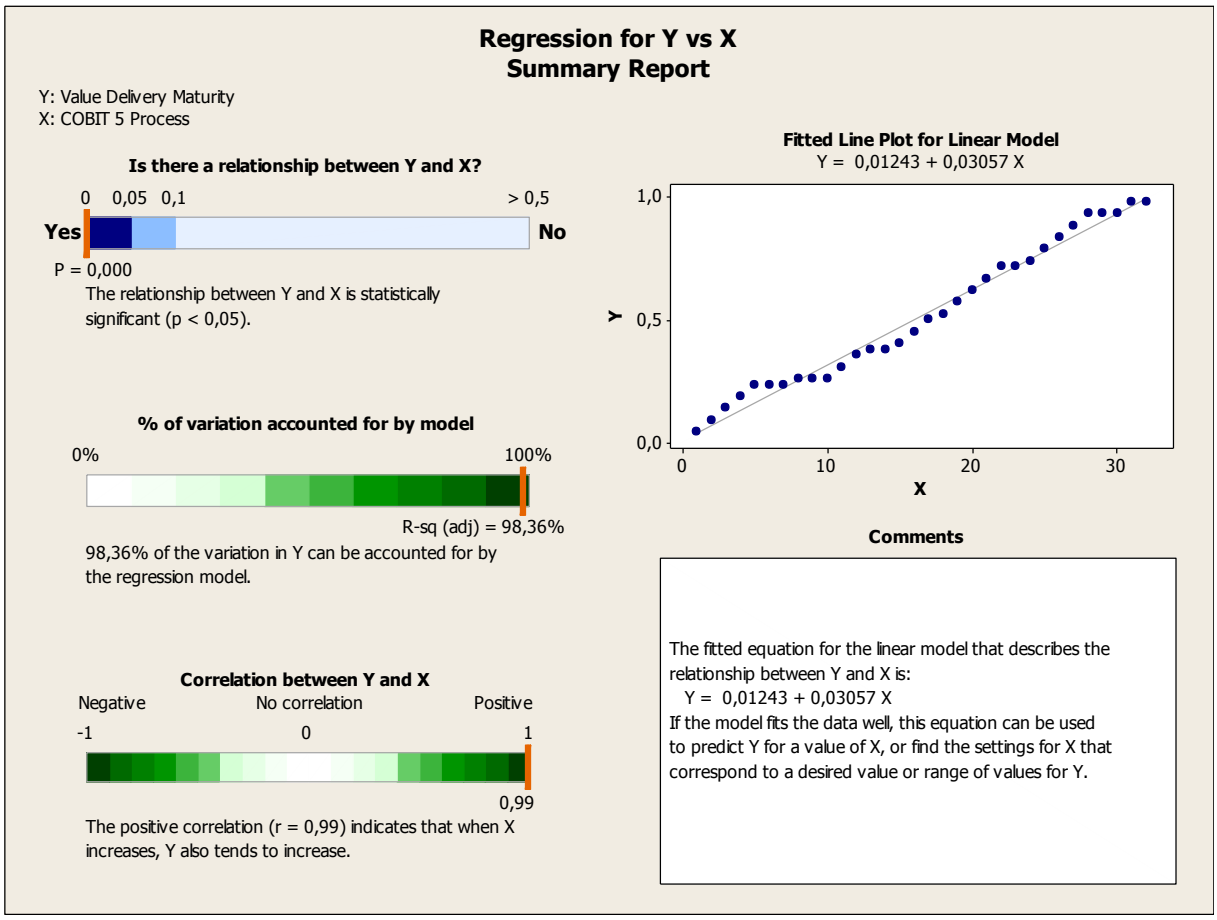
4-2-The relationship between COBIT 5 and Value Delivery:

Y: Value Delivery Maturity

X: COBIT 5 Process

X	Y
01	0,0476
02	0,0952
03	0,1428
04	0,1904
05	0,238
06	0,238
07	0,238
08	0,2618
09	0,2618
10	0,2618
11	0,3094
12	0,357
13	0,3808
14	0,3808
15	0,4046
16	0,4522
17	0,4998
18	0,5236
19	0,5712
20	0,6188
21	0,6664
22	0,714
23	0,714
24	0,7378
25	0,7854
26	0,833
27	0,8806
28	0,9282
29	0,9282
30	0,9282
31	0,9758
32	0,9758



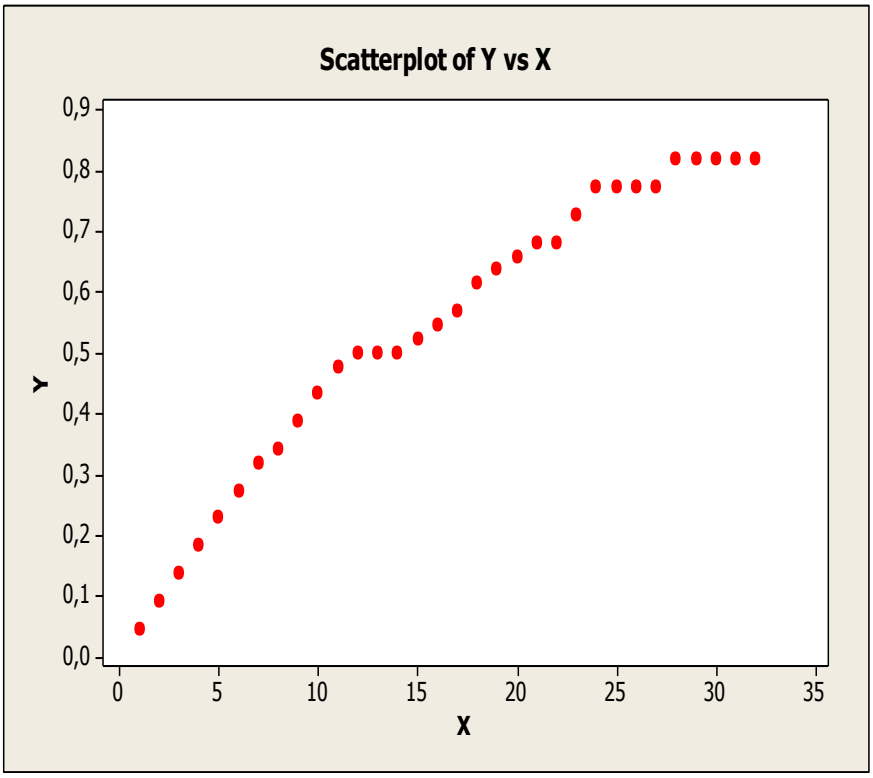

Regression for Y vs X
Summary Report
Y: Value Delivery Maturity
X: COBIT 5 Process
Is there a relationship between Y and X?
0 0,05 0,1 > 0,5
Yes
No
P = 0,000
The relationship between Y and X is statistically significant (p < 0,05).
% of variation accounted for by model
0%
100%
R-sq (adj) = 98,36%
98,36% of the variation in Y can be accounted for by the regression model.
Correlation between Y and X
Negative
No correlation
Positive
-1
0
1
0,99
The positive correlation (r = 0,99) indicates that when X increases, Y also tends to increase.
Fitted Line Plot for Linear Model
Y = 0,01243 + 0,03057 X
1,0
0,5
0,0
Y
0
10
20
30
X
Comments
The fitted equation for the linear model that describes the relationship between Y and X is:
Y = 0,01243 + 0,03057 X
If the model fits the data well, this equation can be used to predict Y for a value of X, or find the settings for X that correspond to a desired value or range of values for Y.

4-3- The relationship between COBIT 5 and Resource Management:

Y: Resource Management Maturity

X: COBIT 5 Process

X	Y
01	0,0455
02	0,0910
03	0,1365
04	0,1820
05	0,2275
06	0,2730
07	0,3185
08	0,3412
09	0,3867
10	0,4322
11	0,4777
12	0,5004
13	0,5004
14	0,5004
15	0,5231
16	0,5458
17	0,5685
18	0,614
19	0,6367
20	0,6594
21	0,6821
22	0,6821
23	0,7276
24	0,7731
25	0,7731
26	0,7731
27	0,7731
28	0,8186
29	0,8186
30	0,8186
31	0,8186
32	0,8186



Regression for Y vs X
Summary Report

Y: Resource Management Maturity
X: COBIT 5 Process

Is there a relationship between Y and X?

P = 0,000

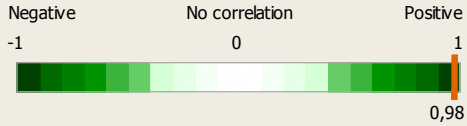
The relationship between Y and X is statistically significant (p < 0,05).

% of variation accounted for by model

R-sq (adj) = 95,44%

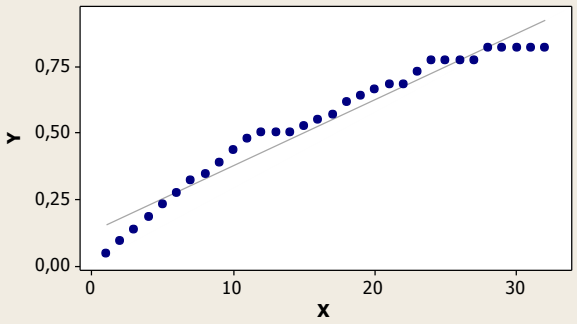
95,44% of the variation in Y can be accounted for by the regression model.

Correlation between Y and X



The positive correlation (r = 0,98) indicates that when X increases, Y also tends to increase.

Fitted Line Plot for Linear Model
Y = 0,1302 + 0,02476 X



Comments

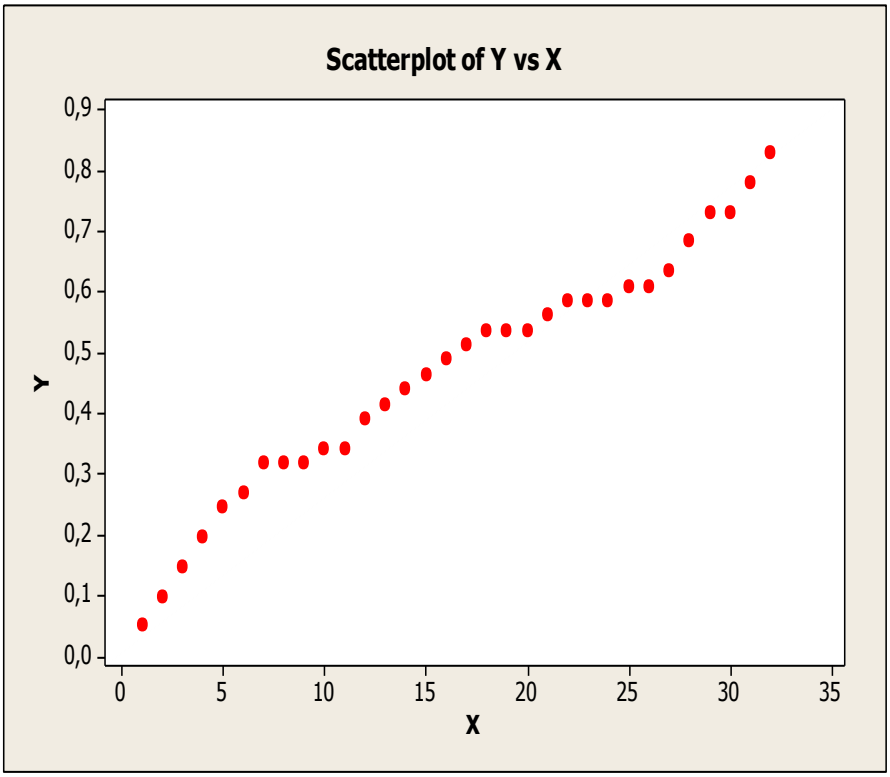
The fitted equation for the linear model that describes the relationship between Y and X is:
Y = 0,1302 + 0,02476 X
If the model fits the data well, this equation can be used to predict Y for a value of X, or find the settings for X that correspond to a desired value or range of values for Y.

4-4- The relationship between COBIT 5 and Risk Management:

Y: Risk Management Maturity

X: COBIT 5 Process

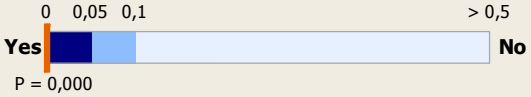
X	Y
01	0,0488
02	0,0976
03	0,1464
04	0,1952
05	0,244
06	0,2684
07	0,3172
08	0,3172
09	0,3172
10	0,3416
11	0,3416
12	0,3904
13	0,4148
14	0,4392
15	0,4636
16	0,488
17	0,5124
18	0,5368
19	0,5368
20	0,5368
21	0,5612
22	0,5856
23	0,5856
24	0,5856
25	0,6100
26	0,6100
27	0,6344
28	0,6832
29	0,7320
30	0,7320
31	0,7808
32	0,8296



Regression for Y vs X
Summary Report

Y: Risk Management Maturity
X: COBIT 5 Process

Is there a relationship between Y and X?



P = 0,000

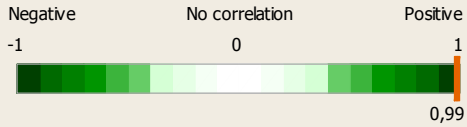
The relationship between Y and X is statistically significant (p < 0,05).

% of variation accounted for by model

R-sq (adj) = 96,98%

96,98% of the variation in Y can be accounted for by the regression model.

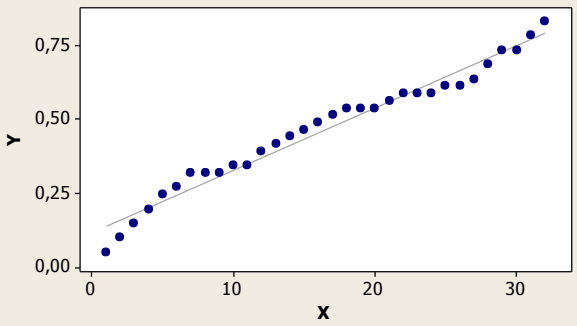
Correlation between Y and X



The positive correlation (r = 0,99) indicates that when X increases, Y also tends to increase.

Fitted Line Plot for Linear Model

Y = 0,1186 + 0,02100 X



Comments

The fitted equation for the linear model that describes the relationship between Y and X is:

Y = 0,1186 + 0,02100 X

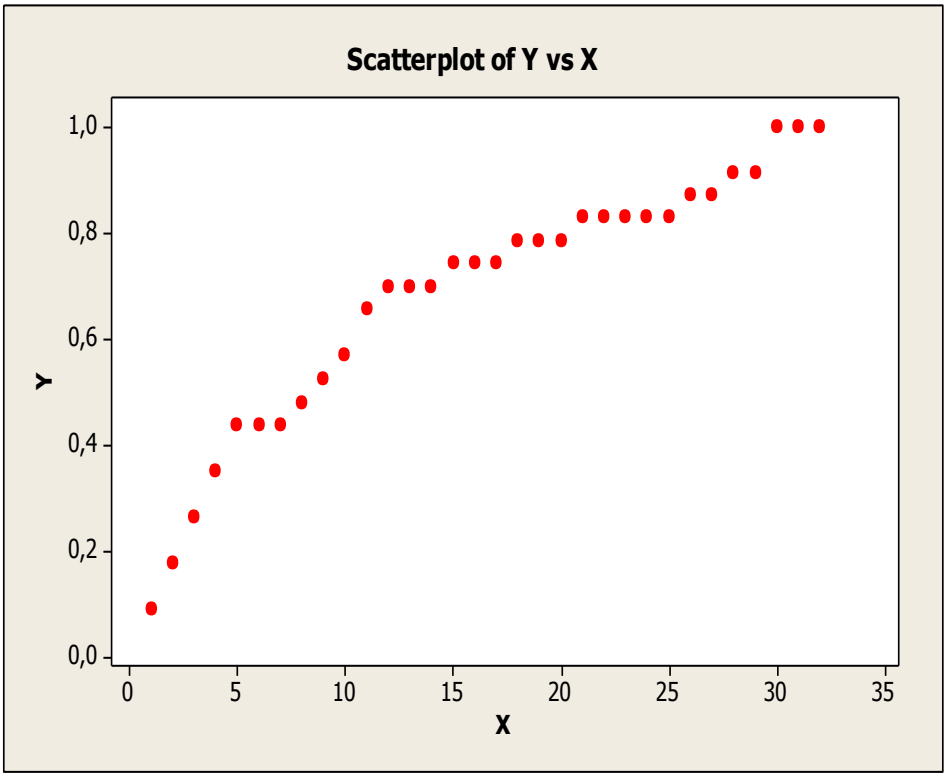
If the model fits the data well, this equation can be used to predict Y for a value of X, or find the settings for X that correspond to a desired value or range of values for Y.

4-5- The relationship between COBIT 5 and Performance Measurement:

Y: Performance Measurement Maturity

X: COBIT 5 Process

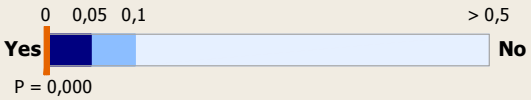
X	Y
01	0,087
02	0,1740
03	0,2610
04	0,3480
05	0,4350
06	0,4350
07	0,4350
08	0,4785
09	0,5220
10	0,5655
11	0,6525
12	0,6960
13	0,6960
14	0,6960
15	0,7395
16	0,7395
17	0,7395
18	0,7830
19	0,7830
20	0,7830
21	0,8265
22	0,8265
23	0,8265
24	0,8265
25	0,8265
26	0,8700
27	0,8700
28	0,9130
29	0,9130
30	1,0000
31	1,0000
32	1,0000



Regression for Y vs X
Summary Report

Y: Performance Measurement Maturity
X: COBIT 5 Process

Is there a relationship between Y and X?



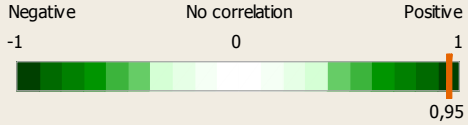
P = 0,000

The relationship between Y and X is statistically significant (p < 0,05).

% of variation accounted for by model

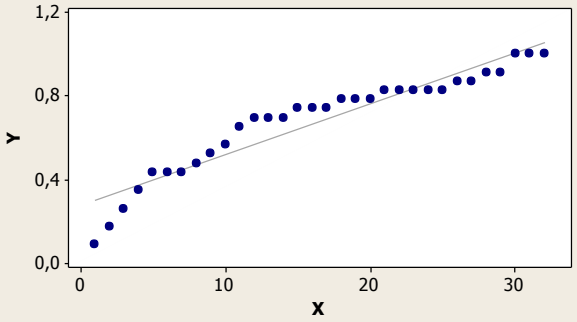
89,99% of the variation in Y can be accounted for by the regression model.

Correlation between Y and X



The positive correlation (r = 0,95) indicates that when X increases, Y also tends to increase.

Fitted Line Plot for Linear Model
Y = 0,2778 + 0,02435 X



Comments

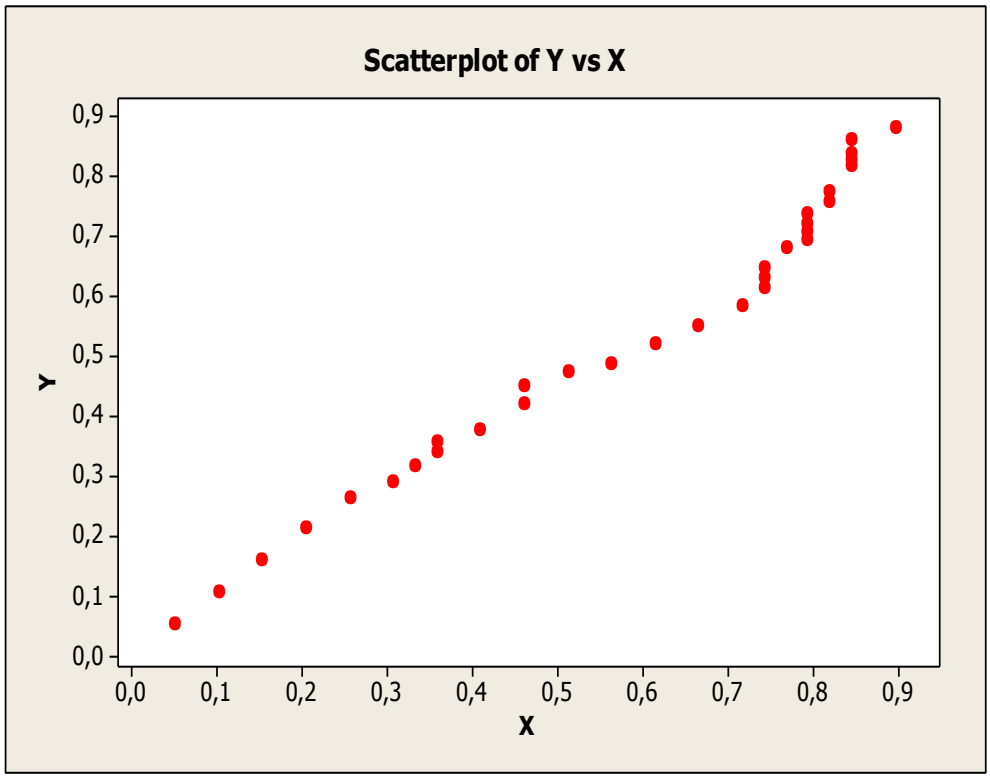
The fitted equation for the linear model that describes the relationship between Y and X is:
Y = 0,2778 + 0,02435 X
If the model fits the data well, this equation can be used to predict Y for a value of X, or find the settings for X that correspond to a desired value or range of values for Y.

4-6- The relationship between Strategic Alignment and IT Governance:

Y: IT Governance Accumulated Effectiveness

X: Strategic Alignment Maturity

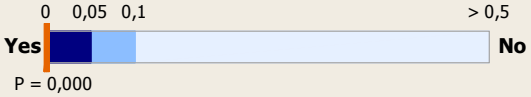
X	Y
0,0513	0,0529
0,1026	0,1058
0,1539	0,1587
0,2052	0,2116
0,2565	0,2645
0,3078	0,291
0,3334	0,3175
0,359	0,3387
0,359	0,3546
0,4103	0,3758
0,4616	0,4181
0,4616	0,4498
0,5129	0,471
0,5642	0,4869
0,6155	0,5186
0,6668	0,5503
0,7181	0,582
0,7437	0,6137
0,7437	0,6296
0,7437	0,6455
0,7693	0,6772
0,7949	0,6931
0,7949	0,7037
0,7949	0,7196
0,7949	0,7355
0,8205	0,7567
0,8205	0,7726
0,8461	0,8149
0,8461	0,8255
0,8461	0,8361
0,8461	0,8573
0,8974	0,8785



Regression for Y vs X
Summary Report

Y: IT Governance Accumulated Effectiveness
X:Strategic Alignment Maturity

Is there a relationship between Y and X?

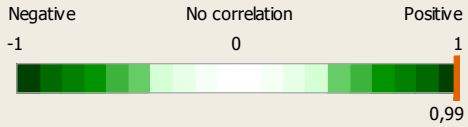


P = 0,000
The relationship between Y and X is statistically significant (p < 0,05).

% of variation accounted for by model

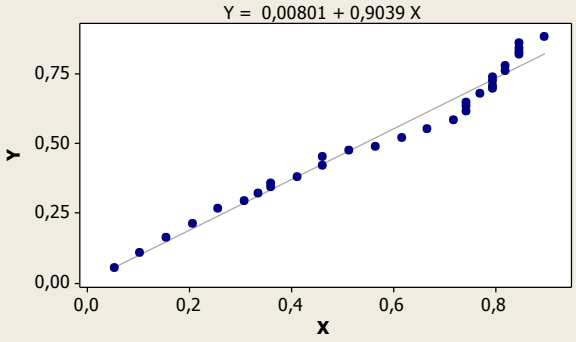
R-sq (adj) = 97,29%
97,29% of the variation in Y can be accounted for by the regression model.

Correlation between Y and X



The positive correlation (r = 0,99) indicates that when X increases, Y also tends to increase.

Fitted Line Plot for Linear Model



Comments

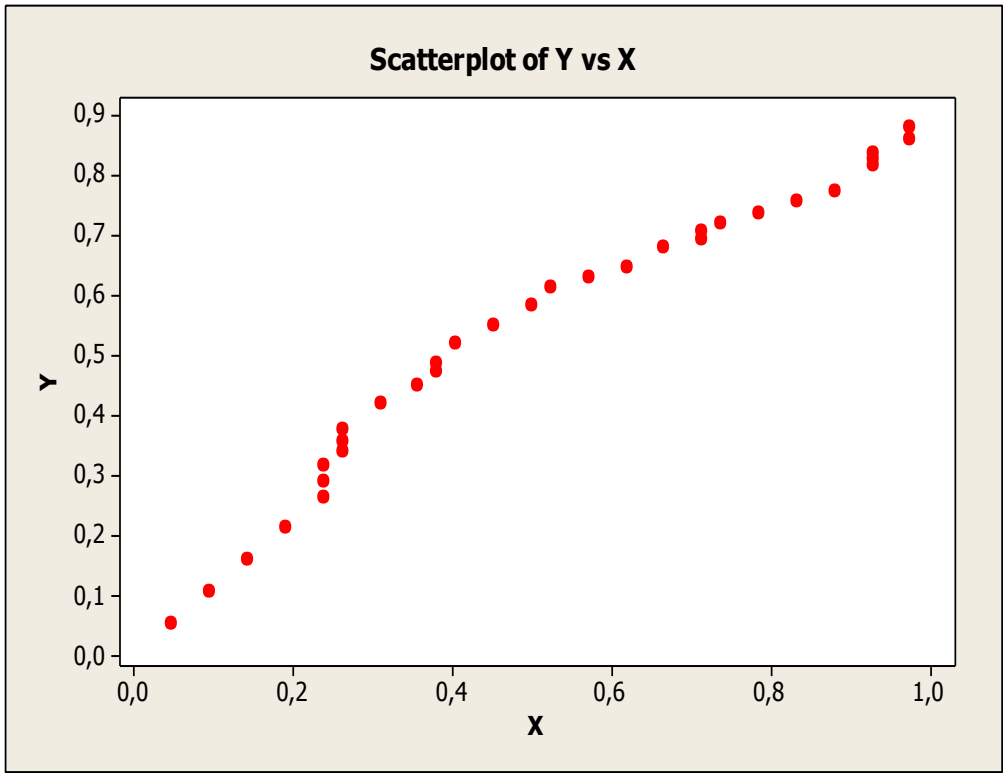
The fitted equation for the linear model that describes the relationship between Y and X is:
Y = 0,00801 + 0,9039 X
If the model fits the data well, this equation can be used to predict Y for a value of X, or find the settings for X that correspond to a desired value or range of values for Y.

4-7-The relationship between Value Delivery and IT Governance:

Y: IT Governance Accumulated Effectiveness

X: Value Delivery Maturity

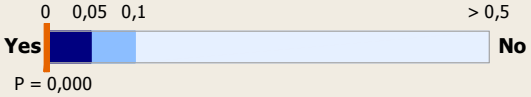
X	Y
0,0476	0,0529
0,0952	0,1058
0,1428	0,1587
0,1904	0,2116
0,238	0,2645
0,238	0,291
0,238	0,3175
0,2618	0,3387
0,2618	0,3546
0,2618	0,3758
0,3094	0,4181
0,357	0,4498
0,3808	0,471
0,3808	0,4869
0,4046	0,5186
0,4522	0,5503
0,4998	0,582
0,5236	0,6137
0,5712	0,6296
0,6188	0,6455
0,6664	0,6772
0,714	0,6931
0,714	0,7037
0,7378	0,7196
0,7854	0,7355
0,833	0,7567
0,8806	0,7726
0,9282	0,8149
0,9282	0,8255
0,9282	0,8361
0,9758	0,8573
0,9758	0,8785



Regression for Y vs X
Summary Report

Y: IT Governance Accumulated Effectiveness
X: Value Delivery Maturity

Is there a relationship between Y and X?



P = 0,000

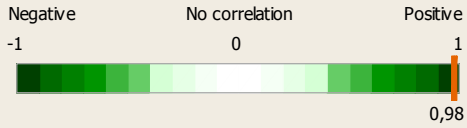
The relationship between Y and X is statistically significant (p < 0,05).

% of variation accounted for by model

R-sq (adj) = 95,25%

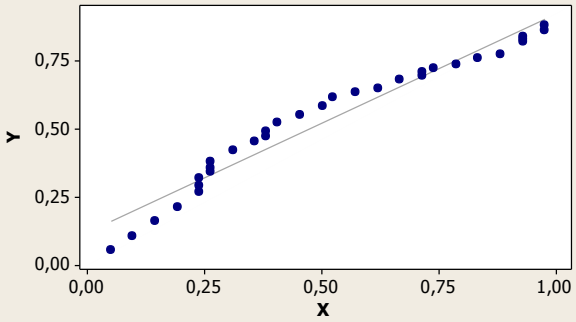
95,25% of the variation in Y can be accounted for by the regression model.

Correlation between Y and X



The positive correlation (r = 0,98) indicates that when X increases, Y also tends to increase.

Fitted Line Plot for Linear Model
Y = 0,1226 + 0,7971 X



Comments

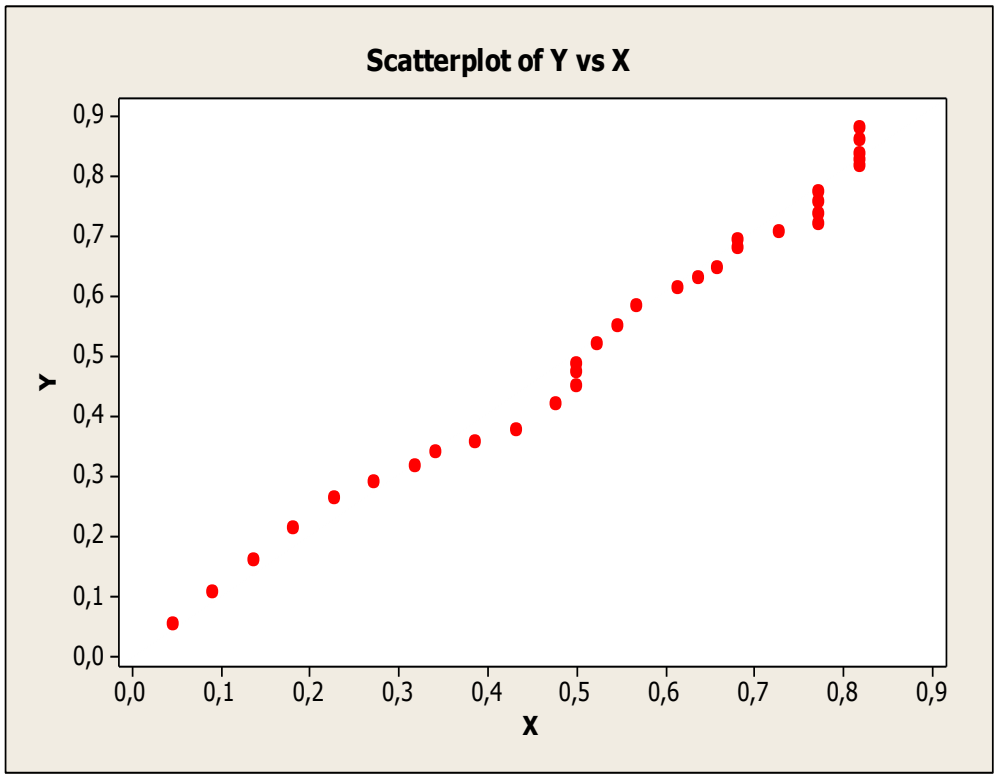
The fitted equation for the linear model that describes the relationship between Y and X is:
Y = 0,1226 + 0,7971 X
If the model fits the data well, this equation can be used to predict Y for a value of X, or find the settings for X that correspond to a desired value or range of values for Y.

4-8-The relationship between Resource Management and IT Governance:

Y: IT Governance Accumulated Effectiveness

X: Resource Management Maturity

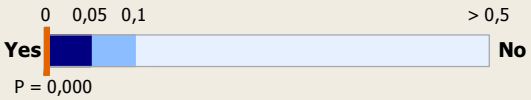
X	Y
0,0455	0,0529
0,0910	0,1058
0,1365	0,1587
0,182	0,2116
0,2275	0,2645
0,2730	0,291
0,3185	0,3175
0,3412	0,3387
0,3867	0,3546
0,4322	0,3758
0,4777	0,4181
0,5004	0,4498
0,5004	0,471
0,5004	0,4869
0,5231	0,5186
0,5458	0,5503
0,5685	0,582
0,614	0,6137
0,6367	0,6296
0,6594	0,6455
0,6821	0,6772
0,6821	0,6931
0,7276	0,7037
0,7731	0,7196
0,7731	0,7355
0,7731	0,7567
0,7731	0,7726
0,8186	0,8149
0,8186	0,8255
0,8186	0,8361
0,8186	0,8573
0,8186	0,8785



Regression for Y vs X
Summary Report

Y: IT Governance Accumulated Effectiveness
X: Resource Management Maturity

Is there a relationship between Y and X?



P = 0,000

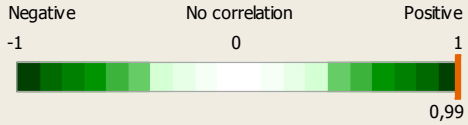
The relationship between Y and X is statistically significant (p < 0,05).

% of variation accounted for by model

R-sq (adj) = 98,50%

98,50% of the variation in Y can be accounted for by the regression model.

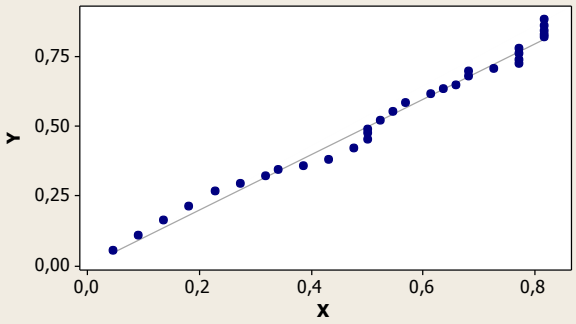
Correlation between Y and X



The positive correlation (r = 0,99) indicates that when X increases, Y also tends to increase.

Fitted Line Plot for Linear Model

Y = 0,00353 + 0,9859 X



Comments

The fitted equation for the linear model that describes the relationship between Y and X is:

Y = 0,00353 + 0,9859 X

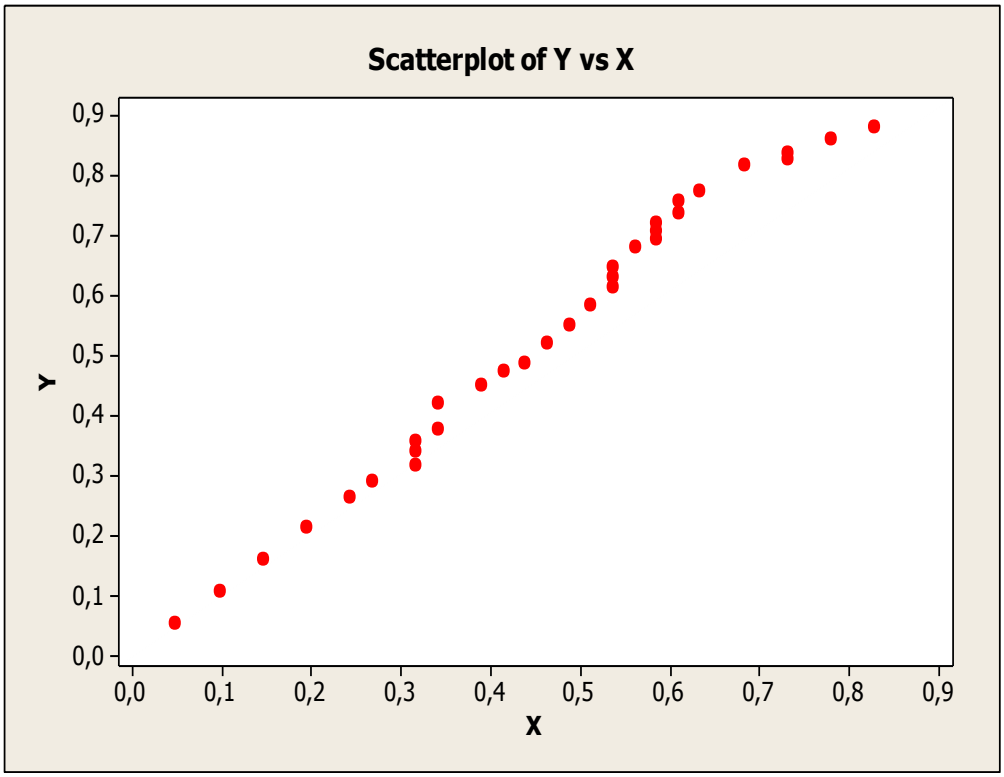
If the model fits the data well, this equation can be used to predict Y for a value of X, or find the settings for X that correspond to a desired value or range of values for Y.

4-9-The relationship between Risk Management and IT Governance:

Y: IT Governance Accumulated Effectiveness

X: Risk Management Maturity

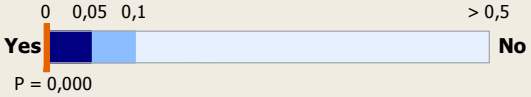
X	Y
0,0488	0,0529
0,0976	0,1058
0,1464	0,1587
0,1952	0,2116
0,244	0,2645
0,2684	0,291
0,3172	0,3175
0,3172	0,3387
0,3172	0,3546
0,3416	0,3758
0,3416	0,4181
0,3904	0,4498
0,4148	0,471
0,4392	0,4869
0,4636	0,5186
0,488	0,5503
0,5124	0,582
0,5368	0,6137
0,5368	0,6296
0,5368	0,6455
0,5612	0,6772
0,5856	0,6931
0,5856	0,7037
0,5856	0,7196
0,6100	0,7355
0,6100	0,7567
0,6344	0,7726
0,6832	0,8149
0,7320	0,8255
0,7320	0,8361
0,7808	0,8573
0,8296	0,8785



Regression for Y vs X
Summary Report

Y: IT Governance Accumulated Effectiveness
X: Risk Management Maturity

Is there a relationship between Y and X?



P = 0,000

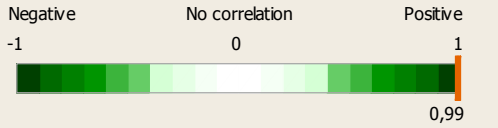
The relationship between Y and X is statistically significant (p < 0,05).

% of variation accounted for by model

R-sq (adj) = 98,50%

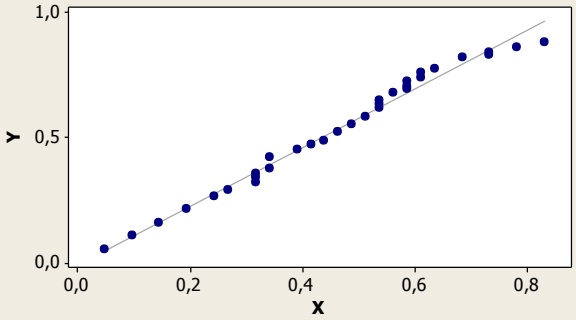
98,50% of the variation in Y can be accounted for by the regression model.

Correlation between Y and X



The positive correlation (r = 0,99) indicates that when X increases, Y also tends to increase.

Fitted Line Plot for Linear Model
Y = - 0,01020 + 1,171 X



Comments

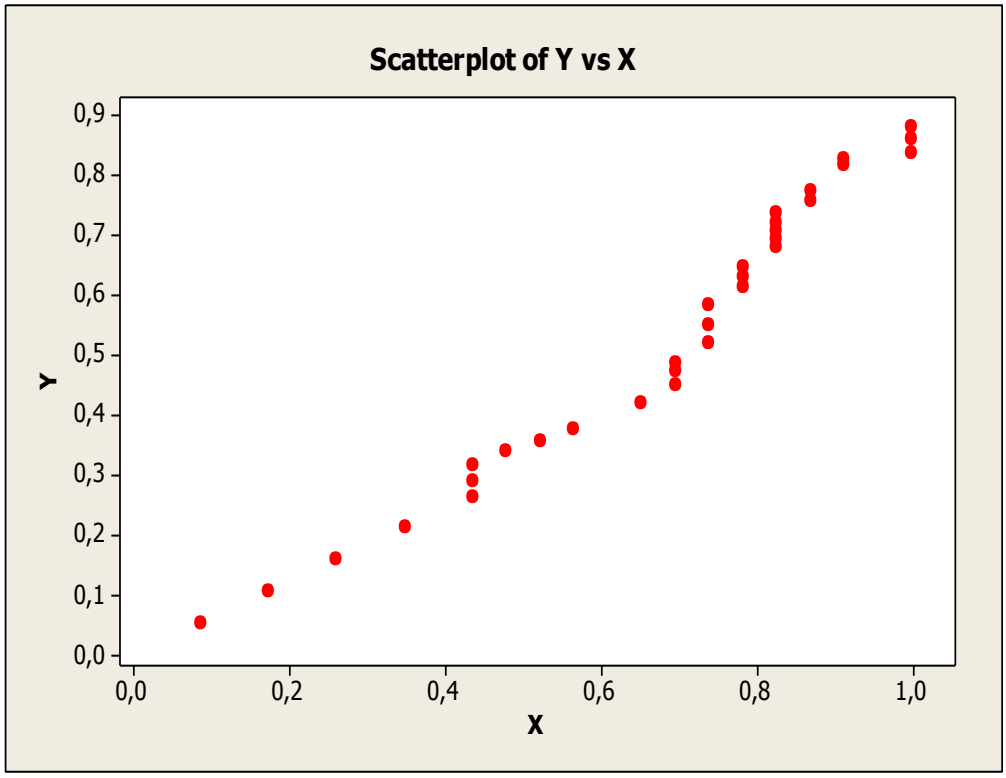
The fitted equation for the linear model that describes the relationship between Y and X is:
Y = - 0,01020 + 1,171 X
If the model fits the data well, this equation can be used to predict Y for a value of X, or find the settings for X that correspond to a desired value or range of values for Y.

4-10- The relationship between Performance Measurement and IT Governance:

Y: IT Governance Accumulated Effectiveness

X: Performance Measurement Maturity

X	Y
0,087	0,0529
0,1740	0,1058
0,2610	0,1587
0,3480	0,2116
0,4350	0,2645
0,4350	0,291
0,4350	0,3175
0,4785	0,3387
0,5220	0,3546
0,5655	0,3758
0,6525	0,4181
0,6960	0,4498
0,6960	0,471
0,6960	0,4869
0,7395	0,5186
0,7395	0,5503
0,7395	0,582
0,7830	0,6137
0,7830	0,6296
0,7830	0,6455
0,8265	0,6772
0,8265	0,6931
0,8265	0,7037
0,8265	0,7196
0,8265	0,7355
0,8700	0,7567
0,8700	0,7726
0,9130	0,8149
0,9130	0,8255
1,0000	0,8361
1,0000	0,8573
1,0000	0,8785



Regression for Y vs X
Summary Report

Y: IT Governance Accumulated Effectiveness
X: Performance Measurement Maturity

Is there a relationship between Y and X?

P = 0,000

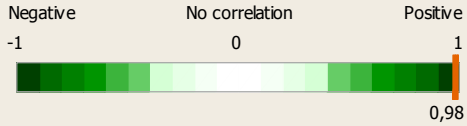
The relationship between Y and X is statistically significant (p < 0,05).

% of variation accounted for by model

R-sq (adj) = 95,61%

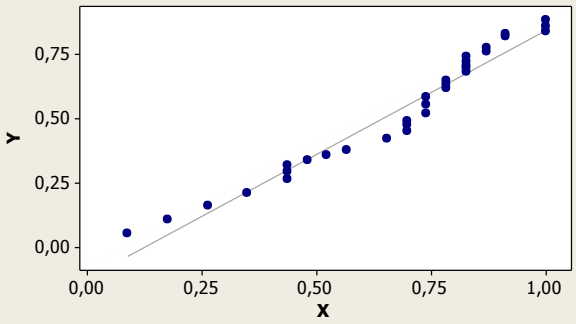
95,61% of the variation in Y can be accounted for by the regression model.

Correlation between Y and X



The positive correlation (r = 0,98) indicates that when X increases, Y also tends to increase.

Fitted Line Plot for Linear Model
Y = - 0,1181 + 0,9603 X

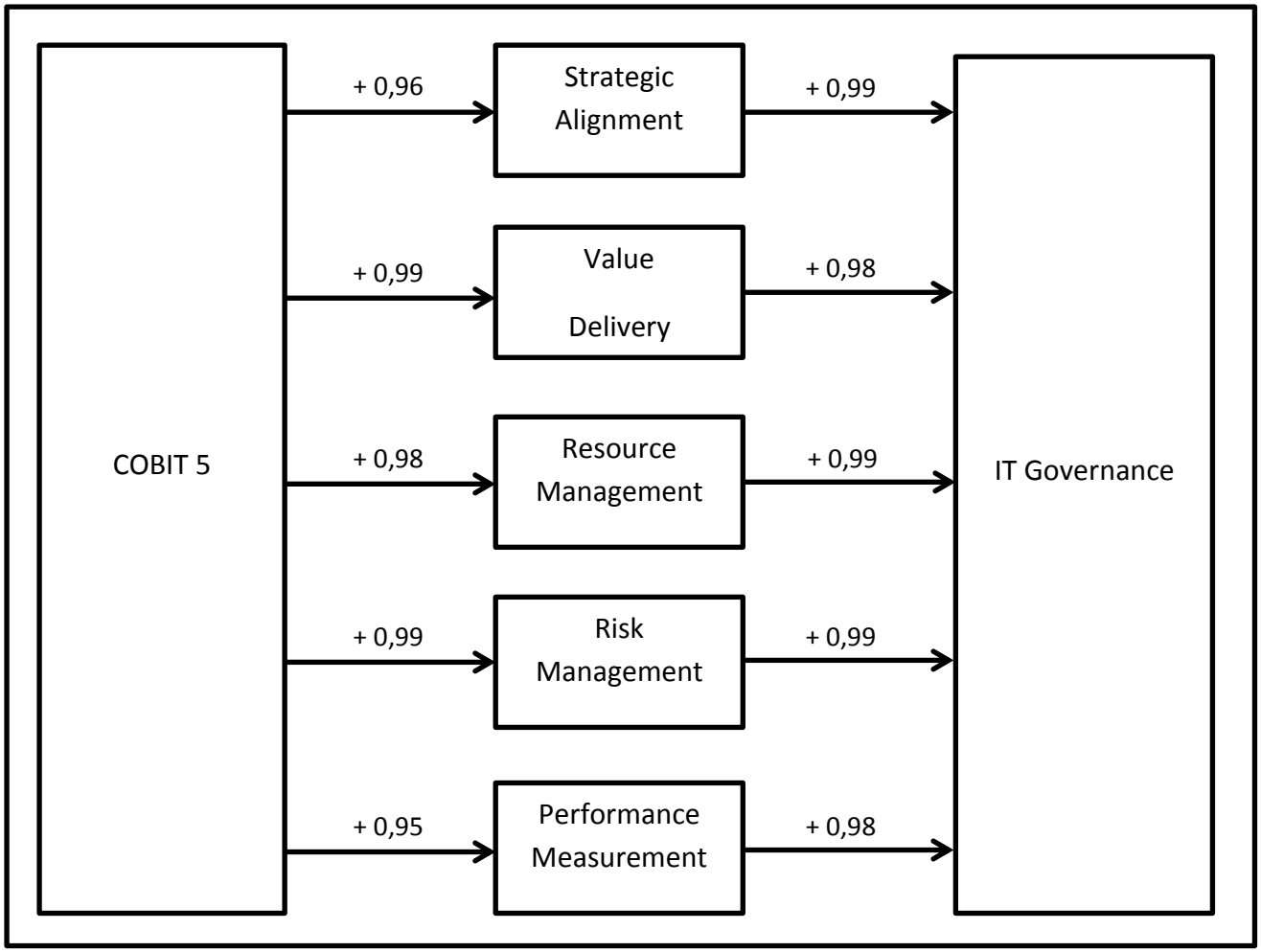


Comments

The fitted equation for the linear model that describes the relationship between Y and X is:
Y = - 0,1181 + 0,9603 X
If the model fits the data well, this equation can be used to predict Y for a value of X, or find the settings for X that correspond to a desired value or range of values for Y.

5 - Discussions and conclusions:

Figure 3-40 : Correlation Statistical results



As it is mentioned previously, the study uses Accumulated Effectiveness as an indicator to IT Governance, and Maturity Level as an indicator to IT Governance Stages. Analysis of IT Management activities, and studying different IT Processes show that COBIT 5 is well implemented in Statoil Company, and it causes well mature or optimised IT Governance Stages (Strategic Alignment Maturity level = 89,74%; Value Delivery Maturity level = 97,58%; Resource Management Maturity level = 81,86%; Risk Management Maturity level = 82,96%; Performance Measurement Maturity level = 100%). The five Graphs: 3-1; 3-2; 3-3; 3-4; and 3-5 show that maturity of each of the IT Governance Stages stills rising over different COBIT 5 steps (processes), except the processes that haven't an impact on this stage, and the missing processes (processes not discovered by the study) such as APO01 (Manage the IT

Management Framework); APO04 (Manage Innovation); APO08 (Manage Relationships); and DSS 08 (Manage Business Process Controls). Their impact on stages is very clear.

Furthermore, statistical results show that there is a very strong correlation between COBIT 5 and maturity level of IT Governance Stages (r(COBIT 5 , Strategic Alignment) = +0,96; r(COBIT 5 , Value Delivery) = +0,99; r(COBIT 5 , Resource Management) = +0,98; r(COBIT 5 , Risk Management) = +0,99; r(COBIT 5 , Performance Measurement) = +0,95).

●How does COBIT 5 contribute to Strategic Alignment solely?

Business & IT Goals, and outcome & performance metrics making the practices clear; maintain IT core competencies at a sufficient level to meet required enterprise strategic objectives; making the company and IT align their objectives; enhancing executive management to take wise strategic initiatives to manage IT's criticality relative to maintenance and growth of the company; making IT participating in overall corporate change-setting and strategic direction; making IT practices and IT culture support and encourage change within the company; Linking and synchronizing company and IT objectives; making the board articulates and communicates the business direction to which IT should be aligned; and making the reporting level of the most senior IT manager commensurate with the importance of IT.

●How does COBIT 5 contribute to Strategic Alignment and Value Delivery together?

Business & IT Goals, outcome & performance metrics, process framework, control objectives, and management practices enhancing IT projects to deliver what they promised.

●How does COBIT 5 contribute to Strategic Alignment and Resource Management together?

Business & IT Goals, outcome & performance metrics, maturity models, control objectives, and management practices providing sufficient IT resources and infrastructure to meet required enterprise strategic objectives; making the company research technology, process and business prospects to set direction for future growth; and Raising the board awareness about the latest developments in IT from a business perspective.

●How does COBIT 5 contribute to Strategic Alignment and Risk Management together?

Business & IT Goals, outcome & performance metrics, process framework, control objectives, and management practices speeding-up the make of major IT decisions, and raising the board awareness about potential conflicts between the company divisions and the IT function.

●How does COBIT 5 contribute to Strategic Alignment and Performance Measurement together?

Business & IT Goals, outcome & performance metrics, IT Balanced Scorecard, COBIT online benchmarks, maturity models, and IT Assurance guide making IT supports the company, complying with regulations and service levels.

●How does COBIT 5 contribute to Value Delivery and Resource Management together?

Performance Metrics, process framework, control objectives, management practices, and maturity models enabling the company to do right things about leveraging its knowledge to increase stakeholder value.

●How does COBIT 5 contribute to Value Delivery and Performance Measurement together?

Performance Metrics, process framework, control objectives, management practices, IT Balanced Scorecard, COBIT online benchmarks, maturity models, and IT Assurance guide making total IT effort and investments transparent, and raising the percentage of revenue spent on IT compared to the industry average.

●How does COBIT 5 contribute to Strategic Alignment, Resource Management, and Risk Management together?

Business & IT Goals, outcome & Performance Metric, maturity models, control objectives, management practices, and process framework Keeping company's internal IT skill decreasing, and making skilled IT resources successfully attracted to the organisation.

●How does COBIT 5 contribute to Value Delivery, Resource Management, and Risk Management together?

Performance Metrics, process framework, control objectives, management practices, and maturity models enabling the board to have a clear view on the major IT investments from a risk and return perspective.

●How does COBIT 5 contribute to Value Delivery, Resource Management, and Performance Measurement together?

Performance Metrics, process framework, control objectives, management practices, maturity models, IT Balanced Scorecard, COBIT Online benchmarks, and IT Assurance guide enabling the board to have a view on how and how much the company invests in IT compared to other like organisations.

●How does COBIT 5 contribute to Value Delivery, Resource Management, Risk Management, and Performance Measurement together?

Performance Metrics, process framework, control objectives, management practices, maturity models, IT Balanced Scorecard, COBIT Online benchmarks, and IT Assurance guide managing IT outsourcing agreements.

●How does COBIT 5 contribute to Strategic Alignment Value Delivery, Resource Management, Risk Management, and Performance Measurement together?

Business & IT Goals, outcome & Performance Metric, process framework, control objectives, management practices, maturity models, IT Balanced Scorecard, COBIT Online benchmarks, and IT Assurance guide Embedding into the enterprise an IT governance structure that is accountable, effective and transparent, with defined activities and purposes and with unambiguous responsibilities.

Graphs 3-6, 3-7, 3-8, 3-9, 3-10 show that IT Governance Effectiveness stills rising over different phases of each stage maturity development, except some steps where the stage hasn't any impact on IT Governance effectiveness and the missing processes (processes not discovered by the study) such as APO01 (Manage the IT Management Framework); APO04 (Manage Innovation); APO08 (Manage Relationships); and DSS 08 (Manage Business Process Controls). These results are supported by the strong correlation between each IT Governance stage maturity, and IT Governance effectiveness (r(SA , ITG) = + 0,99, r(VD , ITG) = + 0,98, r(ReM , ITG) = + 0,99, r(RiM, ITG) = + 0,99, r(PM, ITG) = 0,98).

●How do Strategic Alignment; Value Delivery; Resource Management; Risk Management; and Performance Measurement influence IT Governance effectiveness?

Strategic Alignment influencing IT Governance effectiveness by aligning IT strategy with company strategy; ensuring IT delivers against the strategy; creating the co-responsibility of business and IT; directing the IT Strategy; and ensuring a culture of openness and collaboration among the business, geographical and functional units of the company.

Value Delivery stage provides the appropriate quality, on time and on budget, it clarifies value, it educates and involves stakeholders, it makes formal tracking of business value of IT (business requirements & process change), it provides disciplined approach to project management with a larger role for the business, and it enables the technology standardisation.

Resource Management stage supports inventories of hardware and software, enables practices to train and retain skilled staff, makes procurement policies clear, consistent and enforced, makes infrastructure standardized and interoperable, and enhances service level management.

Risk Management influencing IT Governance effectiveness through raising awareness of IT risks based on proactive and continuous assessment, realising transparency to all stakeholders, establishing responsibility and embedding risk management into the organisation, and ensuring information security.

Finally, Performance Measurement has an influence on IT Governance effectiveness through defining and monitoring measures; providing a management reporting system that feeds back into the strategy; and enabling effective value measurement.

GENERAL CONCLUSION

General Conclusion:

This study explains the central importance of COBIT 5 in IT Governance. It really gives an account of and the reasons for the widespread use of COBIT 5 for implementing IT Governance. It gathers satisfactory information and useful theoretical knowledge about the role of COBIT 5 in IT Governance, and it investigates empirically this role, supporting the theoretical part.

According to empirical investigation results, the study validates hypotheses H01-1(COBIT 5 enables Strategic Alignment), H01-2 (COBIT 5 enables Value Delivery), H01-3 (COBIT 5 enables Resource Management), H01-4 (COBIT 5 enables Risk Management), and H01-5 (COBIT 5 enables Performance Measurement). So, it is confirmed that COBIT 5 enables all IT Governance Stages, and this leads to validate the first global hypothesis (H01: COBIT 5 enables IT Governance Stages).

According to empirical investigation results, the study validates hypotheses H02-1(Strategic Alignment impacts positively IT Governance effectiveness), H02-2 (Value Delivery impacts positively IT Governance effectiveness), H02-3 (Resource Management impacts positively IT Governance effectiveness), H02-4 (Risk Management impacts positively IT Governance effectiveness), and H02-5 (Performance Measurement impacts positively IT Governance effectiveness). So, it is confirmed that IT Governance Stages impact positively IT Governance effectiveness, and this leads to validate the second global hypothesis (H02: IT Governance Stages impact positively IT Governance effectiveness).

The evidence from this study suggests that IT Governance aims to deliver more value from IT investments in a satisfactory method for all stakeholders, meeting the governance objectives. In order to be effective, IT Governance focuses on five stages: Strategic Alignment, Value Delivery, Resource Management, Risk Management, and Performance Measurement. Strategic Alignment is about aligning IT with the business and collaborative solutions. Value Delivery concentrates on optimizing expenses and proving the value of IT. Resource Management aims to optimize knowledge and IT infrastructure. Risk Management purpose is addressing the safeguarding of IT assets, disaster recovery and continuity of operations. Performance Measurement is about tracking project delivery and monitoring IT services. Each one of these stages necessitates a set of factors to become mature. COBIT 5 (Control Objectives for Information and its related Technology) is the latest framework for effective IT Governance. In order to realise maturity of IT Governance Stages, COBIT 5 provides them with Business and IT goals, outcome and performance metrics, process framework, control objectives, Management practices, Maturity models, IT balanced scorecard, COBIT benchmarks and IT Assurance Guidelines.

Recommendations:

The findings of this study have a number of important implications for Statoil about future best practice. Firstly, this study recommends Statoil Company to redefine its management framework in order to provide a consistent management approach to enable the enterprise governance requirements to be met, covering management processes, organisational structures, roles and responsibilities, reliable and repeatable activities, and skills and competencies. Secondly, it should keep continuing innovation management adoption to achieve more competitive advantage, business innovation, and improved operational effectiveness and efficiency. Thirdly, Statoil has to improve the way of managing and formalizing the relationship between business and IT in order to raise its outcomes, increase its confidence, and make its resources' use more effective. Fourthly, Statoil needs to reassess and improve its business process framework to ensure more security of information assets.

The study recommends all companies to make a number of important changes in order to succeed in implementing COBIT 5-based IT Governance. First of all, IT Governance should be integrated within Company Governance, because IT governance ensures that IT goals are met and IT risks are mitigated such that IT delivers value to sustain and grow the enterprise. IT governance drives strategic alignment between IT and the business and must judiciously measure performance. In the second place, the enterprise needs an effective action plan that suits its particular circumstances and needs to get its IT governance initiatives headed in the right direction. Thirdly, any company needs to make its management goal-focused and has the appropriate information on environment and internal processes. In the fourth place, a culture that establishes accountability, encourages cross-divisional co-operation and teamwork, promotes continuous process improvement and handles failure well. Fifthly, it is necessary to make organisational practices enables sound oversight, a control culture, risk assessment as standard practice and appropriate adherence to established standards. Sixthly, the company should establish a rigorous monitoring of and follow-up on control deficiencies and risks. Finally, it is s necessary for the company to understand the complexity of IT, especially for the extended enterprise operating in the networked economy.

References:

Alpaslan Menevse, 2012, Toward Better IT Governance With COBIT 5, ISACA - COBIT FOCUS. 1st Edition. USA.

Broadbent, M. &Weill, P. (1998). Leveraging the new infrastructure – How market leaders capitalize on Information Technology. Harvard Business School Press.

BRIAN K. WILLIAMS & STACEY C. SAWYER, 2011, USING INFORMATION TECHNOLOGY: A PRACTICAL INTRODUCTION TO COMPUTERS & COMMUNICATION: COMPLETE VERSION, 9 th edition.

BearingPoint, (2003), IT governance: Leveraging technology in government, a white paper by BearingPoint Inc.

Center for International Private Enterprise (CIPE), 2002, Instituting Corporate Governance in developing, emerging and transitional economies: A Handbook.

COSO. 1994. Internal Control - Integrated Framework (COSO report). Committee of Sponsoring Organizations of the Treadway Commission.

Derek J. Oliver, Pippa G. Andrews, Elisabeth Judit Antonsson, Steven A. Babb, Steven De Haes, Peter Harrison, Jimmy Heschl, Robert D. Johnson, Erik H.J.M. Pols, Vernon Richard Poole, Abdul Rafeq, John W. Lainhart, and Ravenswood Consultants. 2012. COBIT 5 IMPLEMENTATION. ISACA Publications. 1st Edition. USA.

Ed Chavannes & Debbie Lew. 2006. Conducting an IT Governance Assessment. ISACA The Annual General Meeting Report.

EFFY OZ, 2009, Management Information Systems, THOMSON COURSE TECHNOLOGY , Sixth Edition, Boston, USA

Elizabeth Hardcastle & Ventus, 2011, Business Information Systems, Pearson Education, Harlow.

Erik Guldentops. 2003. *Board Briefing on IT Governance, 2nd Edition*. USA

Ernst & Young, 2013, A globally accepted business framework for the governance and management of enterprise IT, EYGM Limited, United Kingdom.

Floris Ampe, Gert du Preez, Stefanie Grijp, Gary Hardy, Bart Peeters, Dirk Steuperaert . 2012. COBIT 5: Process Reference Guide Exposure Draft. ISACA Publications. UK.

George W. Reynolds, 2010, Information Technology for Managers, CORSE TECHNOLOGY CENGAGE Learning.

Gad J. Selig, 2008, Implementing IT Governance: A Practical Guide to World Class IT Management Using Current & Emerging Best Practices, TCMG 533/MGMT – IT Strategy & Governance, GPS Group, Inc.

Guldentops, E. (2003). IT Governance: Part and parcel of Corporate Governance. CIO Summit, European Financial Management & Marketing (EFMA) Conference, Brussels.

Greg Hughes, 2007, IT Risk Management Report, Symantec Corporation World.

Gary Hardy, Max Blecher, Kris Budnik, Rob Payne, John Thorp, 2012. IT Governance Implementation Guide. IT Governance Institute. USA.

Henry C. Lucas, Jr., 2009, Information Technology for Management, Jacobs Foundation, 1st edition, Zurich, Switzerla.

Henserson, J. C. & Venkatraman, (1993). Strategic alignment: Leveraging Information Technology for transforming organizations. IBM Systems Journal.

Indranil Mukherjee, 2013, CLOUD SECURITY THROUGH COBIT, ISO 27001 ISMS CONTROLS, ASSURANCE AND COMPLIANCE, International Standards Certification, Singapore.

INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA – Board of studies, 2011, Information Technology VOL2, The revised edition.

INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA – BOARD OF STUDIES, January, 2011, INFORMATION TECHNOLOGY, PAPER: 7A, VOLUME – II.

John W. Lainhart, Pippa G. Andrews, Elisabeth Judit Antonsson, Steven A. Babb, Steven De Haes, Peter Harrison, Jimmy Heschl, Vernon Richard Poole, 2012, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA. 1st Edition. USA.

Jan van Bon, 2007, Foundations of IT Service Management Based on ITIL V3, Van Haren Publishing, Zaltbommel, Third edition, first impression.

James A. O'Brien & George M. Marakas, 2007, Enterprise Information Systems, Mc Graw-HILL Irwin, 13th edition.

Jerry Luftman & Tom Brier, 1999. Achieving and Sustaining Business-IT Alignment. CALIFORNIA MANAGEMENT REVIEW VOL 42, NO. I.

J. Luftman, 1996. Competing in the Information Age: Strategic Alignment in Practice. New York, NY: Oxford University Press.

Jukka Perko, 2008, IT Governance and Enterprise Architecture as Prerequisites for Assimilation of Service- Oriented Architecture - An Empirical Study of Large Finnish

Companies, Thesis for the degree of Doctor of Technology, Tampere University of Technology.

Kotter, John; 1996, Leading Change, Harvard Business School Press, USA.

Koen Brand & Harry Boonen, 2007, IT Governance based on CobiT® 4.1 - A Management Guide, Van Haren Publishing, Third edition, first impression.

Ken Laudon & Jane Laudon, 2012, Management Information Systems, 12th edition, Prentice Hall.

Kenneth C. Laudon and Jane P. Laudon, 2011, Essentials of MIS, Prentice Hall, 9th edition.

Kenneth C. Laudon and Jane P. Laudon, 2011, Essentials of Management Information Systems, Prentice Hall, 9th edition.

Mike O. Villegas, 2012, COBIT 5 Update FEI/CFIT Meeting, ISACA. USA.

Mike G. Eccles, Jane M. Nash & Jean-Paul Van Belle, 2003, Discovering Information Systems, Creative Commons Attribution.

M. Garsoux, 2012, COBIT 5 ISACA's new framework for IT Governance, Risk, Security and Auditing, An overview, ISACA, 1st Edition, United Kingdom.

MårtenSimonsson, 2008, PREDICTING IT GOVERNANCE PERFORMANCE: A METHOD FOR MODEL-BASED DECISION MAKING, PHD thesis, Industrial Information and Control Systems KTH, Royal Institute of Technology, Stockholm, Sweden.

Mathew Nicho, 2008, Information Technology Audit: Systems Alignment and Effectiveness Measures, PHD thesis, AUT University, Auckland, New Zealand.

National Computing Centre (UK). 2005. IT Governance Developing a successful governance strategy A Best Practice guide for decision makers in IT. Available on www.ncc.co.uk.

OECD (Organisation for economic co-operation and development). (2004). Principles of Corporate Governance. Paris: Head of Publications Service.

Patrick Soenen, 2012, COBIT 5 Framework, The Institute of Internal Auditors, Belgium, 1st Edition, Available on www.qualified-audit-partners.be

Peter Weill and Jeanne W. Ross, 2004, IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Library of Congress Cataloging-in-Publication Data, Harvard Business School Press.

Peter Weill and Richard Woodham, 2002, “Sate Street Corporation: Evolving IT Governance” working paper 327, MIT Sloan School of Management Center for Information Systems Research, Cambridge.

Peter Weill and Jeanne W. Ross, 2004, Principles of Corporate Governance. Paris: Head of Publications Service.

Richard M. Steinberg ,2004. Enterprise Risk Management - Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission.

Rob Johnson, 2012, Migrating to COBIT 5 for Auditors - ISACA COBIT 5 for Assurance, ISACA, 2nd Publication. USA.

Robert E Stroud, 2012, COBIT 5 : What is new and innovative and of Extreme Value!, ISACA, USA.

Robert S. Roussey, Georges Ataya, Marios Damianides, John Court, 2003, Board Briefing on IT Governance, 2nd Edition.

Steven Hunt & Michael Nelson, 2012, Foundational IT Governance – A Foundational Framework for Governing Enterprise IT adapted from the “ISACA Cobit 5 framework”. ISACA Publications.

SCHWARZ, A; HIRSCHHEIM, R. 2003. An extended plataform logic perspective of TIgovernance: managing perceptios and activities of TI. IN: *Journal of Strategic InformationsSystems*.

Shleifer, A. & Vishny, W. (1997). A survey on corporate governance. The Journal of Finance, 52(2).

S. Shajahan & Priadharshini, 2004, Management Information Systems, NEW AGE INTERNATIONAL (P) LIMITED, PUBLISHERS, New Delhi, India

Tracey Caldwell & Steve Johnson (APM Group), 2012, ISO/IEC 27001 Foundation: A new qualification to help you understand this information security standard.

Van Grembergen (Ed.), 2006, Strategies for Information Technology Governance Hershey, PA: Idea Group Publishing.

Van Grembergen, W., DE Haes, 2008, S. Implementing Information Technology Governance: Models, Practices and Cases. IGI Global.

Wim Van Grembergen, 2004, Strategies for IT Governance, Idea Group Publishing, United States of America.

Webb, P., Pollard, C. & Ridley, G. (2006). Attempting to define IT governance: Wisdom or folly? In Proceedings of the 39th Hawaii International Conference on System Sciences, Hawaii.

www.businessdictionary.com

www.itgovernance.com

www.searchcio-midmarket.techtarget.com

www.searchbusinessintelligence.techtarget.in

www.whatis.techtarget.com

www.blog.infotech.com

www.iisigroup.com

www.pc-history.org

Annexes :

Interview Protocoles :

These are some of the binary questions included in the interview protocols.

	Yes	No
Is an optimum strategic decision-making model for IT achieved, aligned with the enterprise's internal and external environment and stakeholder requirements?		
Is the governance system for IT t embedded in the enterprise?		
Is assurance obtained that the governance system for IT is operating effectively?		
Is the company securing optimal value from its portfolio of approved IT-enabled initiatives, services and assets?		
Is optimum value derived from IT investment through effective value management practices in the enterprise?		
Do Individual IT-enabled investments contribute optimal value?		
Are risk thresholds defined and communicated?		
Is the company managing critical IT-related enterprise risks effectively and efficiently?		
Do IT-related enterprise risks not exceed risk appetite?		
Are the resource needs of the enterprise met in the most optimal manner?		
Is the consistent adoption of resource management principles achieved?		
Is optimal use of resources achieved throughout their full economic lifecycle?		
Is the basis for reporting to stakeholders established?		
Is Reporting complete, timely and accurate?		
Is stakeholder communication effective and requirements are met?		
Are an up-to-date and effective IT control framework and set of policies defined and maintained?		
Are the IT control framework and supporting enablers effectively implemented and communicated?		
Are all aspects of the information technology strategy aligned with the company strategy?		
Is the information technology strategy cost-effective, appropriate, realistic, achievable, enterprise-focused and balanced?		
Is IT considered as a value driver for the enterprise?		
Are there an awareness of the IT strategy and a clear assignment of accountability for delivery?		
Is there an enterprise-appropriate and sustainable enterprise architecture capability?		
Is there a portfolio of enterprise architecture services that supports agile enterprise change?		
Are a common enterprise architecture framework and methodology exist and used to enable re-use efficiencies across the enterprise?		
Is enterprise value created through the qualification and staging of the most		

appropriate advances and innovations in technology, IT methods and solutions?		
Are company objectives met with improved quality benefits and/or reduced cost?		
Is innovation promoted, enabled and forms part of the enterprise culture?		
Is there an appropriate investment mix defined and aligned with enterprise strategy?		
Are sources of investment funding identified and available?		
Are programme business cases evaluated and prioritised before funds are allocated?		
Does a comprehensive and accurate view of the investment portfolio performance exist?		
Are Investment programme changes reflected in the relevant IT service, asset and resource portfolios?		
Have realised benefits been measured?		
Is there a transparent and complete budget for IT?		
Is The allocation of IT resources for IT initiatives prioritised effectively?		
Does a cost management process that compares budgets to actual costs exist?		
Are The IT organisational structure and relationships flexible and responsive?		
Are Human resources effectively and efficiently managed?		
Are IT services identified, defined and catalogued according to enterprise needs?		
Do the service agreements reflect enterprise needs and the capabilities of IT?		
Do IT services perform as stipulated in service agreements?		
Do the suppliers perform as agreed?		
Are supplier risks assessed and properly addressed?		
Are supplier relationships working effectively?		
Are stakeholders satisfied with the quality of solutions and services?		
Are project and service delivery results predictable?		
Are quality requirements implemented in all processes?		
Are relevant data identified and captured to enable effective IT-related risk identification, analysis, management and reporting?		
Does a current and complete risk profile exist?		
Are risk management actions managed as a portfolio of significant?		
Are effective measures for seizing opportunities or limiting the magnitude of loss launched in a timely manner?		
Are relevant stakeholders engaged in the programmes and projects?		
Are the scope and outcomes of programmes and projects linked to enterprise objectives?		
Are programme and project activities planned to address the scope and achieve the expected outcomes?		
Are the programme and project activities monitored, controlled and reported to achieve the plans?		
Are there sufficient programme and project resources to perform activities according to the plans?		
Are the programme and project expected benefits achieved and accepted?		
Are business functional and technical requirements defined and reflect		

enterprise needs and expectations?		
Does the proposed solution satisfy business functional, technical and compliance requirements?		
Have risks associated with the requirements been addressed in the proposed solution?		
Do requirements and proposed solutions meet business case objectives?		
Is the solution which conforms to the design, in accordance with organisational standards, and has appropriate control, security and auditability?		
Is the solution of acceptable quality and has been successfully tested?		
Are approved changes to requirements correctly incorporated into the solution?		
Do maintenance activities successfully address business and technological needs?		
Does the availability plan anticipate the business expectation of critical capacity requirements?		
Do capacity, performance and availability meet requirements?		
Are availability, performance and capacity issues identified and routinely resolved?		
Has Stakeholder desire for the change been understood?		
Is implementation team competent and able to drive the change?		
Is desired change understood and accepted by stakeholders?		
Are role players empowered to deliver the change?		
Are role players enabled to operate, use and maintain the change?		
Is the change embedded and sustained?		
Are authorised changes made in a timely manner and with minimal errors?		
Do impact assessments reveal the effect of the change on all affected components?		
Are all emergency changes reviewed and authorised after the change?		
Are key stakeholders kept informed of all aspects of the change?		
Does acceptance testing meet stakeholders' approval and take into account all aspects of the implementation and conversion plans?		
Are Releases ready for promotion into production with stakeholder readiness and support?		
Are releases promoted successfully and meet expectations?		
Do lessons learned contribute to future releases?		
Are sources of information identified and classified?		
Is knowledge used and shared?		
Knowledge sharing is embedded in the culture of the enterprise?		
Is Knowledge updated and improved to support requirements?		
Are operational activities performed as required and scheduled?		
Are operations monitored, measured, reported and remediated?		
Are licences compliant and aligned with business need?		
Are assets maintained at optimal levels?		
Is configuration repository accurate, complete and up-to-date?		
Are IT-related services available for use?		
Are Incidents resolved according to the agreed service levels?		

Are service requests dealt with according to agreed service levels and to the satisfaction of users?		
Are IT-related problems resolved so that they do not reoccur?		
Is business critical information available to the business in line with minimum required service levels?		
Is sufficient resilience in place for critical services?		
Have service continuity tests verified the effectiveness of the plan?		
Does an up-to-date continuity plan exist and reflect current business requirements?		
Have internal and external parties been trained in the Continuity Plan?		
Do networks and communications security meet business needs?		
Is information processed on, stored on and transmitted by endpoint devices protected?		
Are all users uniquely identifiable and have access rights in accordance with their business role?		
Have physical measures to protect information from unauthorised access, damage and interference when being processed, stored or transmitted been implemented?		
Can security incidents be recognised?		
Are Information assets properly secured throughout their full lifecycle?		
Do complete coverage and effectiveness of key controls to meet business requirements?		
Is the inventory of roles, responsibilities and access rights updated?		
Is the organisation's business continuity plan complete and effective?		
Are business transactions retained completely?		
Do stakeholders approve the goals and metrics?		
Are processes measured against agreed-upon goals and metrics?		
Is the enterprise monitoring, assessing and informing approach effective and operational?		
Are goals and metrics integrated within enterprise monitoring systems?		
Is process reporting on performance and conformance useful and timely?		
Do processes, resources and information meet enterprise internal control system requirements?		
Are all assurance initiatives planned and executed effectively?		
Is Independent assurance that the system of internal control is operational and effective provided?		
Is internal control established?		
Are all external compliance requirements identified?		
Are external compliance requirements adequately addressed?		

ملخص:

ان التعقد المتزايد للبيئة جعل المؤسسة الكبيرة تتبني مفهوم الحوكمة من أجل تحقيق أهداف أصحاب المصالح المختلفة. لكن هذه الحوكمة لا يمكن ان تنجح الا بوجود عامل مساعد. حوكمة تكنولوجيا المعلومات تهدف الى تحقيق استثمار أفضل لهذه التكنولوجيا من شأنه ارضاء كل اطراف المؤسسة. فعالية حوكمة تكنولوجيا المعلومات تتوقف على مدى تركيزها على المراحل التالية: الانسجام الاستراتيجي، اشتقاق القيمة، ادارة الموارد، ادارة المخاطر و قياس الاداء. الانسجام الاستراتيجي يركز على جعل تكنولوجيا المعلومات متلائمة مع نشاط المؤسسة و ما يرتبط به من حلول توافقية. اشتقاق القيمة يهدف الى ترشيد النفقات على تكنولوجيا المعلومات و كذا رفع مستوى خلق هذه الاخيرة للقيمة. ادارة الموارد تهدف الى تحسين المعرفة و البنية التحتية لتكنولوجيا المعلومات. الغرض من وجود ادارة المخاطر هو حماية اصول تكنولوجيا المعلومات، احتواء الاخطار و تحقيق الاستمرارية للعمليات. قياس الاداء يدور حول تتبع انجاز المشاريع و مراقبة الخدمات المقدمة من طرف تكنولوجيا المعلومات. كل مرحلة من هذه المراحل تتطلب مجموعة من العوامل لكي تصبح مكتملة. COBIT5 (الاهداف الخاصة بالرقابة على المعلومات والتكنولوجيا المرتبطة بها) هو آخر الآليات التي ظهرت من اجل تحقيق الحوكمة الفعالة لتكنولوجيا المعلومات. COBIT 5 يهدف الى رفع مستوى نضج و اكتمال مراحل تكنولوجيا المعلومات من خلال امدادها ب: الاهداف المتعلقة بتحقيق التجانس بين تكنولوجيا المعلومات و نشاط المؤسسة، النتائج مع المؤشرات الخاصة بقياس الاداء، هيكل العمليات، الاهداف الخاصة بالرقابة، الممارسات الادارية، نماذج النضج، بطاقة الاداء المتوازنة لتكنولوجيا المعلومات، المقارنة المرجعية و دليل الضمان لتكنولوجيا المعلومات. ستات اويل هي أحد أفضل المؤسسات التي تتبنى تكنولوجيا المعلومات و لها خبرة كبيرة في الميدان؛ هذا ما جعلها نموذج مناسب للدراسة البيانية.

الكلمات المفتاحية: تكنولوجيا المعلومات، أصحاب المصالح، الحوكمة، حوكمة تكنولوجيا المعلومات، الانسجام الاستراتيجي، اشتقاق القيمة، ادارة الموارد، ادارة المخاطر، قياس الاداء، COBIT 5.

Resumé :

La complexité croissante de l'environnement rend les grandes entreprises obligées d'adopter le concept de gouvernance pour atteindre les objectifs fixés par leurs différentes parties prenantes. Cependant, la gouvernance a besoin d'un soutien pour réussir. La Gouvernance TI vise à offrir plus de valeur aux investissements en technologies d'information en adoptant une méthode satisfaisante pour toutes les parties prenantes. Pour être efficace, la gouvernance TI doit toucher cinq volets à savoir: l'Alignement Stratégique, L'Apport de Valeur, La Gestion des Ressources, la Gestion des Risques et La Mesure de la Performance. L'Alignement Stratégique aligne les technologies de l'information avec l'activité de l'entreprise. L'Apport de Valeur; en optimisant les dépenses et en ayant un retour sur investissement quant aux systèmes d'informations. Gestion des ressources vise à optimiser les connaissances et l'infrastructure informationnelle. L'objectif de la gestion des risques est la protection et la sauvegarde des systèmes d'informations en détectant les risques éventuels et en essayant de les éviter, chose qui permet la continuité et la pérennité des opérations. La Mesure de la Performance qui permet le suivi et l'évaluation des projets et des services associés aux TIC . Pour devenir mature, chacun de ces volets nécessite un ensemble de facteurs. COBIT 5 est le dernier modèle de la gouvernance des TI. Visant à atteindre la maturité de chacun des volets précités, COBIT 5 contribue déterminant des objectifs actifs qui concernent l'alignement entre l'activité et la technologie de l'information, les mesures des résultats et de la performance, la structure des opérations, les objectifs de contrôle, les pratiques managériales, les modèles de maturité, la carte balancée des mesures, COBIT 5 benchmarking et le Guide de certification en Technologie de l 'information. Statoil est parmi les meilleurs sociétés qui adoptent la gouvernance TI, et il a une longue expérience dans ce domaine. C'est pur ca il a été choisi comme un modèle adéquat pour l'étude empirique.

Mots clés : la Technologie de l'information, les Parties prenantes, la gouvernance, la Gouvernance TI, l'Alignement Stratégique, l'Apport de Valeur, la Gestion des Ressources, la Gestion des Risques, La Mesure de la Performance, COBIT 5.

Abstract:

The increasing environmental complexity led large companies to adopt the governance concept to meet their different stakeholders' required objectives. However, governance needs a support to be successful. IT Governance aims to deliver more value from IT investments in a satisfactory method for all stakeholders, meeting the governance objectives. IT Governance focuses on five components: Strategic Alignment, Value Delivery, Resource Management, Risk Management, and Performance Measurement. Strategic Alignment is about aligning IT with the business and collaborative solutions. Value Delivery concentrates on optimizing expenses and proving the value of IT. Resource Management aims to optimize knowledge and IT infrastructure. Risk Management purpose is addressing the safeguarding of IT assets, disaster recovery and continuity of operations. Performance Measurement is about tracking project delivery and monitoring IT services. Each one of these stages necessitates a set of factors to become mature. COBIT 5 (Control Objectives for Information and its related Technology) is the latest framework for effective IT Governance. In order to realise maturity of IT Governance components, COBIT 5 provides and elaborates Business and IT goals, outcome and performance metrics, process framework, control objectives, management practices, Maturity models, IT balanced scorecard, COBIT benchmarks and IT Assurance Guide. Statoil is one of the best international companies which adopt IT Governance, and it has a long experience in this area. That's why it has been chosen as an adequate model for empirical study.

Keywords: Information Technology (IT), Stakeholders, Governance, IT Governance, Strategic Alignment, Value Delivery, Resource Management, Risk Management, Performance Measurement, COBIT 5.