Universiteit Leiden

ICT in Business

An Exploratory Examination of the Practicability of COBIT framework

Name: Shengnan (Sophie) Zhang
Student-no: s1124668

Date: 14/03/2013

1st supervisor: Prof. Dr. Hans Le Fever

2nd supervisor: Prof. Dr. Thomas Bäck

MASTER'S THESIS

Leiden Institute of Advanced Computer Science

(LIACS)

Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Abstract

Control Objectives for Information and Related Technology (COBIT) becomes very popular in recent years and is regarded as the most comprehensive IT governance framework. However, its actual utilization and effectiveness are not clear due to the lack of academic studies. Also, the proliferation of other IT standards and best practices, such as ISO27000 series and ITIL, creates great challenges for organizations to understand their relations and to take advantage of them. The main objective of this research is to explore the practicability of COBIT framework and its actual usage in established IT environment. A pilot COBIT program within an IT department was carried out as a case study to collect primary data. The actual usage of COBIT tools is analyzed and compared to their theoretical design. Practical problems and value for adopting COBIT framework are identified and classified. In addition, a COBIT-BSC model is proposed to illustrate a simple way of structuring COBIT control objectives, which is different from the previous usage of Balanced Scorecard. This study will contribute some practical insights to COBIT framework and help organizations take advantage of COBIT as well as other IT control frameworks.

Key words: COBIT, IT Governance, Balanced Scorecard, control frameworks, IT standards, ISO27000 series, ITIL, IT audit

TABLE OF CONTENT

List of Figures

List of Tables

Acknowledgements

I am very grateful for the following people who have contributed a lot of to my thesis.

First of all, I would like to thank my professor Hans Le Fever, who has guided me from the beginning of the design of this study to the final phase of finishing the whole thesis. He gives me a lot insightful advice and encourages me to publish it. It is a great acknowledgement for me to the seven-month’s hard work. My thanks are also extended to Prof. Thomas Bäck, who chairs as the second supervisor to give me guidance.

Secondly, I want to extend my great gratitude to my company supervisor Jan Denys, who offers me the opportunity and all the resources to conduct my research. He takes a lot of time giving me advice and directing me for effective work. He also arranges meetings, interviews, and introduces knowledgeable colleagues to me assisting my research. Also, I cannot thank enough to other colleagues such as Annemieke Wageman, Arno Overgaauw, Jan Constandse, Harro Kooij and many others who lend me great help.

Besides, I am highly appreciated the help from Mr. Bert Martijn Dijkstra, who has great knowledge in IT audit and COBIT. He shares a lot of practical and inspiring thoughts with me from his professional point of view. He also takes great deal of time evaluating my work and giving me suggestions.

Last but not the least, I want to thank my friends, Hao Wang and Yi Wang, who company and support me all the way. Hao spends a lot of time proof reading my thesis and giving me many good advices. I would also like to thank my parents Yong Zhang and Lanyun Liu, for supporting me spiritually throughout my life.

Chapter 1 - Introduction

Statement of the Problems

The increased complexity of IT management and the growing strategic role of IT in business have bring IT governance into an essential part of the corporate governance mechanism. Effective IT governance helps ensure that IT supports business goals, optimises business investment in IT, and appropriately manages IT-related risks and opportunities (ITGI, 2007). It has become a hot topic for scholars and IT professionals in recent years. More and more organizations adopt IT governance to ensure IT efficiency, decrease IT costs and increase control of IT investments (Van Grembergen & De Haes, 2005). A number of IT governance frameworks, such as ITIL, COBIT, ISO 17799 are developed to provide guidance and tools for better IT governance. Among them, Control Objectives for Information and related Technologies (COBIT) is claimed to be the most comprehensive IT governance frameworks. It gives a broad overview of the full life-cycle of IT management.

Despite the growing popularity of COBIT, the actual utilization and effectiveness of COBIT are not clear due to the lack of academic studies. The sources of COBIT related studies mainly come from its publishers: the IT Governance Institute (ITGI) and The Information Systems Audit and Control Association (ISACA). Some researchers (Simonsson, Johnson, & Wijkström, 2007) have pointed out that the biggest disadvantage with COBIT is that it requires a great deal of knowledge to understand its framework before it could be applied as a tool to support IT governance. It is reported (ITGI, 2011) that the usage of COBIT increased from 9% in 2006 to 14% in 2008; however, it decreased to

12.9% in 2010. This trend proves the conclusion from their previous survey that COBIT is not as easily implemented as originally estimated (ITGI, 2006). According to this survey, ITIL and ISO 17799/ISO 27000 are the two most frequently used frameworks. Many executives agree that even though they believe COBIT is a good framework, they prefer to focus on ITIL and ISO27000.

Indeed, the proliferation of various IT standards and best practices such as ITIL, ISO27000, PRINCE2, etc. creates great challenges for organizations to understand these frameworks. The lack of guidance for customization and implementation make it difficult to launch COBIT within established IT environments, especially when some IT frameworks are well in place. How to choose and use various IT frameworks to benefit the organization most? How to start COBIT based on established IT policies and procedures? These questions become big puzzles for management and IT professionals.

Statement of this Research

The main objective of this research is to explore the practicability of COBIT framework and its actual usage in established IT environment. A case study is carried out to gather primary data. A pilot COBIT initiative was rolled out within an IT department of the case company. A great deal of first-degree data is gathered from management, IT professionals as well as IT auditors via questionnaires, interviews and workshop. Practical problems and value for adopting and implementing COBIT framework are identified and classified. In addition, a COBIT-BSC model is proposed to illustrate a simple way of structuring COBIT control objectives. The model categorizes COBIT control objectives into five groups based on its inner relations and the four views in Balanced Scorecard (BSC). It provides an easier way for management to understand COBIT and its relation to other popular IT standards. This study will contribute some practical insights to COBIT framework and help organizations understand and take advantage of COBIT as well as other IT control frameworks.

This paper is organized in nine chapters: the first chapter is this general introduction of this study; the second chapter introduces COBIT and current IT governance frameworks; the third chapter introduces the literature review related to COBIT and IT governance; chapter four clarifies the research questions, research methodology and research design; chapter five describes the case study in details; in chapter six, findings of the literature review and the results of case study are analyzed and discussed; a new model is proposed and explained in chapter eight; the ninth chapter explains the difference between this model and previous works on Balanced Scorecard; Finally, the last section concludes the value of this study and gives recommendations for further research.

Chapter 2 - IT Governance Framework

IT Governance

As part of the scopes of corporate governance, the primary goal of IT governance is to align organization's IT operations with its business strategies. It is defined as "the 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" (Webb, Polland, & Ridley, 2006). Key components of IT governance include defining IT organisational structure and processes, driving alignment of IT goals with business goals, managing risks of IT operations and investments, leveraging IT resources, and ensuring IT performance (ITGI, 2007).

The need for IT governance is accumulated as IT management is becoming increasingly sophisticated due to increased IT costs and strategic value of information and technologies. Also, companies are obligated to comply with various regulations and the requirements such as the Sarbanes-Oxley Act (SOX) in USA, the Third Basel Accord (Basel III) in Europe (Spremic, 2012).

IT Control Frameworks

A control framework is defined as “a recognised system of control categories that covers all internal controls expected in an organisation” by the Institute of Internal Auditors Research Foundation (IIARF). In recent years various groups have developed world-wide known control frameworks and IT governance frameworks to assist IT management issues. Generally, there are three categories of control frameworks according to the study of Nicho (Nicho, 2008):

Business oriented controls:

- COSO (Committee of Sponsoring Organisation);
- SAS (Statement of Auditing Standards);

IT focussed controls:

- ITIL (The IT Infrastructure Library);
- ISO/IEC17799:2000, ISO 27000 ‘family’ (ISO 27001:2005, ISO27002:2005);

Business-IT alignment focused controls:

- COBIT;

Before diving into the discussion of COBIT, the following part will briefly introduce the features of ISO17799/ 27000 and ITIL.

ISO17799/27000

ISO/IEC 17799:2005 Code of Practice for Information Security Management is an international standard, which was published by the International Organisation for Standardisation (ISO) and International Electro technical Commission (IEC). The historic source for the standard was BS 7799-1, which contributed essential parts to ISO/IEC 17799:2005. It was developed and published by the British Standards Institution (BSI), labelled as BS 7799-1:1999. The original British Standard was issued in two parts:

BS 7799 Part 1: Information Technology—Code of Practice for Information Security Management

BS 7799 Part 2: Information Security Management Systems—Specification with Guidance for Use (now known as ISO/IEC 27001).

The goal of ISO/IEC 17799:2005 is to provide information to parties responsible for implementing information security within an organisation. It can be seen as a best practice for developing and maintaining security standards and management practices within an organisation to improve reliability on information security in inter-organisational relationships.

ISO 17799 contains best practices for policies of information security, assignment of responsibility for information security, problem escalation, and business continuity management. This information is organized into 10 sections that contain 36 objectives and 127 controls. These 10 sections and their key elements include:

- Security policy
- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

ITIL

ITIL is a series of eight books that provide consistent and comprehensive best practices for IT service management and delivery. ITIL provides the foundation for quality IT service management. It gives comprehensive best practices of how to plan, design and implement effective service management capabilities, and describes detailed approaches, functions, roles and processes upon which organizations may base their own practices.

The processes of Service Support are:

- Incident management
- Problem management
- Configuration management
- Change management
- Release management

The key practices of Service Delivery are:

- Service level management
- Financial management for IT services
- Capacity management
- IT service continuity management
- Availability management

In its third version, ITIL attempts to move from a process-based framework to a more comprehensive structure reflecting the life cycle of IT services with complete operational phases, namely design, transition and operation, also stresses the importance IT strategy and continual service improvement.

COBIT

Introduction

COBIT is a globally accepted set of tools that executives and IT professionals can use to ensure that IT operations are aligned with business goals and objectives. It was initially created by the Information Systems Audit and Control Foundation (ISACF) in 1996 as part of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) evaluation framework. The IT Governance Institute (ITGI), which founded by ISACA in 1998, released the third edition of COBIT in 2000; the fourth edition was released in 2005, and was revised as 4.1 edition in 2007. Released in 2012, COBIT 5 is the newest framework.

The discussion of this research focuses on COBIT 4.1 as it lays the foundation of COBIT framework and is more widely used. In addition, a large part of COBIT 5 refers back to COBIT 4.1. According to ITGI, COBIT 5 is developed by consolidating and integrating the COBIT 4.1, Val IT 1 and Risk IT2 into one single business framework.

Core Concepts

The underpinning concept of the COBIT framework is that IT should be controlled by concentrating on information that is needed to support the business objectives and requirements. The required information is the result of combined application of IT-related resources and IT processes. The three components, namely information criteria, IT resources and IT processes form the three main dimensions of COBIT conceptual framework (see figure 1):

[1] Val IT™ is a collection of management practices and techniques for evaluating and managing investment in business change and innovation. It is published by ITGI and is closely aligned with and compliments the CobiT framework.
[2] The Risk IT framework is launched by ISACA aiming to integrate the management of IT risk into the overall Enterprise Risk Management.

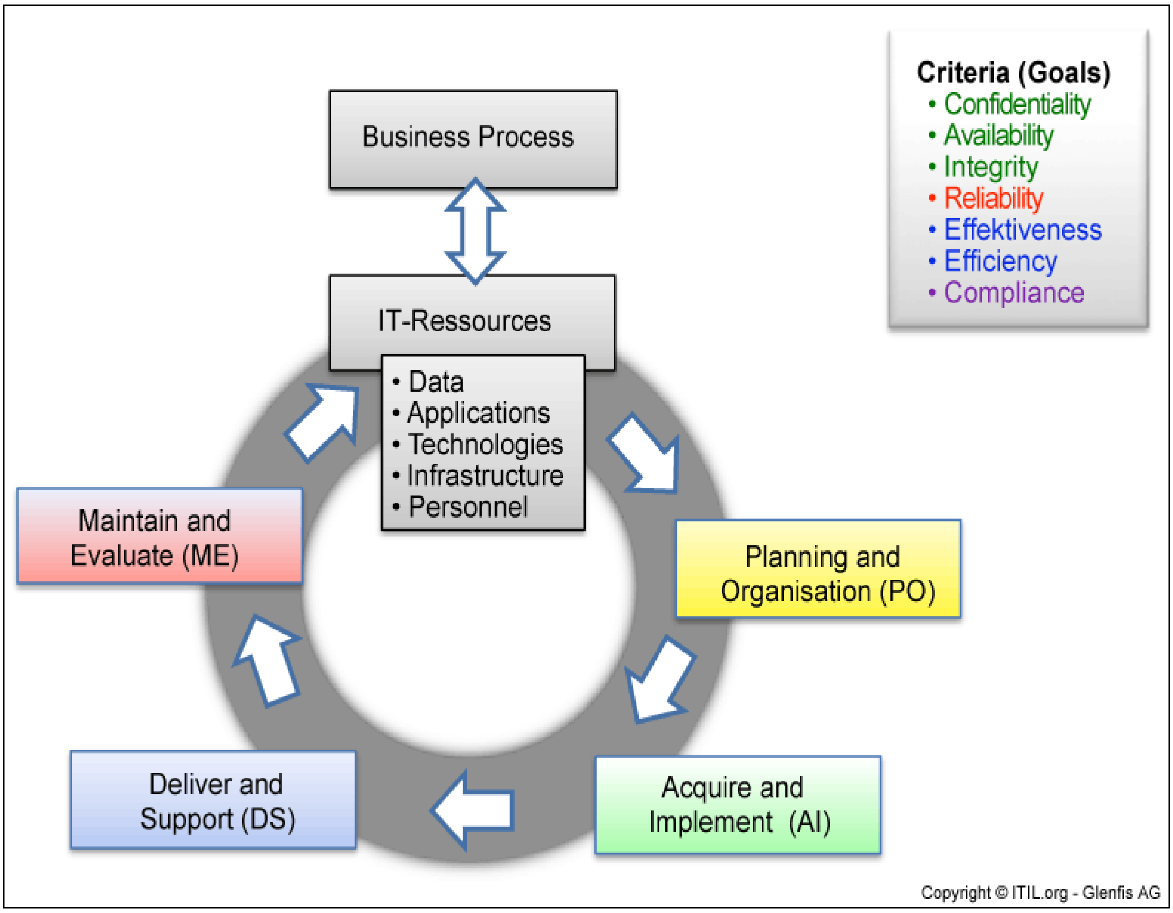


Figure 1: COBIT Core Concepts
Source: ITGI, www.itgi.org

Seven information criteria:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

Five essential IT resources:

- People
- Applications
- Technology
- Facilities
- Data

IT processes:

Each of COBIT's IT processes has a process description and a number of control objectives. COBIT classifies generic IT processes into main domains. The control objectives are identified by a two-character domain reference (such as PO, AI, DS and ME) plus a process number and a control objective number. COBIT 4.1 has 34 high level processes that cover 222 control objectives categorized in four domains, which are mapped and aligned with traditional IT development concept of Plan, Build, Run and Monitor:

-
- Plan and Organise (PO)
- Acquire and Implement (AI)
- Deliver and Support (DS)
- Monitor and Evaluate (ME)

COBIT presents IT activities in a hierarchical structure from the highest domain level to IT processes and to the lowest level of IT activities (see figure 2).

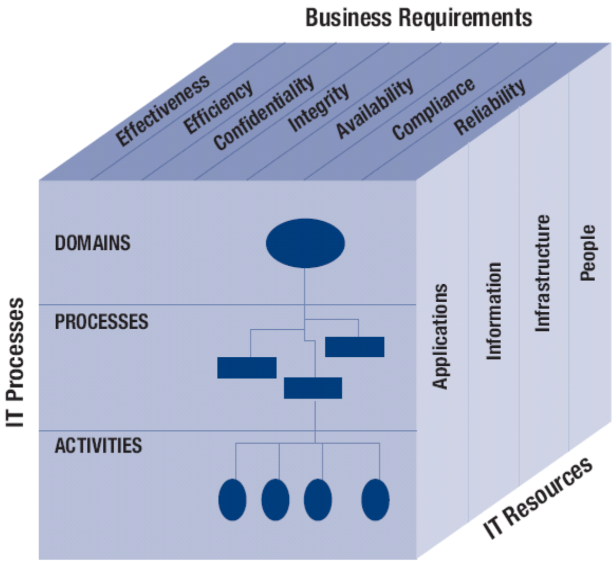


Figure 2 COBIT Structure
Source: ITGI, www.itgi.org

Common COBIT Tools

COBIT contains a set of tools and resources that organizations can use for IT governance and control. Common tools used in COBIT are:

- Performance Goals and Metrics: enabling IT performance to be measured;
- Maturity Model: assisting in benchmarking and decision-making for process improvements;
- RACI Chart: identifying who are Responsible, Accountable, Consulted, or Informed for specific IT process.

Focuses of COBIT

Aiming to bridge the gap between business control models and IT control models, COBIT is designed for management, senior IT professionals and auditors. It helps management balance risk and control in IT investments; provides guidelines for better IT service and performance management; and assists auditors identifying IT risks and establishing adequate IT controls. COBIT is a comprehensive IT governance framework for management to operate at high level; it is not a pure technology standard for IT management. COBIT contributes to enterprise needs by ensuring that:

- IT is aligned with the business;
- IT enables the business and maximizes its benefits;
- IT resources are used responsibly
- IT risks are managed appropriately.

Relations between COBIT, ITIL, ISO27000

ISO17799/27000 & COBIT

As indicated by previous researchers (von Solms, 2005) COBIT is advantageous for information security governance because it provides a larger and wider governance framework and structure that integrates information security into all essential IT processes. However the downside of COBIT is that it is not always very detailed in terms of how to do certain things. On the other hand, ISO17799 is exclusive to information security and only addresses that issue; it provides much more guidance on precisely 'how' things must be done. Despite of its advantages, ISO17799 also suffers the criticism of being very much stand alone.

Solms suggests that it is beneficial to combine these two naturally complement frameworks. Organizations can use COBIT as a high level reference framework in which information security governance is well positioned; and use ISO 17799 as a lower level guideline specifically for information security detailed issues.

ITIL & COBIT

While COBIT focuses on what should be done as an IT governance and control framework, ITIL gives detailed guidance on how thing should be done. Generally, processes fall into DS domain in COBIT are covered by ITIL in a comprehensive manner. Though it tries to capture the full breadth of IT management in its new versions, ITIL are not as comprehensive as COBIT does in term of IT governance. It is mainly used to define and standardize IT service management processes.

Researchers agree that it will create a more powerful IT governance environment if COBIT and ITIL are combined together. On the one hand, COBIT provides a broader context of IT controls and higher views of business priorities; on the other hand, ITIL defines effective ways to translate high level requirements into practical IT services. Figure 3 gives a general illustration of the relations between popular IT governance frameworks.

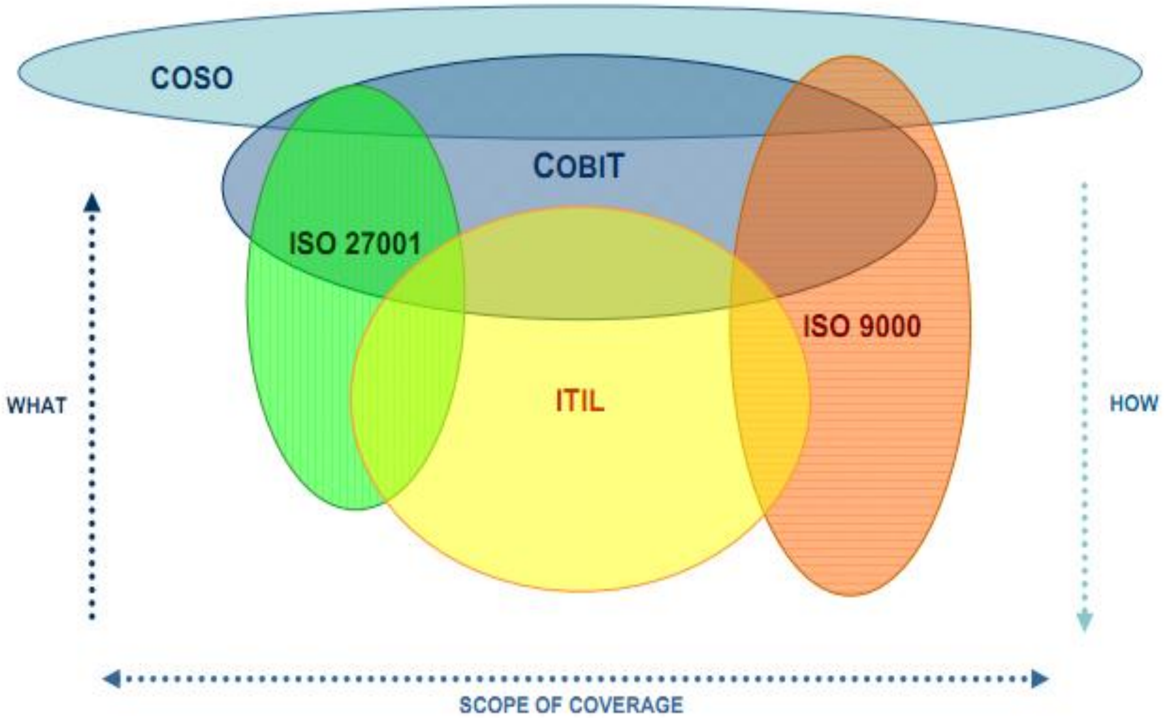


Figure 3 IT governance frameworks

Table 1 compares the differences of these frameworks:

	COBIT	ITIL	ISO27001
Orientation	Audit	Process	Compliance
Scope	IT governance	IT Service MGMT	Information Security
Features	Control objectives	service delivery and support	Information Security Management System
Certification Opportunities	No	Certification of personnel	Certification of organization
Usage	Methodology	guidelines	International Standard
Focus	what	how	how

Table 1: Comparison of IT frameworks

Chapter 3 - COBIT Reviews

Scarce Academic literature

Despite the fact that COBIT is becoming an influential framework for IT control and governance, study on COBIT literature and utilization (Ridley, Young, & Carroll, 2004) reveals that there is relatively little academic literature that has been published investigating the utilization of COBIT. The reason may because that the main sources available for COBIT related publications are through a range of non-academic organizations, mainly the IT Governance Institute (ITGI) and The Information Systems Audit and Control Association (ISACA), which are the publishers of COBIT products. ITIG and ISACA are widely accepted by IT professionals and audit practitioners, but not always referred to by academic researchers. Thus, the majority of COBIT publications appear to have a practitioner focus, very few academically-oriented researches were found. The study also points out that there is a great lack of academic research investigating the range and characteristics of organizations that have utilized COBIT and the outcomes of implementation. Therefore, more rigorous researches in COBIT implementation are highly needed.

This study also categorizes COBIT literature into a three-level framework, which shows clearly the reality of current literature on COBIT. The first level literature are mainly "illustrations of IT governance control document", typically including one or more references to COBIT to explain some aspect of IT governance, the control objectives approach, audit procedures or similar. Discussion tends to be at a theoretical or conceptual level rather than at an applied or implementation level. The second level literature concerns with "reviews of specific IT governance control methodologies", which is also primarily theoretical, either focusing entirely on COBIT, or presenting a comparison between COBIT and one or more other IT governance control methodologies. The third level, “COBIT implementations” has an applied orientation, with literature typically considering the actual use of COBIT in individual organizations, including case studies.

Strengths of COBIT Framework

According to COBIT publications (ITGI, 2007), COBIT addresses a broad spectrum of duties in IT governance and management. It includes the most significant parts of IT management, including those covered by other standards. Although no technical details have been included, the necessary tasks for complying with the control objectives are self-explanatory. Its good practices represent the consensus of experts. It helps management build a good internal IT control system.

These claims are confirmed by some researchers. Rouyet-Ruiz (Rouyet-Ruiz, 2008) argues that COBIT’s origin in auditing makes it a perfect reference frame for internal control of IT. It guarantees performance measurement, value creation and risk management, which are defined in COBIT’s process orientation and in the structured metrics system that measures those processes. Hardy (HARDY, 2006) also agrees that COBIT provides a useful instrument to help organizations get started evaluating their own IT governance systems. The IT governance self-assessment checklist helps auditors to determine each of the COBIT processes. COBIT also provides a sound approach for implementing IT governance related initiatives in a well-controlled environment.

Haes and Grembergen (Van Grembergen & De Haes, 2005) think that COBIT has important business value, including increased compliance, corporate risk reduction, good accountability, and proves to be a useful tool to establish a baseline for process maturity. Colbert and Bowen (Colbert & Bowen, 1996) claim that COBIT is arguably the most appropriate control framework to help an organization ensure alignment between use of Information Technology (IT) and its business goals, as it places emphasis on the business need that is satisfied by each control objective. It has become a de-facto standard especially in financial organizations (Robinson, 2005) and is being used increasingly by a diverse range of organizations throughout the world.

Forrester Research (Symons, 2006) suggests that the starting point for an IT governance framework should be COBIT, because it is the most comprehensive IT governance framework available today. COBIT's strengths lie in its focus on IT management and control and in its breadth, which covers every important IT process. It helps management understand what they need to do to ensure that investments in IT are maximized around business value, do not represent unacceptable risks, comply with all required regulatory requirements, and can be audited.

Weaknesses of COBIT Framework

Some researchers (Simonsson, Johnson, & Wijkström, 2007) think that one of the biggest disadvantages with COBIT is that it requires a great deal of knowledge to understand COBIT framework before it could be applied as a tool to support IT governance or to assess the IT organization's performance. This may be the main reason why practitioners do not use this framework. They explain that there is a lot of incongruence between control objectives, process and business requirements. Even though a vast number of processes, activities, and responsibilities are described in the framework, the connection between them and how they are reflected in the featured maturity model is not specified. The maturity model then mainly serves as a stand-alone analysis tool. Besides, COBIT does not provide guidelines or options for partial implementation, and there is no aid for efficient data collection. Due to these problems, it is not easy for practitioners to understand and use COBIT.

Williams (Williams, 2006) reveals that while there are abundant studies showing that IT governance can bring great value, few studies concentrate on the difficulties that many organisations experience in developing, implementing, maintaining and monitoring effective IT governance structures and processes. Many organisations embarking on the road of IT governance try to seek assistance among peers and external advisors. However, that will incur relatively high costs and may be inhibited by competitive pressures.

Buzina (Buzina, 2011) thinks that COBIT has very complicated structure and too many unpractical measurements for practical use. He gives an example of how complicated it is of linking just one business goal to IT processes (figure 5).

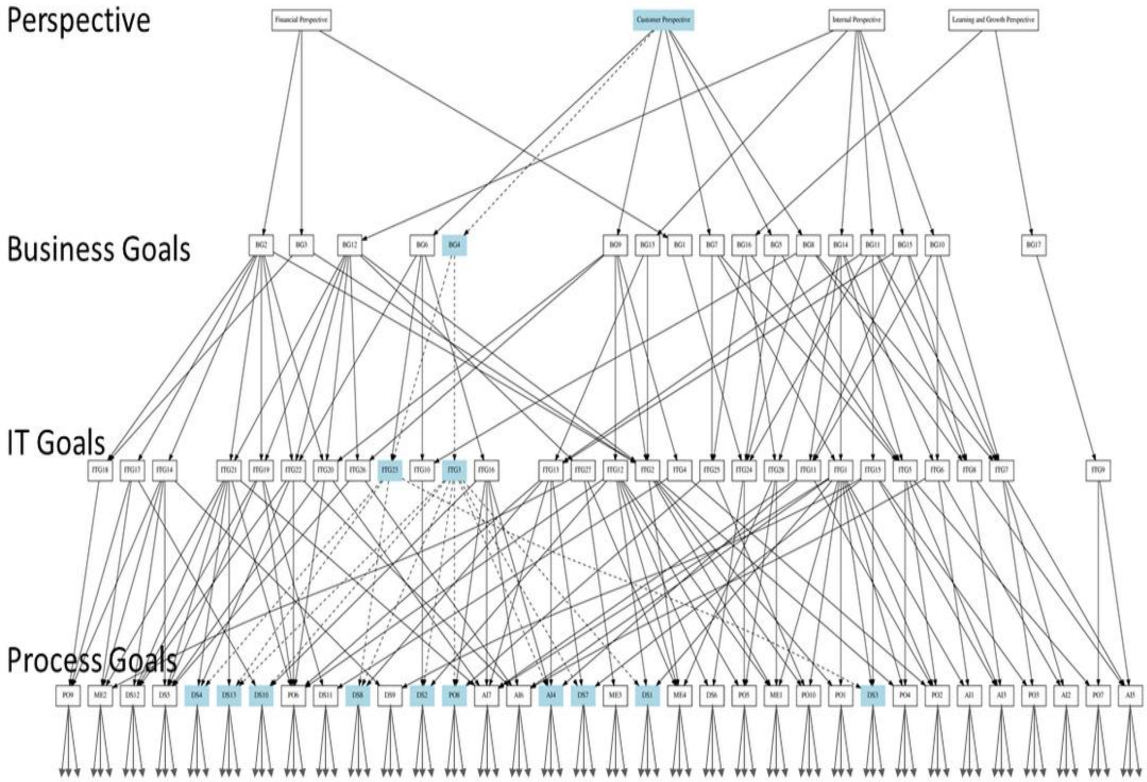


Figure 4: link business goals and IT processes
Source:http://buzina.wordpress.com/2011/08/30/is-cobit-practical-enough-for-real-world-usage/

Nicho (Nicho, 2008) also summarizes some generic analysis of the issues within COBIT framework from both academic and non-academic sources. He concludes that, first of all, the metrics described in COBIT, including Key Performance Indicators (KPIs) and Key Goal Indicators (KGIs), are very generic and hard to trace back to particular goals. Secondly, there is no guidance for best implementation practice. Solms (von Solms, 2005) highlights this limitation by stating that "it (COBIT) is not always very detailed in terms of 'how' to do certain things. The detailed control objectives are more addressed to 'what' must be done". Thus organisations still have to figure out how to implement those processes by themselves.

Another problem is the misuse of Maturity Model. The Maturity Model is an important tool in COBIT to benchmark each of the control processes and identify necessary capability improvements. But the definitions of maturity levels are very generic. In addition, the right maturity level will be influenced by the enterprise's business objectives, the operating environment and industry practices, such as the enterprise's dependence on IT, its technology sophistication, the value of its information, etc. So it is misleading to use maturity level assessing the level of adherence to the control objectives (ITGI, 2007).

The generic nature of COBIT identified by these scholars is admitted by COBIT in its Management Guidelines and Implementation Tool Set:

"…it needs to be emphasised that these guidelines remain generic, generally applicable and do not provide industry specific measures. Organisations will in many cases need to customise this general set of directions to their own environment."

"COBIT is a framework that must be tailored to the organisation. For example, COBIT's IT processes must be compared to the organisation's existing processes, the organisation's risks must be reviewed, and responsibilities for the IT processes must be established. Organisations will in many cases need to customise this general set of guidelines to their specific environment."

However, COBIT does not provide concrete methods or guidelines facilitating organizations to accomplish this kind of customization. Other limitations of COBIT are also mentioned by some researchers, such as lacking a roadmap for continuous process improvement (Anthes, 2004), requiring costly procedural re-engineering (Oliver, 2003), etc.

COBIT Case Studies

Council (Council, 2007) describes a case study of implementing DS5 Ensure Systems Security at South Louisiana Community College. The study attempts to examine the managerial aspects of contributing to or detracting from the success of an IT governance program in higher education. It summarizes many implications and suggestions of the management aspects of IT governance programs for practitioners and academic studies. Council also concludes that IT governance is in its infancy and the area is rich with potential for improvement and research opportunities. His study was one of many steps needed to allow organizations to realize the full benefits of COBIT and similar frameworks.

Hardy (HARDY, 2006) conducts a case study at Unisys, which is one of the leading international IT service companies in the USA. He researches in the effects of having a standardized IT strategy to support Unisys' global operations, align the IT infrastructure with the company's overall business strategy and help comply with SOX. Unisys evaluated its options and adopted COBIT to provide an effective IT control and IT governance framework. As a result of implementing COBIT, business processes within IT were improved and SOX related controls were established. Unisys has also utilized COBIT as a guideline for developing its approach for outsourcing work to third parties by identifying processes and tasks within the domains of COBIT. The results of the study revealed that Unisys' business process within IT had improved as a result of using COBIT for ongoing SOX compliance and other IT governance related projects.

Some researchers (Bowen, Rohde, & Cheung) explore the factors influencing IT governance structures, processes, and outcome metrics. The study reveals that IT governance performance outcomes are associated with a shared understanding of business and IT objectives; active involvement of IT steering committees; a balance of business and IT representatives in IT decisions; and comprehensive and well-communicated IT strategies and policies. IT governance also plays a prominent role in fostering project success and delivering business value. The study also suggests that researchers should carry out more in-depth case studies across a variety of industries. A large scale of surveys of enterprise practices would likely provide more valuable insights.

Conclusions of COBIT Reviews

Based on the review of COBIT studies, we can conclude that there is a great need of academic research on the actual usage of COBIT framework. In theory, COBIT has great value in aligning IT operations with business strategies. It provides a comprehensive view over the full life-cycle of IT management and helps integrate other IT standards. Also, it has great strengths in assisting internal control and auditing processes. However there are also many weaknesses identified by researchers, such as the lacks of guidance, complex structures. The number of case studies on COBIT is very limited and most of them are provided by ITGI. Related academic studies are in great paucity.

In order to fill this gap and add more practical insights on COBIT, this research will explore the actual usage of COBIT by a case study, investigating how COBIT is used in established IT environment, examining the practical values and problems of COBIT.

Chapter 4 - Research Design

Research Questions

This study attempts to investigate the main research question of "How COBIT is used in established IT environment?"

The main research question can be divided into the following secondary research questions:

- RQ1: What are the fundamental methodologies and common tools in COBIT framework? How are they used?
- RQ2: What IT standards or frameworks are being used for IT governance? How they are used?
- RQ3: What is the practical value of COBIT in established IT environment?
- RQ4: What are the practical problems for adopting and implementing COBIT?

Research Methodology

This study will use qualitative research methodology to explore the practicability of COBIT framework and how it is implemented in established IT environment. Qualitative research is an empirical research method which is widely used in social, behavioural, organisational and evaluative research (Kaplan & Duchon, 1998). Most data in qualitative research are not normally in the form of numbers and to be collected from various sources, which involves many techniques such as data description, decoding, translation, etc. to understand their meaning in a natural setting (Van Maanen, 1979). A qualitative approach is deemed suitable for this research as it requires primary data from various points of views of certain participants and in a particular IT organization context.

To collect primary data regarding the implementation of COBIT methodologies in real-life context, a case study is needed. Case study is a useful research method to study complex issues. According to Yin (Yin, 1994), a case study is “an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident.” Case studies emphasize detailed contextual analysis of a limited number of events or conditions and their relationships. Researchers have used the case study research method for many years across a variety of disciplines.

There are several categories of case study. Yin notes three categories, namely exploratory, descriptive and explanatory case studies. Other researchers also mention about other categories. For instance, McDonough (McDonough & McDonough, 1997) includes interpretive and evaluative case studies as two other categories. Regarding the interests of this research, it is an exploratory study which investigates the practicability of COBIT framework and its value and weaknesses in established IT environment. As data will be only collected in one organization, this research is a single case study.

A key strength of the case study method is that it involves multiple sources and techniques in the data gathering process. Surveys, interviews, documentation review, observation, etc. are common tools to collect data. To evaluate the practicability of COBIT methodologies in established IT context, we have to obtain primary data, such as organizational structure, existing IT governance frameworks, IT operational processes, performance, measurements, comments and opinions towards COBIT methodologies from a range of related stakeholders in the case context. Thus documentation review, survey, meetings and interviews are common instruments used to collect these data.

Despite various advantages in that it can present data of real-life situations and provide better insights into the detailed behaviours of the subjects of interest, Yin notes that case studies also suffer criticisms for its lack of rigour and inability to provide a generalising conclusion. One way of overcoming this is by triangulating the study with other methods in order to confirm the validity of the process.

Design of Case Study

Based on the above methodology, this research will be conducted in a combination of literature review, case study and structured interviews. The initial phase is literature review which focuses on studying the fundamental methodologies and common tools in COBIT framework, the utilization of other IT governance frameworks and attempt to identify gaps between the theories and practical problems. This mainly focuses on the Control Objectives, Maturity Model and its relations with other IT governance frameworks. Then a case study is conducted within the context of LogisticX Benelux Infrastructure division, where a pilot COBIT project is undergoing. Data are mainly collected through document reviews, observations, meetings, workshops, questionnaires and interviews with IT managers, team leaders and other related stake holders. The steps and related instruments are summarized in the following figure 6.

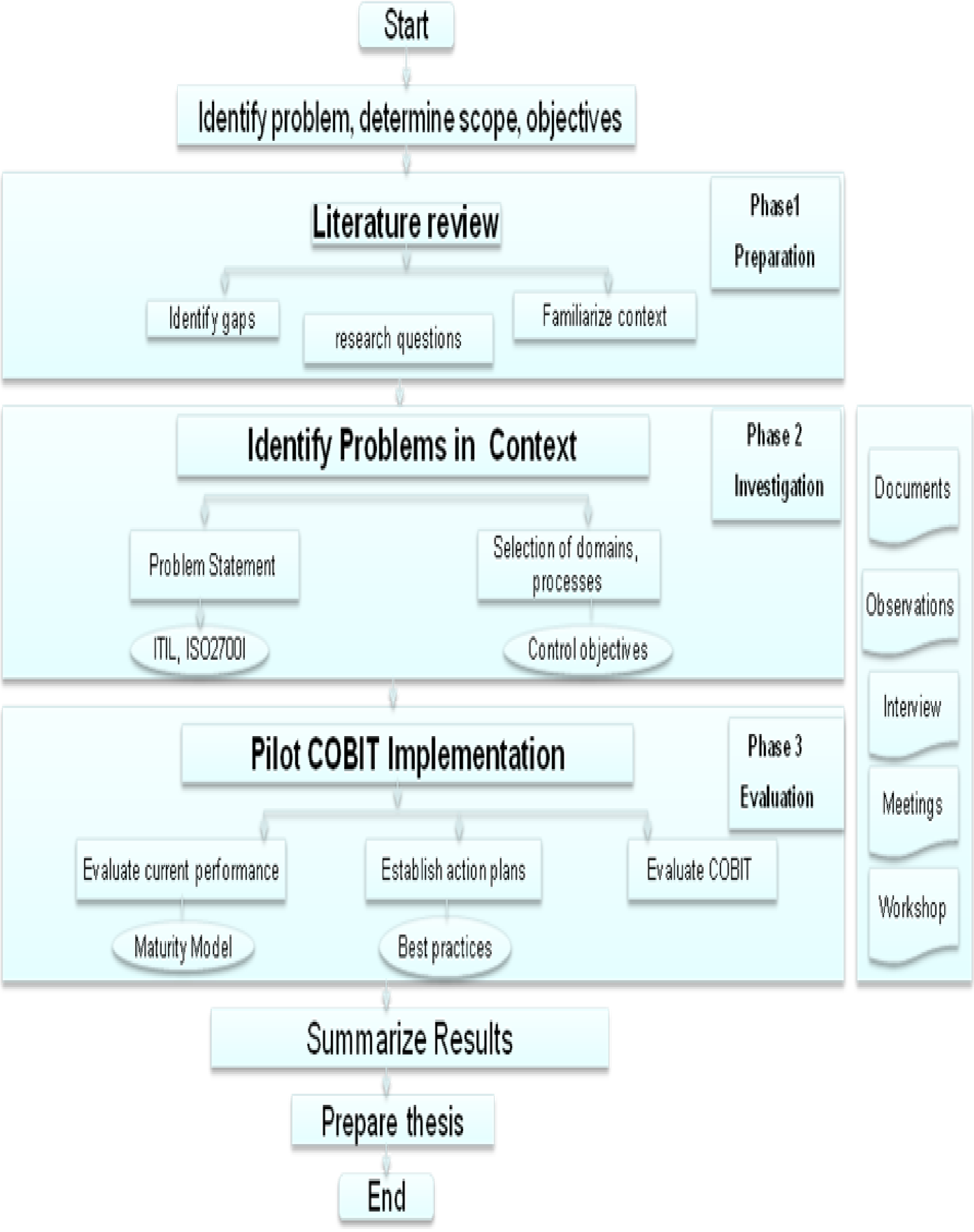


Figure 5: Design of Case Study

Chapter 5 - Case Study

In consideration of confidentiality issues, the company in this case study is referred as LogisticX and its Benelux business unit will be referred as BNL BU. All the figures revealed here are only simple illustrations, not indicating the actual situations. The details of the questionnaires and results are presented in Appendix.

Case Study Context

LogisticX & Benelux Business Unit (BNL BU)

LogisticX is an international courier delivery services company. The firm has fully owned operations in 65 countries and delivers documents, parcels and pieces of freight to over 200 countries, which are covered by a wide range of road and air transportation networks in Europe, the Middle East and Africa, Asia-Pacific and the Americas. BNL BU is a local business unit of LogisticX. Its main business is operating in Belgium, Netherlands, and Luxemburg.

Information & Communication Services (ICS) Division of BNL BU

Department of Information & Communication Services (ICS) is an internal supplier to the regional operating of BNL BU, delivering ICS solutions and services to LogisticX internal users and customers. ICS are not only responsible for standard IT issues, but also provide support and consultancy on all interfaces between IT and the business.

Currently, there are five main departments in ICS BNL BU, namely Business System development, Service Desk, Customer Interface Technology, Service Development & Control, and Infrastructure. The general context of this case study is within ICS BNL BU, and the detailed implementation and evaluation of COBIT are mainly conducted in ICS Infrastructure department.

The goal of ICS BNL BU is to provide excellent information services:

- Develop and manage strategy and priorities;
- Develop ICS customer budget plans and review performance;
- Design and manage ICS infrastructure
- Develop and provide new ICS products and services
- Deliver day-to-day ICS service

Infrastructure Department of ICS

The Infrastructure department is responsible for managing all information and communication infrastructure of ICS BNL BU. The main responsibilities of the infrastructure department include:

- managing all ICS components
- monitoring technical and security policies
- managing the data centre
- monitoring fundamental support contracts with third or fourth line infrastructure suppliers
- managing and maintaining user data
- refreshing and maintaining technical infrastructure
- implementing technical projects

The general context of this case study is within ICS BNL BU, and the detailed implementation and evaluation of COBIT are mainly conducted in ICS Infrastructure department.

Motivation for COBIT

Operational Excellence Programme

Infrastructure team started an Operational Excellence program in 2010 and have conducted an IT performance evaluation based on COBIT Maturity Model. Each process was evaluated based on the five maturity attributes:

- Awareness and communication
- Policies and standards
- Tools and automation
- Skills and expertise
- Responsibility and accountability

They evaluated 9 control objectives as listed below, and all these processes are below 3 in maturity according the final results. The team set target maturity level to be 3 for all the processes and made action plans for improving maturity levels in 2010.

ICS infra process
DS7 Train users
DS5 Systems security
PO3 Technology direction
DS12 Physical environment
DS4 Continuous Service
DS13 Operations
AI3 Acquire Infrastructure
ME1 Monitor
DS2 Third party

Table 2: COBIT 2010

Due to certain reasons, this program didn't continue in the following years. In 2012, they had a detailed process evaluation of DS3 - Manage Performance and Capacity for its five sub-control objectives by students from Antwerp University.

DS3 - Manage Performance and Capacity

DS3.1 - Performance and Capacity Planning
DS3.2 - Current Performance and Capacity
DS3.3 - Future Performance and Capacity
DS3.4 - IT Resources Availability
DS3.5 - Monitoring and Reporting

Table 3: COBIT 2012

Resume COBIT Implementation

In meeting with more demanded quality and safety requirements from customers and partners of LogisticX, all business units of BNL BU including ICS are subjected to all kinds of internal and external audit programmes. In addition, ICS department obtained the ISO27001 certification in 2012, which requires their continuous commitment for assuring and improving IT operations and management. In that regards, the infrastructure manager intends to take the initiative of implementing COBIT best practices, working proactively to meet the control objectives.

Phased COBIT Case Study

It is acknowledged both from literature studies and interviews of this case study that COBIT requires great efforts for customization and adaptation in order to achieve desired objectives. It is crucial to integrate COBIT with existing internal policies and procedures, and tailor the standards and best practices to suit specific requirements for an IT department. Therefore, different phases were designed for the case study.

Phase 1-Understanding IT Processes

Several different sources of information were used for understanding existing IT processes and performance of ICS BNL BU and Infrastructure department, such as interviews, documentation review and observations. Both first degree and second degree of data are collected. The aim is to avoid the limitations of incomplete interpretation of single data source.

Interviews

First Round Interviews

Interviews at this period were mainly conducted with IT managers. It started with a few semi-structured interviews with the infrastructure manager to achieve the following goals:

- Clarify the motivation and expectation of implementing COBIT
- Familiarize the general structure and processes of ICS and main responsibilities of infrastructure department
- Identify a list of people who have knowledge for the following interviews
- Identify available resources, such as documents, tools, shared folders, etc.
- Suggest proper methods for conducting this case study
- Plan a rough timeline of key steps

Second Round Interviews

The second round interviews were with team leaders, project managers from infrastructure department, and also managers and IT officers from other ICS departments. The interviewees were selected based on their responsibilities and working experience. The interviews were designed to be semi-structured, where questions on specific topics regarding the roles of interviewees were planned, but also allowing for improvisation and exploration of interviewees for related topics and issues. The main goal was to capture a broad view of IT processes within ICS and infrastructure department.

During each interview, the objectives of the interview and the use of data were communicated to the interviewees. Some interviews were recorded given the consent of the interviewees. Summaries of the interviews were confirmed by interviewees afterwards, assuring the reliability and accuracy of the researcher's understanding and interpretation.

Documentation Review

The main sources of documentations describing existing ICS IT processes are scattered in different places, such as corporate Intranet, shared folders, managing tools and software. Because the BNL BU has to comply to central IT policies and procedures, the study of central IT policies are crucial too. In that case, the tactic was to look into available documents as much as possible to get the most comprehensive picture of existing IT processes. A general categories and examples of the studied documents are listed as the following:

- Central IT policies and procedures
- Local IT policies and procedures
- Responsibility charts, descriptions
- Manuals, reports, minutes of meetings
- IT auditing reports
- Demonstrations of managing tools and software

Observations

Since the author stayed in the head office of LogisticX for seven months, observations were done intentionally and unintentionally, covering many intangible aspects of IT operations, such as how each department or team work with the others; how people interact and communicate issues and problems; the culture of the company; the work ethics of employees, etc. The researcher also visited their data centres, computer rooms and other local offices. Different levels of personnel and embedded practices were observed in the meanwhile.

Summary of Current IT Processes

ICS Mission and Processes

The mission of ICS is to create an ICT environment that provides services and products based on business needs. It is an obligation of ICS to constantly focus on and contact with business and clients. The goal of ICS is to provide excellent information services by:

- Developing and managing strategy and priorities;
- Developing ICS customer budget plans and reviewing performance;
- Designing and managing ICS infrastructure;
- Developing and providing new ICS products and services
- Delivering day-to-day ICS service

Accordingly, there are 5 main ICS departments supporting these goals, namely Business System development, Service Development & Control, and Infrastructure, Customer Interface Technology (CIT) and Service Desk.

Core ICS Procedures

The core of ICS operations are the Change Management, the Incident Management and the Problem Management procedures. Every internal or external process, guideline or procedure communicates and interact with these three core procedures.

In order to standardize IT processes and provide consistent quality of services, IT support and delivery provided by ICS operations are mainly based on ITIL framework, which groups 21 IT processes into 4 main groups.

Among these 21 processes, Incident Management, Problem Management and Change Management are at the core of ICS operations. As revealed from the interviews, everyone within ICS can’t do anything without running through these procedures. ICS relate most of their work to these procedures because what they do mostly either leads to a change, an incidence, or a problem. Most problems coming from incidences that cannot be solved quickly and need further root-cause analysis. Incident Manager and Change Manager will make documents with all kinds of measurements reporting the process performances. The documents are first generated from standard reports, and then revised by the managers. All IT departmental managers will review these reports and solve problems falling into their responsibilities.

Responsibilities of Infrastructure Department

The Infrastructure department is responsible for managing all information and communication infrastructure, such as data centre, network, telephony, etc. It aims to provide a stable and efficient ICS platform. The main responsibilities of the infrastructure department include:

- managing all ICS components
- monitoring technical and security policies
- managing the data centre
- monitoring fundamental support contracts with third or fourth line infrastructure suppliers
- managing and maintaining user data
- refreshing and maintaining technical infrastructure
- implementing technical projects

The department is divided into three teams:

- Communication Services (Voice and Network): management of the wireless, local and international network and voice infrastructure (fixed telephony and contact centres);
- Operation Equipment Services: structural management and support of all installations to measuring, weighing, scanning and sorting;
- Windows Services: structural management and support of all windows based systems.

There is also a technical project leader who is responsible for carrying out technical projects on infrastructure.

Phase 2-Selection of Control Objectives

As COBIT is a comprehensive framework that covers the full lifecycle of IT processes, it is advisable to select a subset of all the control objectives for concerned IT groups. It is quite obvious that the PO and ME domains are on the management level, while the AI and DS are more on the operational level. However, there is no clear cut between these domains; control objectives are always overlapping with each other. Besides, there are also organizational or structural considerations for different levels of controls and responsibilities for certain areas.

For example, In LogisticX, central ICS plays the leading role in establishing general policies and procedures. There is a Central Process Model in central ICS addressing all IT management issues, including IT strategy, IT governance framework, Plan-design-build-run IT lifecycle. The discretion of local ICS for different issues varies a lot. For example, local ICS should adhere strictly to central policies for portfolio management, project management, IT financial management. Some services like network and security are provided by Central ICS based on SLAs; thus local ICS are not responsible for these areas.

So the first step using COBIT framework was to narrow down the scope of control objectives, removing processes that Infrastructure department were not empowered to address, focusing on the most relevant processes. This was achieved by a two-level assessment, namely a high level assessment and a low level assessment.

High level assessment

The high level assessment is an evaluation the importance of 34 COBIT control objectives from ICS Management Board. It is carried out by a survey for all members of ICS management board, including the director of ICS and the six departmental managers:

- Director of ICS and Service

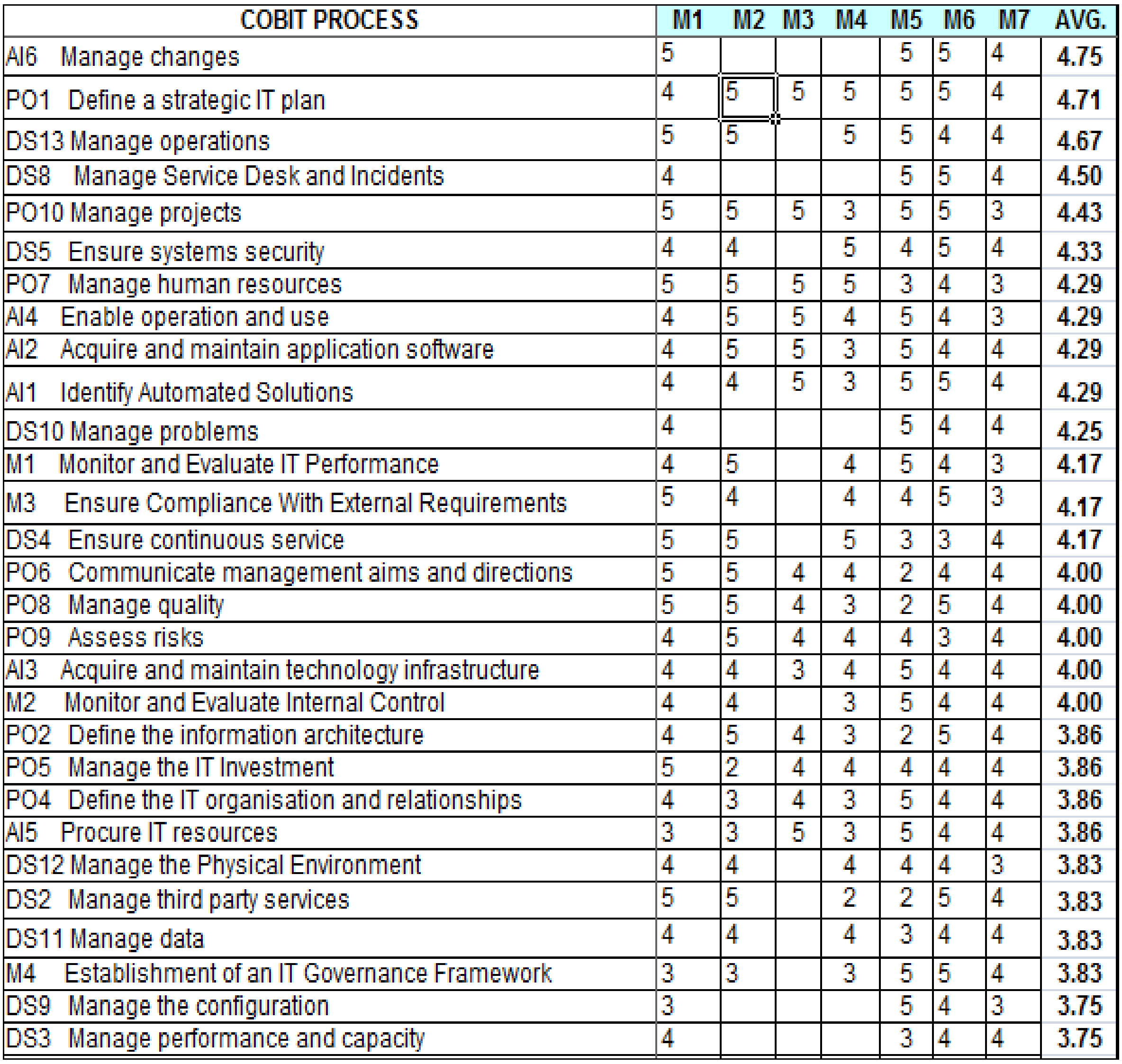
- ICS Service Development & Control Manager
- ICS Service Desk Manager
- ICS Infrastructure Manager
- Service Desk Manager of Head Office
- ICS Business Systems Development Manager
- ICS CIT (Customer Interface Technology) Manager

The survey is designed to gather a general evaluation of all 34 COBIT control objectives based on main responsibilities and concerns of ICS BNL BU.

The evaluation of the desirability of control objectives is based on a scale of 1-5(table 4), from the least useful to most useful. The aim is to get a general assessment of all of the COBIT's 34 control objectives based on the business requirements and IT realities of ICS BNL BU. The final score is the average of evaluation of all the participants (figure 7). Complete results are shown in Appendix B: High Level Assessment.

Score	Process Importance
1	Inapplicable
2	Can be useful
3	Is useful
4	Is desirable
5	A must

Table 4: process evaluation



COBIT PROCESS	M1	M2	M3	M4	M5	M6	M7	AVG.
AI6 Manage changes	5				5	5	4	4.75
PO1 Define a strategic IT plan	4	5	5	5	5	5	4	4.71
DS13 Manage operations	5	5		5	5	4	4	4.67
DS8 Manage Service Desk and Incidents	4				5	5	4	4.50
PO10 Manage projects	5	5	5	3	5	5	3	4.43
DS5 Ensure systems security	4	4		5	4	5	4	4.33
PO7 Manage human resources	5	5	5	5	3	4	3	4.29
AI4 Enable operation and use	4	5	5	4	5	4	3	4.29
AI2 Acquire and maintain application software	4	5	5	3	5	4	4	4.29
AI1 Identify Automated Solutions	4	4	5	3	5	5	4	4.29
DS10 Manage problems	4				5	4	4	4.25
M1 Monitor and Evaluate IT Performance	4	5		4	5	4	3	4.17
M3 Ensure Compliance With External Requirements	5	4		4	4	5	3	4.17
DS4 Ensure continuous service	5	5		5	3	3	4	4.17
PO6 Communicate management aims and directions	5	5	4	4	2	4	4	4.00
PO8 Manage quality	5	5	4	3	2	5	4	4.00
PO9 Assess risks	4	5	4	4	4	3	4	4.00
AI3 Acquire and maintain technology infrastructure	4	4	3	4	5	4	4	4.00
M2 Monitor and Evaluate Internal Control	4	4		3	5	4	4	4.00
PO2 Define the information architecture	4	5	4	3	2	5	4	3.86
PO5 Manage the IT Investment	5	2	4	4	4	4	4	3.86
PO4 Define the IT organisation and relationships	4	3	4	3	5	4	4	3.86
AI5 Procure IT resources	3	3	5	3	5	4	4	3.86
DS12 Manage the Physical Environment	4	4		4	4	4	3	3.83
DS2 Manage third party services	5	5		2	2	5	4	3.83
DS11 Manage data	4	4		4	3	4	4	3.83
M4 Establishment of an IT Governance Framework	3	3		3	5	5	4	3.83
DS9 Manage the configuration	3				5	4	3	3.75
DS3 Manage performance and capacity	4				3	4	4	3.75

Figure 6: process evaluation results

Low level assessment

The low level assessment is a selection of the most relevant control objectives for infrastructure team. The result of the survey from ICS Management Board is used as a reference for prioritization and selection of the most relevant control processes for infrastructure team. It aims to narrow down the scope of COBIT implementation. In the end, 10 processes (table 5) were chosen based on its rank from the evaluation of Management Board and also the infrastructure manager. Most of them coincide with the main responsibilities of Infrastructure team.

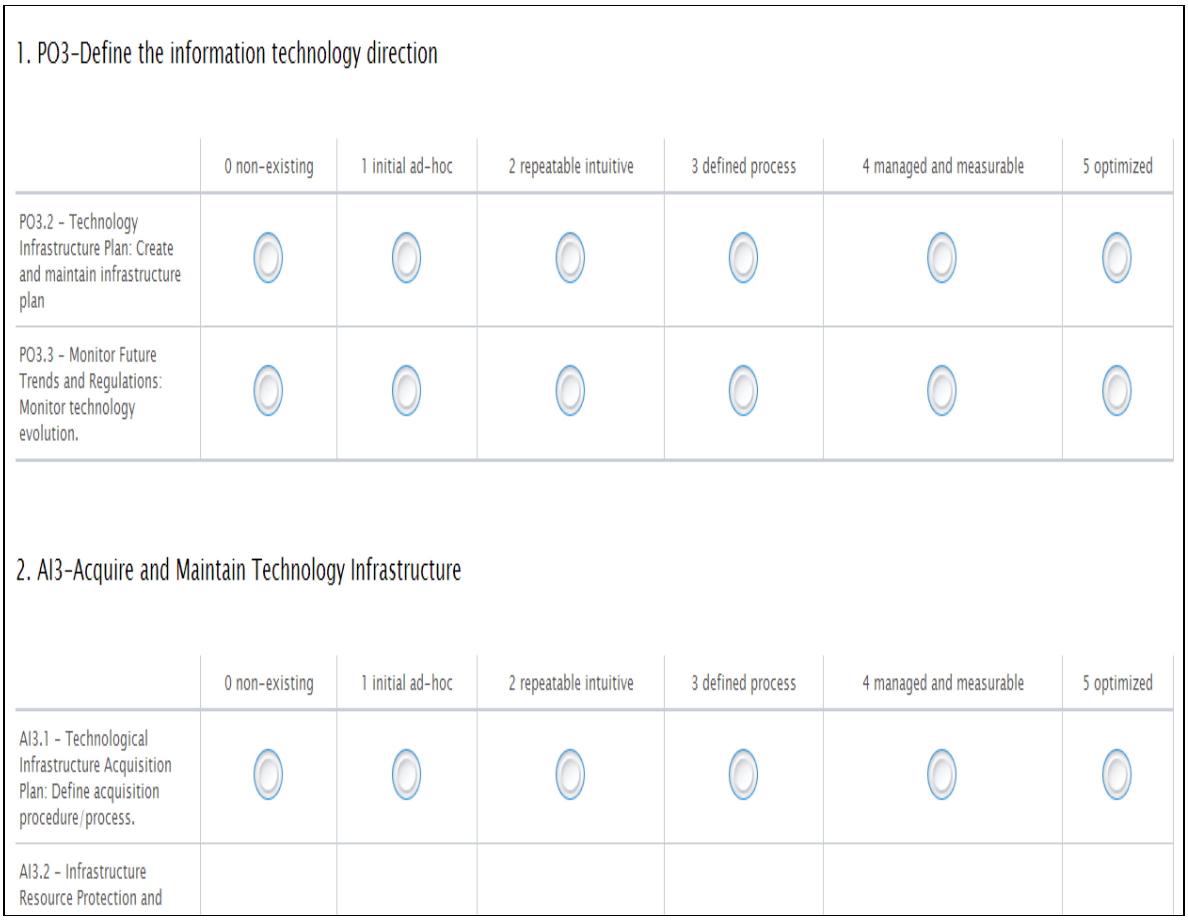
Selected 10 Process
DS7 Train users
DS5 Systems security
PO3 Technology direction
DS12 Physical environment
DS4 Continuous Service
DS13 Operations
AI3 Acquire Infrastructure
ME1 Monitor
DS2 Third party
DS3 Performance& capacity

Table 5: 10 COBIT processes

Phase 3-COBIT Implementation

Evaluating Maturity Level

The evaluation of the maturity level of 10 selected control objectives was carried out within the whole infrastructure team, including team leaders, engineers, technicians, specialists and the infrastructure manager. It was designed as an on-line survey (http://www.instant.ly/s/vzcGq) using the survey tools provided by Instant.ly, a free on-line survey platform. The survey is anonymous, asking the profile of the participant and his or her assessment of the maturity of the stated processes. Figure 7 shows a screen shot of the on-line survey. Full content is in Appendix B: Low Level Assessment.



1. PO3-Define the information technology direction

	0 non-existing	1 initial ad-hoc	2 repeatable intuitive	3 defined process	4 managed and measurable	5 optimized
PO3.2 - Technology Infrastructure Plan: Create and maintain infrastructure plan	○	○	○	○	○	○
PO3.3 - Monitor Future Trends and Regulations: Monitor technology evolution.	○	○	○	○	○	○

2. AI3-Acquire and Maintain Technology Infrastructure

	0 non-existing	1 initial ad-hoc	2 repeatable intuitive	3 defined process	4 managed and measurable	5 optimized
AI3.1 - Technological Infrastructure Acquisition Plan: Define acquisition procedure/process.	○	○	○	○	○	○
AI3.2 - Infrastructure Resource Protection and						

Figure 7: screen shot of on-line survey

In the survey there were 10 high level control objectives relevant to Infrastructure team; for each of the ten processes, there are a few detailed control objectives. Participants were asked to evaluate each of the detailed control objectives based on the scale of COBIT Maturity Model. Participants were asked to assess as many processes as possible that they are aware of within Infrastructure team and choose non-existing if they didn't think the stated process was established.

In the end, there were 9 valid fill-ins of the survey. The maturity evaluation results are summarized in table 6:

Process	Department	Team1	Team2	Team3
DS7 Train users	1.8	1.3	1.1	1.4
DS5 Systems security	2.4	0.9	2.5	2.5
PO3 Technology direction	2.2	3.3	2.1	1.4
DS12 Physical environment	2.5	0	1.6	3.6
DS4 Continuous Service	2.4	3.2	2.6	1.9

DS13 Operations	2.5	1.8	3.3	2.3
AI3 Acquire Infrastructure	2.2	2.8	2.6	2.2
ME1 Monitor	2.6	1	3.2	2.7
DS2 Third party	2.6	3.3	2.4	2.6
DS3 Performance & capacity	3.1	4.2	3	2.6

Table 6: maturity evaluation results

Identify and close gaps in COBIT

Workshop

The aim of the workshop was to implement the COBIT best practices based on current IT processes of ICS BNL BU and collect feedbacks from the infrastructure team of the effectiveness and applicability of COBIT methodology and best practices.

The attendants of the workshop were the three team leaders and the manager of infrastructure department, who are responsible for all the daily operations and management of ICS infrastructure. During the workshop, the participants discussed the gaps between COBIT best practices and their current processes. Concrete action plans of improvements were drawn at the end of the workshop. The workshop was scheduled for three hours focusing on four main parts:

Start-up and Introduction to COBIT framework

The aims and agenda of the workshop were explained at the beginning of the workshop. Then the participants were given a brief introduction of COBIT framework, including its development backgrounds, key components, main structure, core methodology, potential benefits, relations to other control frameworks, etc. Questions were asked and discussed in between.

Discussion of Survey Results

Participants were shown the results of the process maturity evaluation survey; based on the radar chart (figure 8), they compared and discussed the maturity level of the ten processes in view of individual team and the infrastructure department as a whole. Some problems and weaknesses were identified during the discussion. For example, they were surprised to find that the User Education was rated as the lowest of all the tem processes. Because they had done a lot of training programs in the past a few years and hadn't anticipate the low feedback from their team members.

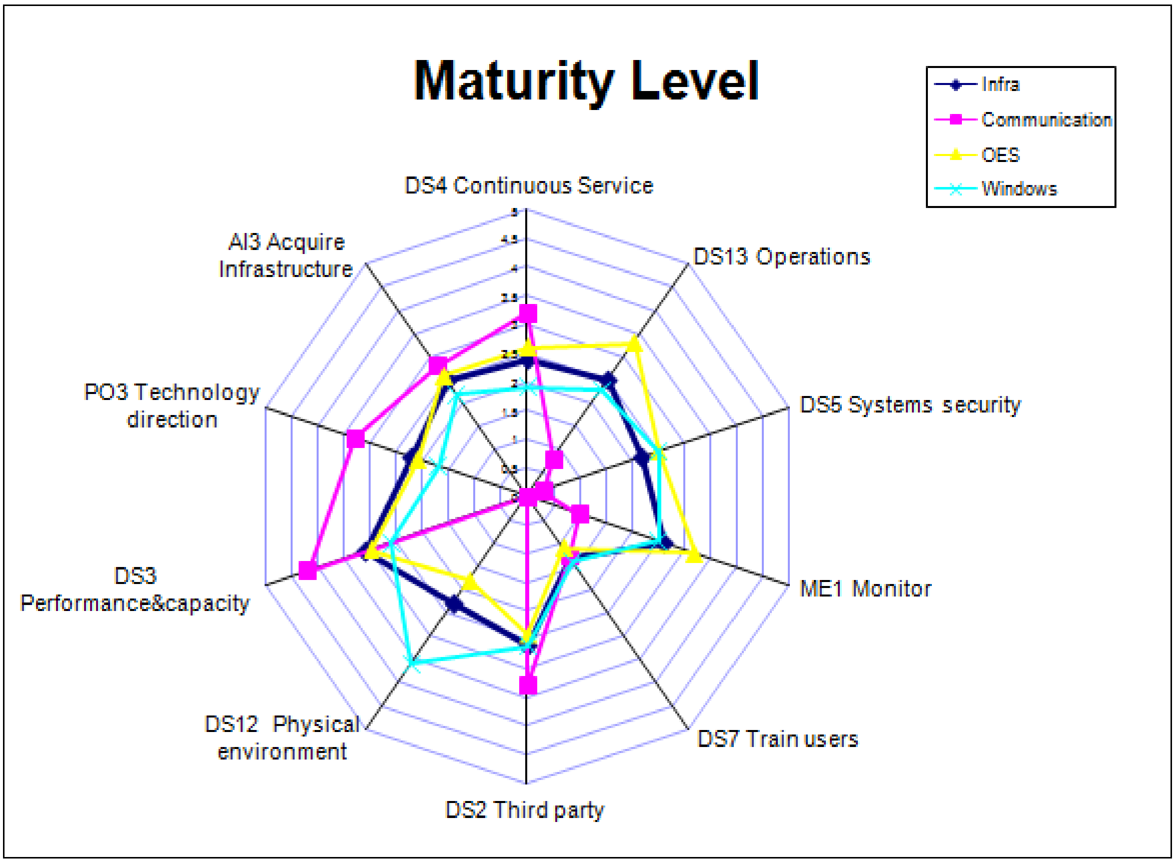


Figure 8: process maturity

Gap Analysis based on COBIT best practices

After careful study of COBIT Control Practices, for each of the ten processes, a number of best practices were selected as benchmarks for gap analysis. They were outlined in flip charts and presented to the participants. By going through each of the best practices, participants were encouraged to spell their opinion of applicability of these best practices from COBIT, such as:

- Is it practical to implement the best practices in infrastructure team?

- What processes or programs have already cover part of the solutions?
- What other actions they can take to solve the problems?

The discussion was very interactive; each of the team leaders and the manager spoke out their opinions and commented on others'. Possibilities and difficulties were identified.

Making Action Plans based on current processes and projects

All participants made agreements on the actions would be taken for closing the identified gaps. Relating to their current roles and on-going projects, responsibility and accountability were assigned. This action plan is also included in their year plan of 2013. Table 7 is an illustration of the draft of action plan during the workshop. The plans are corresponding to the improvements of the 10 processes. Responsible people and require actions are identified in the Owner and Comments columns. A more complete action plan was drafted after the workshop and was included in the new year-plan for each team.

	Control Objectives	Owner	Comments
1	**Training**		
	Create TEMPLATE for skills pool	all	• create a list of skills required for work (refer to job profile); • fill in people's skills (maybe with level like elementary, good, proficient); • update their new skills / skill level each year or after training
	Personal Development Plan		ask people's skills, include training into personal development plan each year
	EVALUATION training results / FORM		evaluate the effectiveness of trainings (taking tests, inquiries)
2	**Security**		
	Communication get involved	Person A	add to his slides for communication security (physical network and mobile)
	Security Awareness training	Person B	combine with internal security training from Manager D and Manager E (in the middle of the year)
	Security Policy ICS Express		learn policies from Person G; security issues in information/asset/third parties/ password/ mobile/ network…
	Internal Penetration Test	Person D	test internal security risks, check people's awareness and action;(maybe checked by people from outside)
3	**Contingency Plan**		

	regular test		have small/large tests; keep records of the problems and lessons learned
	yearly risk assessment	all	find out single point of failures
…	…	…	…

Table 7: draft of action plan

Chapter 6 - Research Results

The following part summarizes the main conclusions from the COBIT reviews in combination with the case study. The results are organized in four parts, namely,

- The Actual Usage of COBIT Tools
- The Current Situation of IT Frameworks
- The Practical Value of COBIT
- The Practical Problems of COBIT

They also present the answers to the four research questions:

- RQ1: What are the fundamental methodologies and common tools in COBIT framework? How are they used?
- RQ2: What IT standards or frameworks are being used for IT governance? How they are used?
- RQ3: What is the practical value of COBIT in established IT environment?
- RQ4: What are the practical problems for adopting and implementing COBIT?

Actual Usage COBIT Tools

The fundamental tools introduced in COBIT are Performance Goals, Metrics, Control Practices, RACI Charts, and Maturity Model. Though they all have very valuable use, the managers in the case company are more interested in the Maturity Model and high-level control objectives.

Usage of Performance Goals and Metrics

Theoretically, the Goals Cascade concept provides a good way aligning IT and business goals. Nevertheless, there are practical problems using them. First of all, the concepts and their relationships are very confusing at first sight. Performance Goals and Metrics are defined at three levels in COBIT 4.1: IT goals and metrics, Process goals and metrics, Activity goals and metrics. It requires great time and efforts understanding them. Besides, there are no implications of how the metrics match with the goals. For example, there are 3 IT goals for DS8 Manage Service Desk and Incidents, which are measured by 2 metrics and driven by 5 metrics; 3 process goals are measured by 5 metrics and driven by 5 metrics; and the 4 activities are measured by 5 metrics. How can management establish a performance measurement system using unmatched goals and metrics?

Secondly, the various measurements and metrics do not make much sense for real IT management. As it is pointed out by Buzina (Buzina, 2011) that COBIT has very complicated structure and too many unpractical measurements for practical use. Many ambiguous terms are used and they are not worthy of reporting in some way.

For example, one measurement for DS5 Ensure System Security is defined as “Frequency and review of the type of security events to be monitored”. Then we cannot help to ask: What does the “security events” mean? Which “security events” should be monitored and which should not? “Frequency AND review”? Are they actually two different measures? However, COBIT does not provide explanations of this metrics and there is no guidance of how to collect these data.

Worst still, there are simply too many of goals and metrics. How can management looking at more than 300 KPIs everyday to monitor IT performance? How can they design an automated tool showing all these indicators?

Usage of RACI Charts

The RACI Charts are valuable in defining the roles and responsibilities of different stakeholders for IT processes. However, it is still at very high level and generic for practical use. In COBIT 4.1, the roles in RACI chart are CEO, CFO, CIO, Business Executives, Head Operations, Chief Architects and so on. The problem is how can we make sure that all these people, especially those are out of IT function, take all their various IT responsibilities? Besides, the IT organizational structure varies a lot from one organization to another. They cannot directly map into the RACI Charts in COBIT. Also, when the COBIT is only partially implemented, as the situation in this case study, many of the stakeholders are out of scope. So for the COBIT implementations of this case study, the RACI was largely ignored.

Usage of Maturity Model

The Maturity Model is a key tool for COBIT implementation as shown in various case studies provided by ITIG and also the case study in this research. The main reason is that it is easy to understand and can be quantified with maturity scores. For example, The IT managers and internal auditors were very interested in knowing which maturity levels they were for different processes. The results in the radar chart showed clearly where their strengths and weaknesses were. They also planned to re-evaluate these processes next year in a similar manner.

It is also agreed that maturity modelling is very effective in identifying gaps of current IT capabilities. In this case study, after identifying critical IT processes and assessing the maturity levels, action plans were quickly developed during the workshop by learning related detailed control objectives and discussing specific circumstances of their IT processes.

However, it should be noticed that companies must customize an efficient method to measure their maturity levels. The descriptions of Maturity Model in COBIT 4.1 is still complicated, which includes six attributes (Awareness and communication, Policies, plans and procedures, Tools and automation, Skills and expertise, Responsibility and accountability, Goal setting and measurement) and three dimensions (capability, coverage and control). The questionnaire provided in the Implementation Guide 1is not very efficient either.

Many case studies from ITGI show that they have to device more efficient and effective ways to obtain the maturity scores with respect to various issues of specific context, such as the strategy of the company, the relationship between IT and business, the maturity of IT governance, etc. As it is shown in this case study, when the first questionnaire, which was designed in line with the COBIT implementation guide, the manager found it was too complicated to understand. It would take a long time explaining related concepts to participants before it could be actually filled in. After revising it to a simple version, most participates were willing to fill in and little extra explanation was needed.

Usage of Control Objectives

In COBIT 4.1, there are 222 control objectives for all 34 IT process. The control objectives provide generic good practice for IT management and auditor to evaluate their IT processes. However, as they are less-structured and many of them are overlapped with other IT frameworks, like ITIL and ISO27000, it creates great confusions of how to use them. In the case study, the control objectives were used to evaluate their maturity level on the focused processes. Besides, the detailed control practices were used to draft action plans. However, most of the study and selection of control objectives were by us, because it was too much

[1] COBIT 3rd Edition *Implementation Tool Set* includes some questionnaires to help users collect required information.

work for IT managers. Sufficient knowledge in current IT processes and COBIT methodologies are needed. Therefore a great deal of time and effort should be put into before we can use the control objectives.

Current Situation of IT Frameworks

ITIG and ISACA admit that COBIT is more suitable to be used at the highest level of IT governance, providing an overall control framework. There is still a great need for specific IT practices and standards to define more detailed, standardised processes for practitioners. The most popular and widely adopted international standards are ISO/IEC 17799:2005 or ISO 27001, ITIL, PRINCE2, etc. which address different aspects of information technology issues.

However, it is probably not always the case described by ITIG that organizations use COBIT as a reference first and seek for guidance for certain processes in more detailed frameworks. On the contrary, the more common situation is that detailed IT standards and practices such as ITIL and ISO27000 are well in place before the adoption of COBIT.

According to the “IT Governance Global Status Report–2011”, carried out by ITGI, ITIL was the most frequently used IT standards, followed ISO27000 as the second. Also, the trends in the use of these standards are steadily increasing from 2006 to 2010. In contrast, the usage of COBIT increased from 9% in 2006 to 14% in 2008; but decreased to 12.9% in 2010(figure 9).

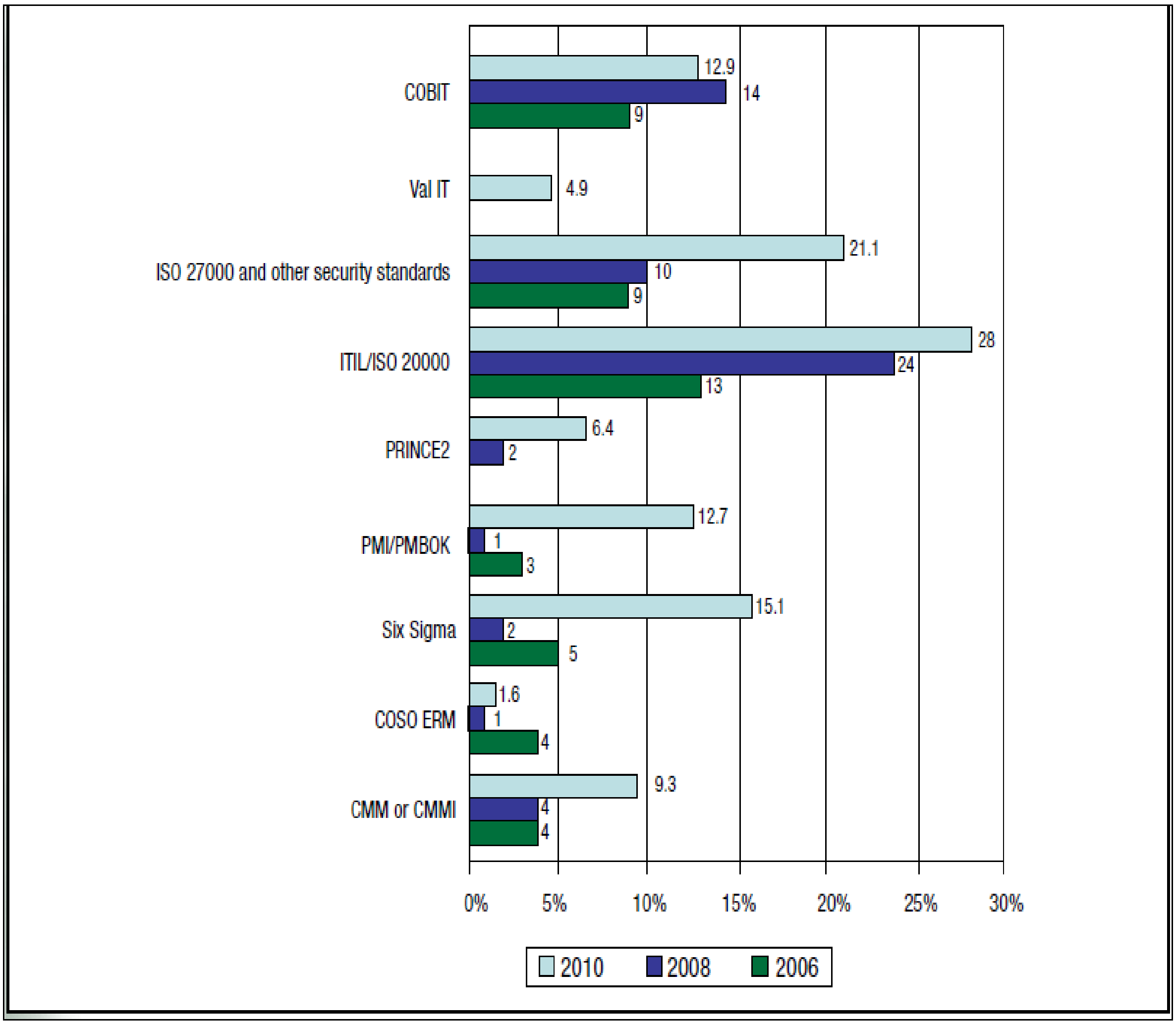


Figure 9: Trends in Usage of IT Framework
Source: ITGI, Global Status Report on the Governance of Enterprise IT (GEIT)—2011

The main reason for this trend is that detailed frameworks are more matured and have more direct impacts. For example, organizations can assure their customers and partners by obtaining the ISO27000 certification as it is an internationally accepted code of practice for information security. Similarly, ITIL, which focuses on IT service delivery and support, can help organizations develop and standardize their IT processes quickly.

Practical Value of COBIT

According to literature reviews, the leading factors that compel organizations to adopt IT standards and frameworks are stringent regulatory and compliance requirements, increased IT costs and investments, the growing strategic role of information and technologies. The motivation of adopting COBIT in this case study reveals more practical value of COBIT framework.

Problems of Multi-audit Programmes

There is a tendency in the market that customers are requiring all kinds of certifications from companies to assure the quality and safety of products and services. In order to be a competitive player in logistic market, LogisticX has the goal of all business units worldwide to be certified according to a series of standards such as ISO 9001(Quality), ISO 14001(Environment), OHSAS 18001(Health & Safety), IiP (Investor in People, People Management), TAPA (Transported Asset Protection Association, Security), etc.

Compliance with Enterprise Internal Control

In order to obtain and preserve various required certificates, a number of internal and external audit programmes are implemented within all units of BNL BU. The goal is to conduct preventive assessments and improve overall operations. The internal and external audits are executed by qualified auditors at different intervals based on the scope and aim of the auditing programme. These audits are carried out on the basis of checklists from certain frameworks. Auditors collect required information through interviews, document review and observations. Upon completion of an audit, the findings and recommendations are presented to managers of the unit reported. This manager shall react on the 'Corrective and Preventive Action " of the audit report and is responsible for further implementation and evaluation.

Compliance with IT-specific Certifications and Standards

Aside from the general enterprise certifications such as ISO9001, OHSAS18001, Iip, ICS department is also subjected to IT-specified certifications and standards, such as ISO27001 for Information Security, PRINCE2 for Project Management, ITIL for IT Services, etc. At present, ICS has established an Information Security Management System (ISMS) based on ISO27001framework. Internal and external audits are carried out to obtain the desirable assurance of IT management. It influences mainly three parties: IT departmental managers, ICS Information Security Officer and auditors.

First of all, in conjunction with enterprise governance and control unit, the Information Security Officer creates policies and standards according to internal and external assurance requirements. The Information Security Officer is also responsible for communicating and involving IT departmental managers and their first-line employees to implement these policies in their daily operations. To test the effectiveness of the implementation, auditors will conduct related audit programmes, checking the actual performance. The tests are based on two levels: the existence of certain controls and the effectiveness of these controls.

Redundant Compliances for IT Managers

IT managers shall facilitate the audit program by providing required documents, such as performance reports, operating logs, contracts, etc, and also arrange responsible people for demonstration and interviews. Audit programs can be initiated with different purposes: some are to obtain certain certifications like ISO27001, some are for preserving existing standards like ISO9001, and others may be due to overall internal or external financial audit like SOX. The current problem is that ICS has to cooperate with so many audit programmes that they are repeatedly audited by different parties maybe for the same process. For example, the Change Management process was audited several times for the purposes of SOX and ISO27001audits.

This is obviously ineffective, especially for IT managers and ICS internal service assurance managers, who have to prepare and assist all audit related processes. They have to prepare many documents, such as performance reports, operating logs, contracts, etc.; arrange responsible people for demonstration and interviews; attend all kinds of meetings for explaining, reporting, reviewing these programs. It is quite time-consuming and distracts IT people from their normal work. Even though the actual audit content is more or less the same, it may come in different forms and require different efforts for providing related resources. Therefore, ICS calls for an integrated audit process to avoid redundant work.

Value of COBIT

Providing Consistent IT Audit Process

Unlike the adoption of ITIL, ISO27000 that aims at meeting external regulatory compliance and contractual requirements, the primary driving factor for implementing COBIT comes inside the case company. The Internal Control Manager and the Information Security Officer are considering using COBIT as an internal audit "basket", which will incorporate various audit and certification requirements of IT into one single repository. It aims to provide a consistent framework for IT risk controls. IT managers do not have to prepare for repeated audit programs. This also proves the strength of COBIT mentioned in literatures that it is a good framework for assisting internal control processes and integrating different IT standards.

Proactive Process Improvement

In the view of IT managers, it is very passive to comply with all kinds of internal and external audit requirements. It is common that auditors come with a long checklist with many controls given by certain standards or frameworks. They ask various questions and test the effectiveness of implementation of the standards. They search for tangible evidences of compliances and render non-compliance warnings to IT managers for corrective and preventive actions. IT managers can only passively react to auditors' checks and sometime feel getting short of controls of what they should do for their responsibilities. They are not aware of their control weaknesses until they are checked by auditors.

In that case, it is reasonable for managers to take the initiative of learning and implementing best practices in the first place, working proactively to meet the control objectives. COBIT can help managers identify gaps and improve their IT operations. It is a reference book for managers to check in which areas they should pay attention to, at which level of control they should have, what documents or records they should keep track of, and so on.

As it happened in the case study, the IT manager found that they had very practical culture where many work was accomplished without going through standard procedures. More efficient manners are preferred. People were not good at keeping records of what they had done. For example, they did review the physical access in data centre, but they didn't regularly record this process. After studying the best practices in the COBIT workshop, they realized that it was necessary to require a regular review report from the data centre provider.

Practical Problems of COBIT

Complicated Concepts and Structure

It is acknowledged by previous researchers and also the managers in the case study that it is not easy to understand COBIT framework. The single document COBIT4.1 includes Framework[1], Control Objectives[2], Management Guidelines[3], Maturity Model[4], which requires a great deal of time learning all its concepts and tools. For example, only for the Control Objectives, there are 34 IT processes with 222 control objectives and more than 300 KPIs and KGIs. It provides even more control practices for each of the control objectives in COBIT Control Practices[5]. Obviously, it is overwhelming for most people. Even for people who have studied COBIT for a while or have related experience, it is difficult to capture the essence of COBIT quickly.

Besides, a family of COBIT 4.1 products have been created by ITGI and ISACA, including IT Assurance Guide[6], and IT Governance Implementation Guide[7], etc. It is by no means easy to understand all its methodologies; great efforts are needed to obtain a complete view of their focuses.

However, we should notice that the targeted audiences of COBIT are management, senior IT professionals and auditors, who, in most cases, are the busiest people in an organization. Therefore, COBIT can be easily ignored by these high-profile people if they couldn't understand it and realize its benefits quickly, no matter how beneficial this framework is. In

[1] Framework—Explain how COBIT organises IT governance, management and control objectives and good practices by IT domains and processes, and links them to business requirements.

[2] Control objectives—Provide generic good practice management objectives for IT processes.

[3] Management guidelines—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability.

[4] Maturity models—Provide profiles of IT processes describing possible current and future states.

[5] Control Practices –Provide detailed guidance on all the steps that are necessary and sufficient for achieving the control objective.

[6]IT Assurance Guide –Provides guidance on how COBIT can be used to support a variety of assurance activities together with suggested testing steps for all the IT processes and control objectives.

[7]IT Governance Implementation Guide- Provides a generic road map for implementing IT governance using the COBIT and Val IT resources.

that case, COBIT would become some kind of good theory on-the-shelf but have little practical usage. In the case study, both the Internal Control Manager and Information Security Officer, who have abundant experience in IT control frameworks, express that though they believe COBIT is a very useful framework, they don't know how to take the most of it.

Lack of Implementation Guidance and Proven Benefits

The generic nature COBIT creates great difficulty for organizations to understand and use it. Though in COBIT Management Guidelines and Implementation Guidelines it mentions that COBIT needs to be customised to specific environment, it does not provide concrete methods or guidelines facilitating organizations to accomplish this. Only a few case studies are available from its publisher ITGI and ISACA, but they do not provide many details.

In contrast to ISO27000 and ITIL, the value of COBIT is hard to perceive. Though it claims to have many advantages in aligning IT with business and mitigating IT risks, there are no proven statistics or studies confirming these statements. As it is revealed in ITGI's report (ITGI, 2006), many executives agreed that even though it was obvious that a COBIT program should be initiated, they preferred to focus on ITIL and ISO27000, which had more significant values.

So, one great weakness of COBIT is its implicit value. It is hard to determine what benefit COBIT will bring in comparison to more matured IT standards like ITIL, and ISO27001. Despite of many advantages claimed in ITGI and ISACA's publications, there are no industrial or academic statistics or studies substantiate these statements. So management are still dubious about the true value of COBIT. Therefore, organizations tend to go for detailed IT standards first to harvest the low-hanging fruit. COBIT, if it is being considered at all, is more likely to come at later stage.

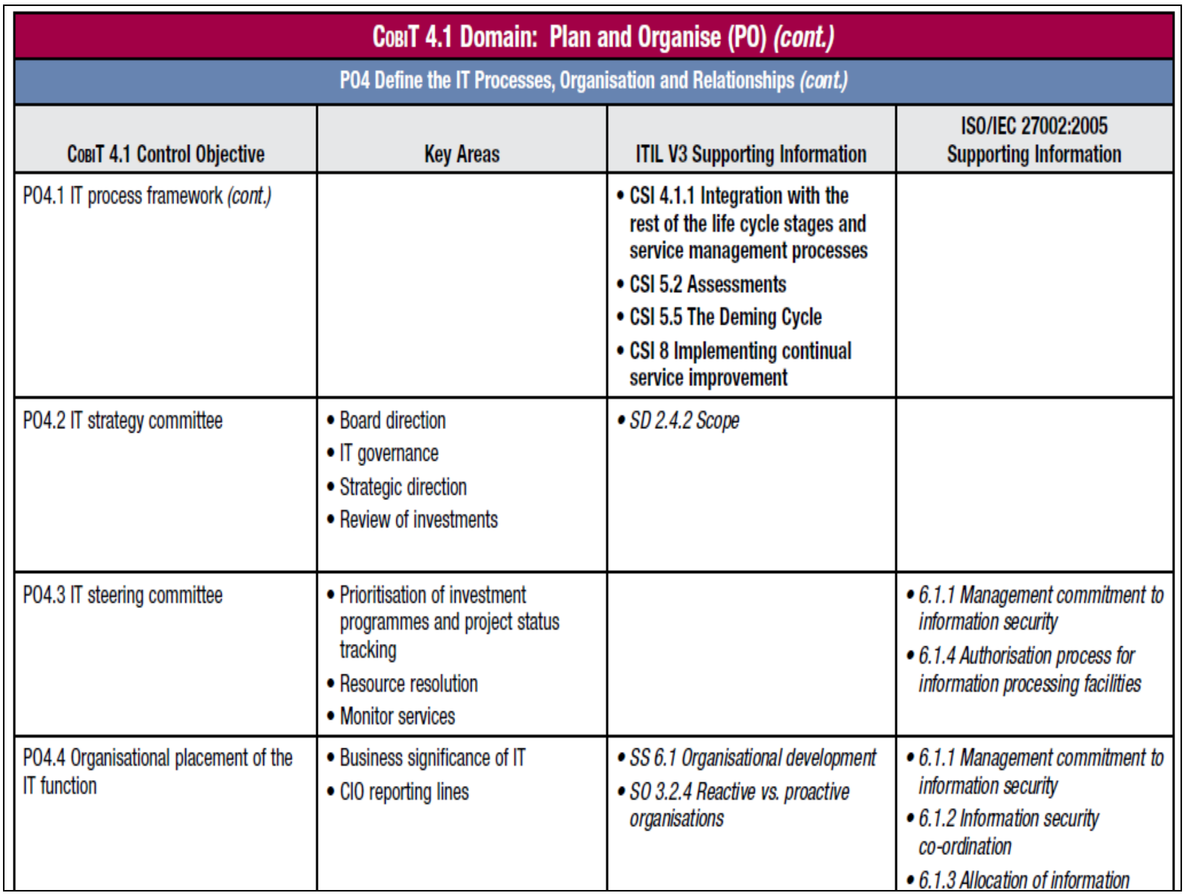
Confusion with other IT Standards

The proliferation of other IT standards creates great challenges for organizations to understand their relations. It will add more confusion to management by introducing COBIT, especially when standards like ITIL and ISO27001 are well in place. During the interviews with the Internal Control Manager and Information Security Officer, they express that though they believe COBIT is a very useful framework, they don’t know how to take the most of it. It seems that many COBIT processes have already been addressed by their ISO27001 certification program and ITIL standard. They have improved a lot of their information security management and IT service support and delivery through these programmes. Some COBIT processes are nice to have but are out of ICS’ control, as they are more influenced by business stakeholders. Still there may be some controls in COBIT that ICS lacks of, but they don’t know how to find them.

Then the problem comes to how organizations could take the most of COBIT as well as other IT standards to improve overall IT management. Which detailed control objective of COBIT can map to the counterpart in ISO27000 or ITIL and vice versa? Which are the distinctive control objectives of COBIT that organizations should pay attention to?

ITIG also realizes this problem and is spurred to initiate several projects mapping the most commonly used standards into COBIT processes and control objectives. Some studies have been accomplished and a few publications are available now. The Overview of International IT Guidance (2nd Edition) gives a brief overview of a list of popular frameworks and explanations of how to align or map them into COBIT. But it doesn’t contain detailed mappings. The Aligning CobiT4.1, ITIL V3 and ISO/IEC27002 for Business Benefit is a following publication that completes a detailed mapping of COBIT and ISO/IEC 17799:2000.

These works do help organizations to understand the relations between these frameworks. But the mappings are still at a high level. Besides, as each framework defines its own scope, definitions, terminologies, structures and approaches, sometime the literally mapping can be misleading. The following picture shows how ITIG maps the three frameworks.



CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*

PO4 Define the IT Processes, Organisation and Relationships *(cont.)*

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO4.1 IT process framework *(cont.)*		• **CSI 4.1.1 Integration with the rest of the life cycle stages and service management processes** • **CSI 5.2 Assessments** • **CSI 5.5 The Deming Cycle** • **CSI 8 Implementing continual service improvement**	
PO4.2 IT strategy committee	• Board direction • IT governance • Strategic direction • Review of investments	• *SD 2.4.2 Scope*	
PO4.3 IT steering committee	• Prioritisation of investment programmes and project status tracking • Resource resolution • Monitor services		• *6.1.1 Management commitment to information security* • *6.1.4 Authorisation process for information processing facilities*
PO4.4 Organisational placement of the IT function	• Business significance of IT • CIO reporting lines	• *SS 6.1 Organisational development* • *SO 3.2.4 Reactive vs. proactive organisations*	• *6.1.1 Management commitment to information security* • *6.1.2 Information security co-ordination* • *6.1.3 Allocation of information*

Figure 10: Mapping *CobiT4.1, ITIL V3 and ISO/IEC27002*
Source: ITGI, www.itgi.org

Chapter 7 - New COBIT-BSC Model

Call for Simple Structure

As stated in previous chapter, the complex nature of COBIT makes it difficult for organizations to adopt COBIT. One obvious problem that causes the complexity is that the control objectives are presented in a less-structured manner. Though there are grouped into four main domains, many of them are overlapped in content or bear some structural relations. The identified problems are categorized in three groups:

Generic vs. Concrete

Some of the control objectives are very generic, such as PO8-Manage Quality, PO9-Assess Risks, PO5-Manage the IT Investment. They cannot be implemented independently but embedded in many concrete control objectives, like DS5-Ensure systems security, DS12-Manage the Physical Environment, AI5-Procure IT resources, etc.

Whole vs. Part

Some of the control objectives are addressing the same problems simply from different point of views. For example, PO4-Define the IT Organization and Relationships and ME4-Establishment of an IT Governance Framework are obviously dealing with the same problem of establishing IT functions and governance. Similarly, PO2-Define the information architecture, PO3-Determine the technology direction and PO6-Communicate management aims and directions are part of and should be included in PO1-Define a strategic IT plan.

Logic-linkages:

Many processes are logically linked to others that cannot separates as independent processes. For example, AI1-Identify Automated Solutions is the pre-requisite of AI2-

Acquire Application Software. Thus AI1 will not happen alone and should be part of the whole A2 process.

Therefore, it is necessary to structure the COBIT control objectives in a more logical and sensible way in order to understand it quickly and take advantage of it.

Implications from the Case Study

The idea of grouping is also triggered by the interviews and survey results within the case company. First of all, in the aim of complying with international standards, the company already have the ISO27001 initiative for quite a long time. When it comes to control objectives such as DS5-Ensure systems security, DS12-Manage the Physical Environment, which are addressed at full length by ISO27001, IT managers think that there is no need to go through them again, as they have already established adequate controls over these processes. Similarly, as reviewing control objectives such as AI6-Manage changes, DS9-Manage the configuration, DS8-Manage Service Desk and Incidents, DS10-Manage problems, etc. managers also express that these processes have been standardized by ITIL practices. Policies, procedures, tool and reports are well in place.

Secondly, according to the survey results, those control objectives ranked low in maturity level are not covered by any existing IT frameworks. For example, DS7-Educate and Train Users was rated the lowest of the detailed evaluation within Infrastructure department. This process is neither addressed by ITIL nor by ISO27001. It is only mentioned by ISO27001 for security awareness education. On the other hand, those control objectives have high maturity level are well executed either by ITIL or ISO27001, such as DS8-Manage Service Desk and Incidents, DS10-Manage problems, DS12-Manage the Physical Environment, and so on.

Last but not the least, in term of the wide adoptions of ISO27001 and ITIL, it should be quite common that organizations come to know and implement these matured IT frameworks long before becoming interested in COBIT. In that case, this selection can be broadly applied, because the implementations of ISO27001 and ITIL do not vary a lot from one organization to another due to the maturity and standardized structure of these frameworks. Minor variation may be needed in consideration of the actual executions in a specific IT environment.

Grouping COBIT Control Objectives

The starting point is to screen out control objectives that are well addressed by detailed frameworks, such as ISO27001, ITIL. This selection is based on previous studies on framework mappings and practical analysis.

Based on both literature study and case study, we find that the motivation for ISO27001 certification mainly comes from the outside requirements of customers and stakeholders. As ISO27001 is a de facto international standard, it becomes a must for organizations to compete in the market. Most Large companies feel obligated to comply with ISO series standards in the aim of assuring customers and stakeholders of their good conducts. In addition, this kind of compliance is closely related to the work of internal control function, whose main responsibility is to provide desirable assurance of potential risks. The ISO27000 series has designated sections addressing asset management, risk assessment, business continuity and compliance issues. The control objectives falling into this group are:

PO8-Manage quality
PO9-Assess risks
DS4-Ensure continuous service
ME2-Monitor and evaluate internal control

ME3-Ensure compliance with external requirements
DS11- Manage data
DS5-Ensure systems security
DS12-Manage the physical environment
DS2-Manage third party services

The control objectives that are covered by ITIL are easy to be identified as most of them share same terms. These control objectives are:

DS1-Define and manage service levels
AI7-Install and accredit solutions and changes
AI4-Enable operation and use
AI2-Maintain application software
AI3-Maintain technology infrastructure
AI6-Manage changes
DS9-Manage the configuration
DS1-Manage service desk and incidents
DS10-Manage problems
DS13-Manage operations
DS3-Manage performance and capacity
PO10-Manage projects
ME1 Monitor and evaluate IT performance

In contrast to ISO27000, the implementation of ITIL is an internal call for efficient IT service delivery and support. Because ITIL provides a set of comprehensive practices, including detailed approaches, functions, roles and processes, organizations can quickly standardize their IT services based on the ITIL standards. Besides, ITIL is more mature and has been implemented by many organizations.

After excluding above control objectives, the remaining ones fall into three categories:

High-level IT strategies, such as:

PO4-Define the IT organization and relationships
ME4-Establishment of an IT governance framework
PO1-Define a strategic IT plan
PO2-Define the information architecture

PO3-Determine the technology direction

PO6-Communicate management aims and directions

IT Financial issues, such as:

PO5-Manage the IT Investment

AI5-Procure IT resources

DS6-Identify and allocate costs

Learning and Training, such as:

PO7-Manage human resources

DS7-Educate and train users

For the first category, the strategic-level control objectives are more influenced by the IT role and business strategy of an organization. The responsibilities of strategic planning mainly fall into the Management Board, not very relevant to the frontier IT workers. For the second category, these financial related processes are well controlled by corporate financial department. In most cases, standardized procedures are well in place; request and reporting templates are readily available; status and issues are regularly reviewed. This is quite reasonable because companies all have rigorous policies and procedures with respect to financial issues. For the third category, processes related to learning and growth, are closely linked to the work and responsibilities of corporate HR; IT department only plays a supporting role.

Fitting into Balanced Scorecard

It is interesting to notice that these five categories fit well into the views in Balanced Scorecard (BSC) as shown in figure 11. BSC is first developed by Kaplan and Norton (Kaplan & Norton, 1996) as a business performance management system. It evaluates business performance not only from the traditional financial perspective, but also take into consideration of customer satisfaction, internal processes and the ability to innovate, which are critical factors that will assure future financial results. It is suggested that a balanced view of these four perspectives drive businesses toward their strategic goals.

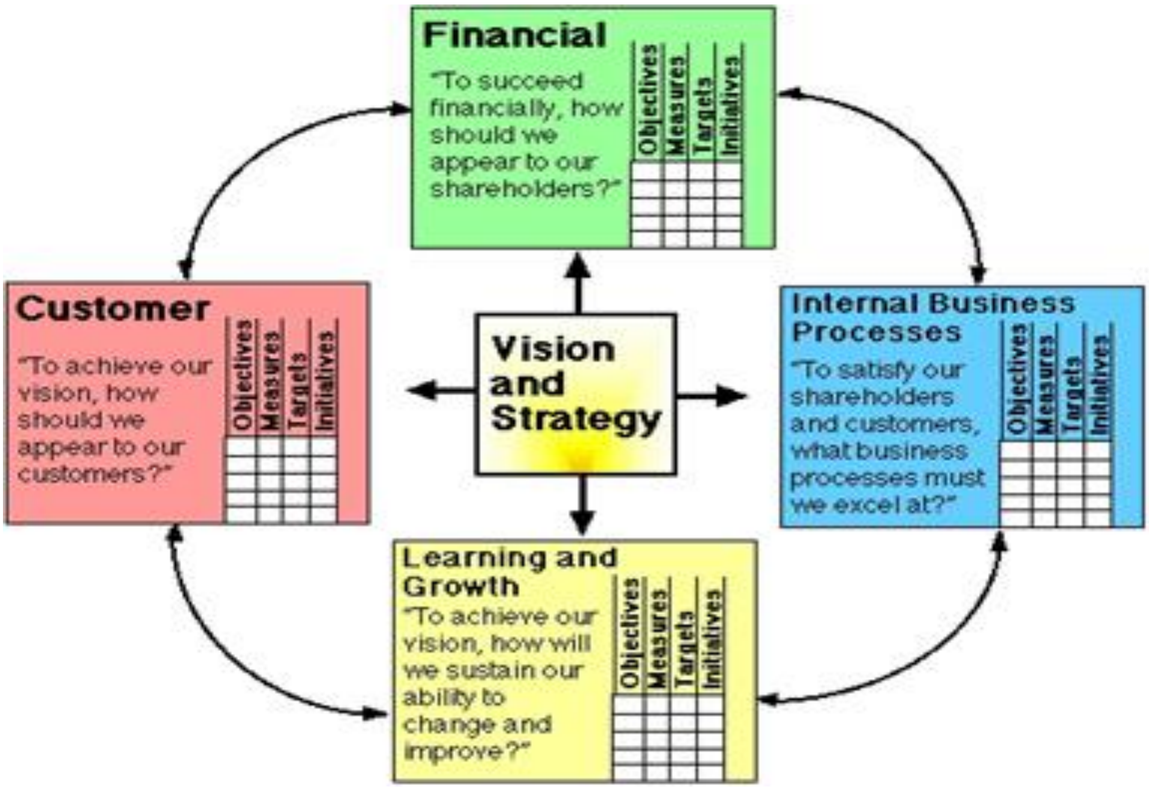

Financial
"To succeed financially, how should we appear to our shareholders?"
Objectives
Measures
Targets
Initiatives
Customer
"To achieve our vision, how should we appear to our customers?"
Objectives
Measures
Targets
Initiatives
Vision and Strategy
Internal Business Processes
"To satisfy our shareholders and customers, what business processes must we excel at?"
Objectives
Measures
Targets
Initiatives
Learning and Growth
"To achieve our vision, how will we sustain our ability to change and improve?"
Objectives
Measures
Targets
Initiatives

Figure 11: BSC

Therefore, we group the 34 control objectives into five groups, namely IT Vision & Strategy, IT Financial Perspective, Internal IT Process, IT Stakeholder Perspective and IT Learning & Growth. Generally, control objectives addressing high-level IT strategies belong to IT Vision & Strategy view; ITIL covered control objectives are within the Internal IT Process view; Most ISO27001 and risk-control related processes fall into the IT Stakeholder Perspective; IT financial and investment related control objectives are in the IT Financial Perspective; The remaining control objective concerning IT human resources and training fall into the IT Learning & Growth view. Figure 14 illustrates this model.

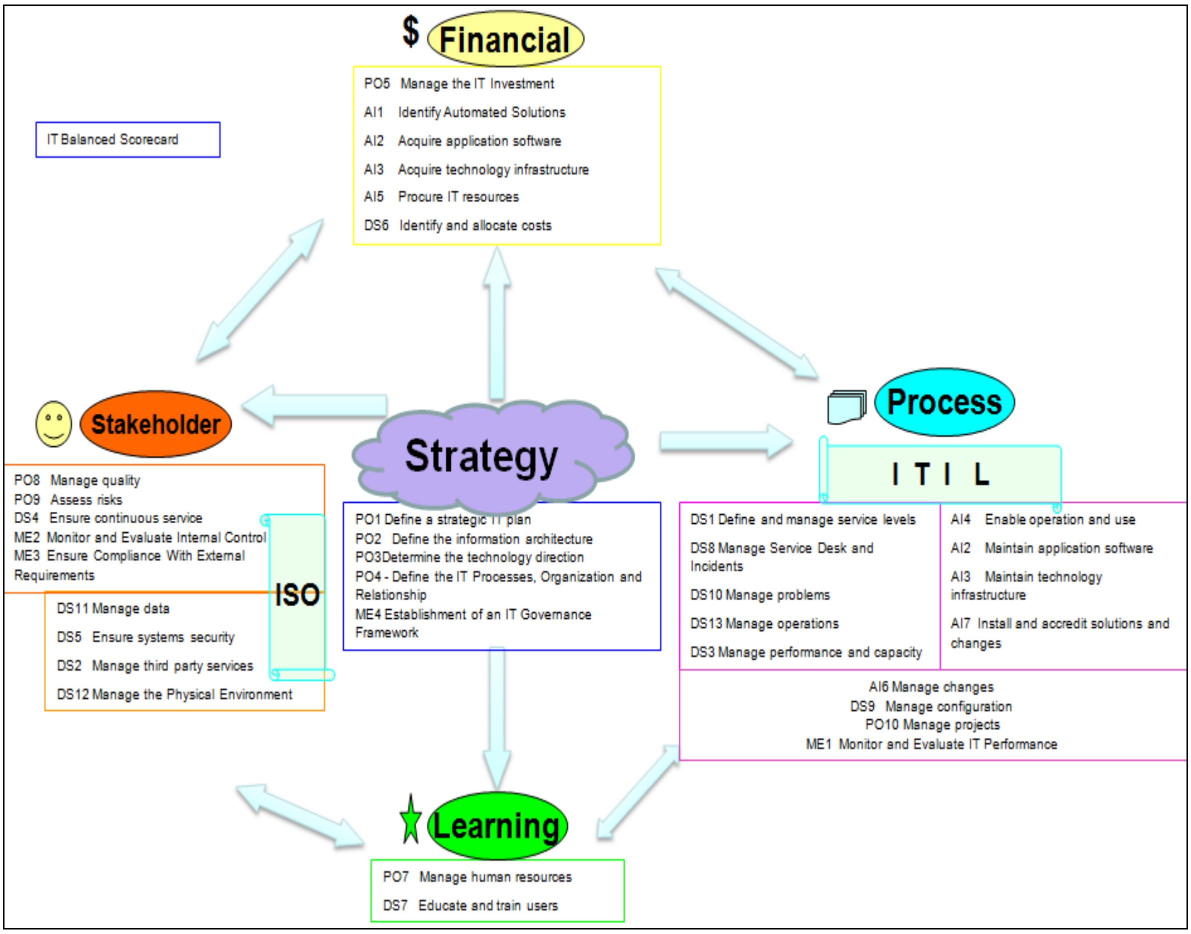

$ Financial
PO5 Manage the IT Investment
AI1 Identify Automated Solutions
AI2 Acquire application software
AI3 Acquire technology infrastructure
AI5 Procure IT resources
DS6 Identify and allocate costs
IT Balanced Scorecard
Stakeholder
PO8 Manage quality
PO9 Assess risks
DS4 Ensure continuous service
ME2 Monitor and Evaluate Internal Control
ME3 Ensure Compliance With External Requirements
ISO
DS11 Manage data
DS5 Ensure systems security
DS2 Manage third party services
DS12 Manage the Physical Environment
Strategy
PO1 Define a strategic IT plan
PO2 Define the information architecture
PO3Determine the technology direction
PO4 - Define the IT Processes, Organization and Relationship
ME4 Establishment of an IT Governance Framework
Process
I T I L
DS1 Define and manage service levels
DS8 Manage Service Desk and Incidents
DS10 Manage problems
DS13 Manage operations
DS3 Manage performance and capacity
AI4 Enable operation and use
AI2 Maintain application software
AI3 Maintain technology infrastructure
AI7 Install and accredit solutions and changes
AI6 Manage changes
DS9 Manage configuration
PO10 Manage projects
ME1 Monitor and Evaluate IT Performance
Learning
PO7 Manage human resources
DS7 Educate and train users

Figure 12: COBIT-BSC Model

Detailed Analysis

Aside from the five groups, the categorization of each control objective is also based on the common structural problems identified in previous chapter. The in-depth analysis of why one control objective fall into one of the five views is illustrated in the following table 8.

PROCESS	KEY POINTS	COMMENTS	COBIT-BSC Type
1. PLANNING & ORGANISATION			
PO1 Define a strategic IT plan	• defines IT goals and priorities based on business objectives •align all IT resources with business strategy and priorities •analyse and manage project and service portfolios	Generic controls that is embedded many other control objectives	Strategy
PO2 Define the information architecture	• develop a corporate information architecture and data model • maintain a data dictionary to promote a common use of data throughout all IT applications	Part of the a strategic IT plan(PO1)	Strategy

PO3 Determine the technology direction	• creates a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer, such as systems architecture, technological direction, acquisition plans, standards, migration	Part of the a strategic IT plan(PO1)	Strategy
PO4 Define the IT organisation and relationships	• Processes, administrative policies and procedures are in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, segregation of duties and supervision	For established IT functions, this process has already been accomplished. Improvement can be made based on ITIL&ISO27001	Strategy
PO5 Manage the IT Investment	• manage IT investment programmes, ensure effective use of IT resources • provides transparency and accountability into the total cost of ownership (TCO)	Generic controls that embedded in many other control objectives	Financial
PO6 Communicate management aims and directions	• articulate IT mission, service objectives, policies and procedures to stakeholders • ensures awareness and understanding of business and IT risks, objectives and direction and compliance with relevant laws and regulations	Can be included in the IT strategic plans or internal communication process.	Strategy
PO7 Manage human resources	• follow defined practices supporting recruiting, training, evaluating performance, promoting and terminating IT workforce	Main responsibility fall into corporate HR; synergy can be achieved by cooperation.	Learning &Growing
PO8 Manage quality	• provides clear quality requirements, procedures and policies • quality management system is developed and maintained by proven development and acquisition processes and standards	Generic controls that embedded in many other control objectives covered by ITIL	Stakeholder
PO9 Assess risks	• develop a risk management framework documenting a common and agreed-upon level of IT risks, mitigation strategies and residual risks	Generic controls that embedded in many other control objectives, covered by ISO27001	Stakeholder
PO10 Manage projects	• establishes an IT project management framework which includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, QA, a formal test plan, and testing and post-implementation review after	Specially addressed by PRINCE2	Internal IT Process

2. ACQUISITION & IMPLEMENTATION			
AI1 Identify Automated Solutions	• analysis of new application or function before acquisition or creation	First step of AI2	Financial
AI2 Acquire and maintain application software	• Align application development with business requirements and standards	Acquisition related to IT financial management Maintenance related to internal process	Financial Internal IT Process
AI3 Acquire and maintain technology infrastructure	• develop processes for the acquisition, implementation and upgrade of the technology infrastructure • ensures that there is ongoing technological support for business applications	Acquisition related to IT financial management Maintenance related to internal process	Financial Internal IT Process
AI4 Enable operation and use	• provide documentation and manuals for users and IT • provide training to ensure the proper use and operation of applications and infrastructure	Post-implementation, covered by ITIL	Internal IT Process
AI5 Procure IT resources	• Procure IT resources, including people, hardware, software and services • develop procedures for procurement, selection of vendors, setup of contractual arrangements, the acquisition itself	Related to IT financial management	Financial
AI6 Manage changes	• formally manage and control all changes, including emergency maintenance, patches for infrastructure and applications within the production	covered by ITIL	Internal IT Process
AI7 Install and accredit solutions and changes	• tests new systems in a dedicated environment with relevant test data • define rollout and migration instructions • release planning, actual promotion to production, and post-implementation review	covered by ITIL	Internal IT Process
3. SERVICE DELIVERY MANAGEMENT			
DS1 Define and manage service levels	• provide documented definition IT services of and agreement on service levels • monitor and timely report to stakeholders on the accomplishment of service level	covered by ITIL	Internal IT Process
DS2 Manage third party services	• clearly define the roles, responsibilities and expectations in third-party agreements • review and monitor such agreements for effectiveness and compliance	covered by ITIL & ISO27001	Stakeholder
DS3 Manage performance	• periodically review current performance and capacity of IT resources	covered by ITIL	Internal IT Process

and capacity	• forecast future needs based on workload, storage and contingency requirements		
DS4 Ensure continuous service	• develop, maintain and test IT continuity plans • utilize offsite backup storage and provide periodic continuity plan training	covered by ITIL & ISO27001	Stakeholder
DS5 Ensure systems security	• establish and maintain IT security roles and responsibilities, policies, standards, and procedures • perform security monitor and periodic test and implement corrective actions	covered by ISO27001	Stakeholder
DS6 Identify and allocate costs	• build and operate a fair IT costs allocating system to capture, allocate and report IT costs to the users of services	Related to IT financial management	Financial
DS7 Educate and train users	• identify training needs of internal and external users • define and execute effective training and measure the results	Closely related to HR's responsibility	Learning &Growing
DS8 Manage Service Desk and Incidents	• develop a well-designed and well-executed service desk and incident management process including incident registration, escalation, trend and root cause analysis, and resolution	covered by ITIL	Internal IT Process
DS9 Manage the configuration	• establish and maintain an accurate and complete configuration repository • collect initial configuration information, establish baselines, verify and audit configuration information, and update the configuration repository as needed	covered by ITIL	Internal IT Process
DS10 Manage problems	• identify, classify and resolve problems based on root cause analysis • formulate recommendations for improvement, maintain problem records and review the status of corrective actions	covered by ITIL	Internal IT Process
DS11 Manage data	• identify data requirements, establish effective procedures to manage the media library, backup and recovery of data, and proper disposal of media	Related to service continuity, covered by ISO27001	Stakeholder
DS12 Manage the Physical Environment	• define physical site requirements, select appropriate facilities, design effective processes for monitoring environmental factors and managing physical access	covered by ISO27001	Stakeholder
DS13 Manage operations	• define operating policies and procedures for effective management of scheduled processing • protect sensitive output, monitor infrastructure performance and ensure preventive maintenance of hardware	covered by ITIL	Internal IT Process
4. MONITORING & CONTROL			
ME1	• define relevant performance indicators,	covered by ITIL	Internal IT

Monitor and Evaluate IT Performance	systematically and timely report performance, and promptly act upon deviations		Process
ME2 Monitor and Evaluate Internal Control	• monitor and report control exceptions, results of self-assessments and third-party reviews to ensure effective and efficient operations	covered by ISO27001 for information security	Internal IT Process
ME3 Ensure Compliance With External Requirements	• comply with laws, regulations and contractual requirements by identifying compliance requirements, optimising and evaluating responses, obtaining assurance and integrating IT's compliance reporting with business	covered by ISO27001	Stakeholder
ME4 Establishment of an IT Governance Framework	• define organisational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives	Partially covered by ITIL	Strategy

Table 8: Detailed Analysis

It should also be mentioned that the grouping some control objectives that fall into ITIL or ISO27001 categories are not detailed mappings of COBIT to these frameworks. The publications (ITGI, 2008) from ITGI present more detailed mappings. The categorization of this study does refer to these studies; however, more practical considerations are taken into account.

Summary List

A summary of each view is showed below:

IT Vision & Strategy

PO4 Define the IT organisation and relationships
ME4 Establishment of an IT Governance Framework
PO1 Define a strategic IT plan
PO2 Define the information architecture
PO3 Determine the technology direction
PO6 Communicate management aims and directions

IT Stakeholder Perspective

PO8 Manage quality

PO9 Assess risks

DS4 Ensure continuous service

ME3 Ensure Compliance with External Requirements

DS11 Manage data

DS5 Ensure systems security

DS12 Manage the Physical Environment

DS2 Manage third party services

IT Financial Perspective

PO5 Manage the IT Investment

AI1 Identify Automated Solutions

AI2 Acquire application software

AI3 Acquire technology infrastructure

AI5 Procure IT resources

DS6 Identify and allocate costs

IT Internal Process

DS1 Define and manage service levels

AI7 Install and accredit solutions and changes

AI4 Enable operation and use

AI2 Maintain application software

AI3 Maintain technology infrastructure

AI6 Manage changes

DS9 Manage the configuration

DS8 Manage Service Desk and Incidents

DS10 Manage problems

DS13 Manage operations

DS3 Manage performance and capacity

PO10 Manage projects

ME1 Monitor and Evaluate IT Performance

ME2 Monitor and Evaluate Internal Control

IT Learning & Growth

PO7 Manage human resources

DS7 Educate and train users

Chapter 8 - Clarification on COBIT-BSC Model

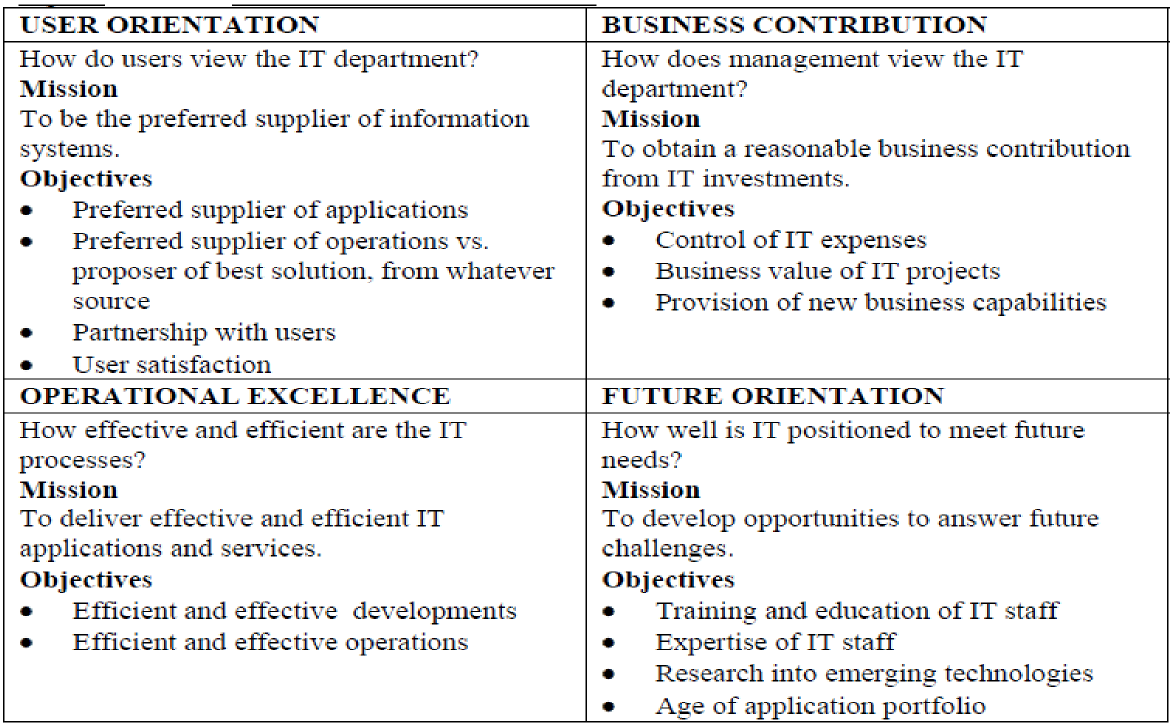
There are many studies using Balanced Scorecard (BSC) in combination with COBIT for better IT governance. The Goal Cascade method in COBIT framework is based on BSC too. It should be pointed out that these studies focus on the alignment of business and IT goals. They exemplify how BSC can be effectively used to define IT process goals and metrics that are closely linked to business strategies. Although this study also uses the BSC concept, its focus is to provide a simple view of the inner relations of COBIT control objectives and its relation to popular frameworks. It merely uses the four views of BSC in categorizing control objectives. No further concepts of BSC are involved.

Previous Studies on COBIT and BSC

According to the study of Cram (Cram, 2007), most of the early research of IT BSC aligned closely with Kaplan and Norton's BSC techniques, concentrating on the theory and concepts, due to the lack of practical experience. As implementation experience increased, IT BSC was refined based on contemporary ideas of aligning IT with business measurement and strategy. More practical results of the design, operation and management of an IT-specific scorecard were available. More recently, the content of IT BSC has expanded beyond the previously academic-dominated environment. Increasing number of publications has emerged, which covers a broad range of IT management issues, such as IT governance, service level management, enterprise resource planning, knowledge management and IT audit (Cram, 2007).

IT BSC

The balanced scorecard can also be applied to the IT function and IT processes (Van Bruggen & Van Grembergen, 1997). A standard IT balanced scorecard (figure 12) evaluates IT performance is based on the four BSC perspectives: the User perspective represents the user evaluation of IT. The internal process perspective represents the IT processes employed to develop and deliver IT services. The learning and growth perspective represents the development of human and technology resources needed by IT. The financial perspective captures the business value of the IT investments.



USER ORIENTATION	**BUSINESS CONTRIBUTION**
How do users view the IT department? **Mission** To be the preferred supplier of information systems. **Objectives** • Preferred supplier of applications • Preferred supplier of operations vs. proposer of best solution, from whatever source • Partnership with users • User satisfaction	How does management view the IT department? **Mission** To obtain a reasonable business contribution from IT investments. **Objectives** • Control of IT expenses • Business value of IT projects • Provision of new business capabilities
OPERATIONAL EXCELLENCE	**FUTURE ORIENTATION**
How effective and efficient are the IT processes? **Mission** To deliver effective and efficient IT applications and services. **Objectives** • Efficient and effective developments • Efficient and effective operations	How well is IT positioned to meet future needs? **Mission** To develop opportunities to answer future challenges. **Objectives** • Training and education of IT staff • Expertise of IT staff • Research into emerging technologies • Age of application portfolio

Figure 13: IT BSC

Van Grembergen developed the application of IT BSC with a series of studies, such as the development of generic IT BSC (Van Bruggen & Van Grembergen, 1997), the real-life IT BSC application in an information services division at a Canadian financial group, using IT BSC as instruments for service level agreements (Van Grembergen, De Haes, & Amelinckx, 2003). Drawing on previous work on balanced scorecards measuring the IT function and the board performance, a generic IT governance balanced scorecard (figure 13) is proposed by Grembergen and Haes (Grembergen & Haes, 2005). This model also forms the basis of the Goal Cascade concept in COBIT.

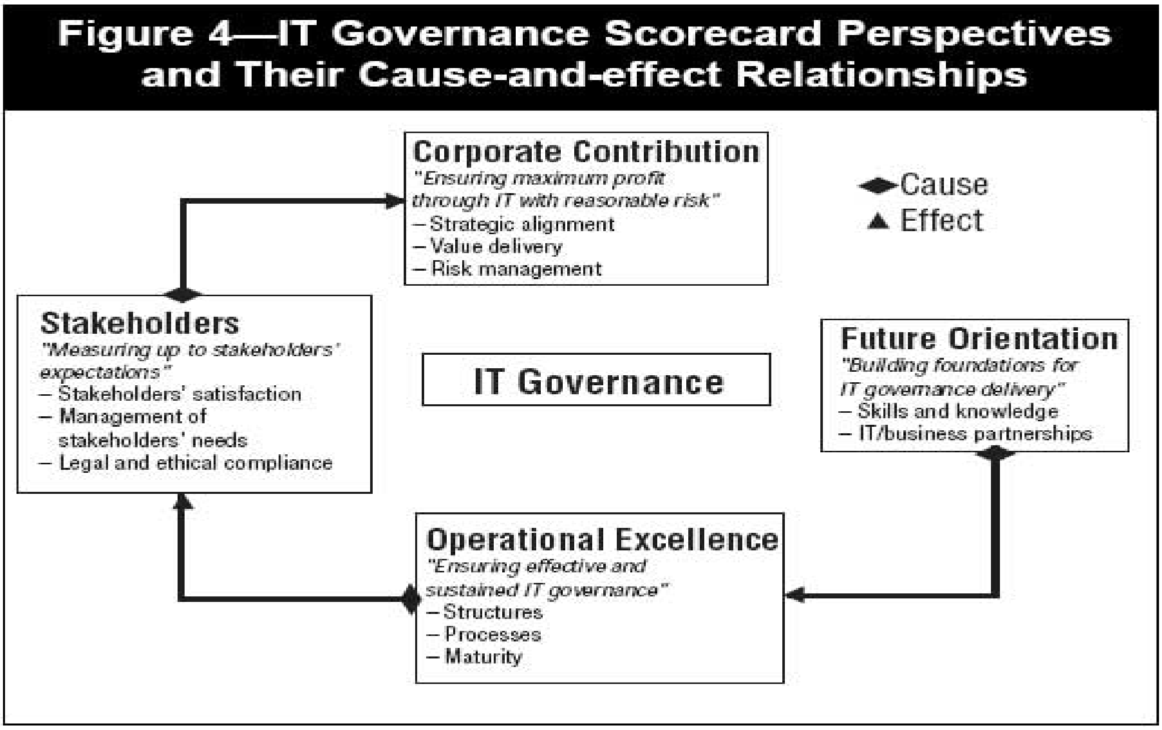


Figure 4—IT Governance Scorecard Perspectives and Their Cause-and-effect Relationships
Corporate Contribution
"Ensuring maximum profit through IT with reasonable risk"
– Strategic alignment
– Value delivery
– Risk management
Cause
Effect
Stakeholders
"Measuring up to stakeholders' expectations"
– Stakeholders' satisfaction
– Management of stakeholders' needs
– Legal and ethical compliance
IT Governance
Future Orientation
"Building foundations for IT governance delivery"
– Skills and knowledge
– IT/business partnerships
Operational Excellence
"Ensuring effective and sustained IT governance"
– Structures
– Processes
– Maturity

Figure 14: IT Governance BSC

Sallé and Rosenthal (Sallé & Rosenthal, 2004) present how the COBIT framework contributes to the formulation and implementation of the strategy of Hewlett-Packard (HP) Information Technology program (ITP). Built on the goals and enablers specified in COBIT and a mapping to HP IT Service Management (ITSM) processes, they reformulated HP's ITP strategy using a BSC. Another study of from Ahuja compares the strengths, weaknesses of COBIT, BSC and the Systems Security Engineering Capability Maturity Model (SSECMM) (Ahuja, 2009), and formulates a comprehensive framework for strategic information security management. Ahuja concludes that the integration of COBIT and BSC could bridge the gaps, mitigate the weaknesses of each framework and provide a more comprehensive mechanism for strategic information security management.

BSC & Goal Cascade in COBIT

In fact, business-orientation is one of the main features of COBIT. Rather than just measuring what are critical from IT perspective, COBIT tries to define measurements of IT performance that make sense to business. From IT strategic level to tactic and operational level, the selection of Performance Goals and Metrics are based on BSC method. Performance Goals and Metrics are defined at three levels in COBIT:

- IT goals and metrics: define what the business expects from IT and how to measure it;
- Process goals and metrics: define what the IT process must deliver to support IT's objectives and how to measure it;
- Activity goals and metrics: establish what needs to happen inside the process to achieve the required performance and how to measure it

All the goals are directly or indirectly measured by different metrics, including Outcome Measures and Performance Measures. The Outcome Measures, previously known as KGIs, indicates whether the goals have been met; and the Performance Measures, known as KPIs, indicates whether goals are likely to be met. The outcome measures of the lower level become performance indicators for the higher level. This is called as Goals Cascade, which derives from the concept of IT governance scorecard introduced by Grembergen and Haes (Van Grembergen & De Haes, 2005). Figure 4 is an illustration from COBIT 4.1 explaining the relationship between these concepts. It shows the goal cascade of DS5.

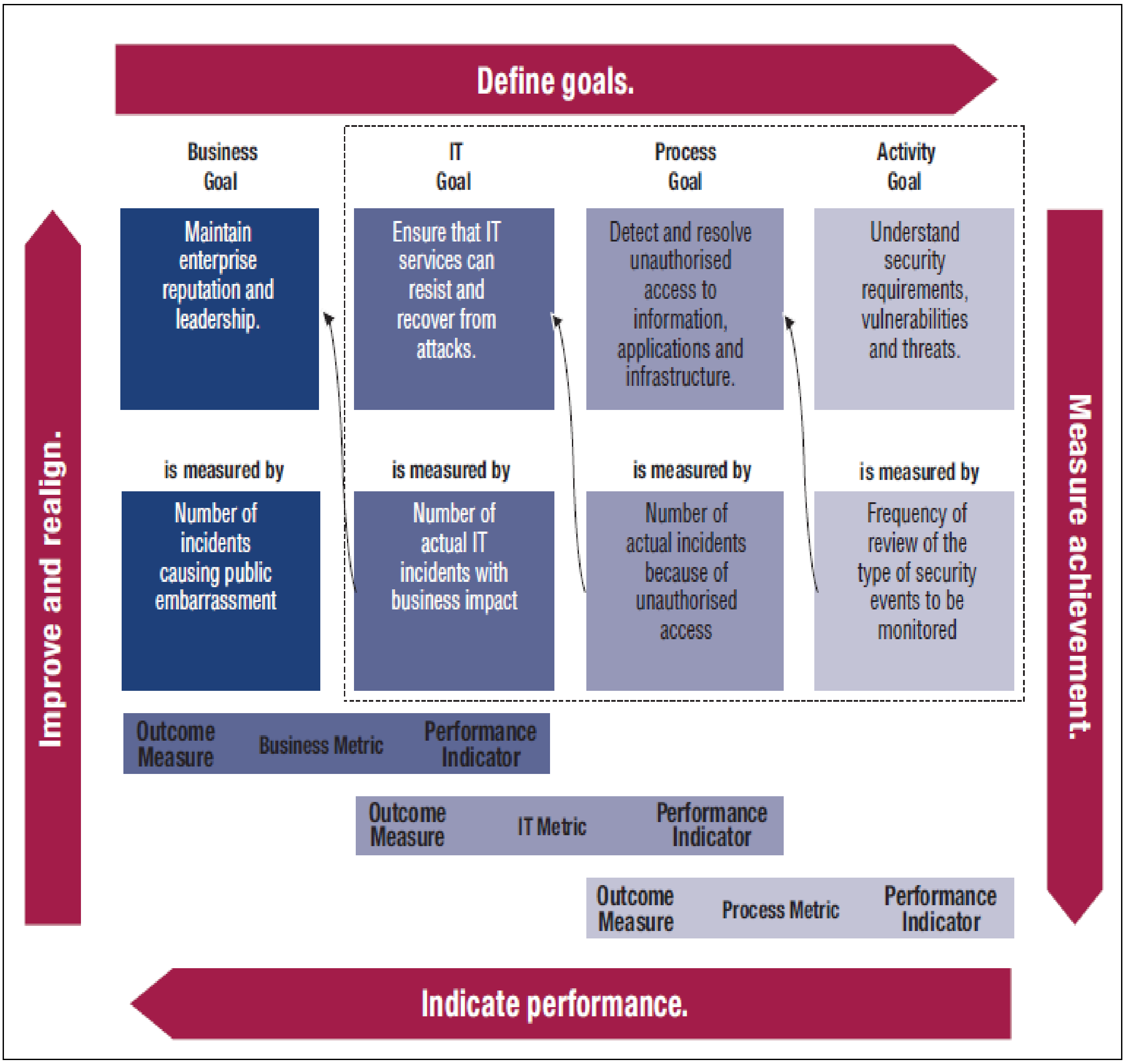

Define goals.
Business Goal
IT Goal
Process Goal
Activity Goal
Maintain enterprise reputation and leadership.
Ensure that IT services can resist and recover from attacks.
Detect and resolve unauthorised access to information, applications and infrastructure.
Understand security requirements, vulnerabilities and threats.
is measured by
is measured by
is measured by
is measured by
Number of incidents causing public embarrassment
Number of actual IT incidents with business impact
Number of actual incidents because of unauthorised access
Frequency of review of the type of security events to be monitored
Outcome Measure
Business Metric
Performance Indicator
Outcome Measure
IT Metric
Performance Indicator
Outcome Measure
Process Metric
Performance Indicator
Improve and realign.
Measure achievement.
Indicate performance.

Figure 15: Relationship between Process, Goals, and Metrics (DS5)
Source: ITGI, www.itgi.org

In the latest version COBIT 5, it includes an updated version of the BSC methodology for structuring and communicating performance measurement. It places IT BSC more prominently at the front of the new framework in goals cascade, which aims to enable IT organizations establishing a culture of performance management and accountability. In COBIT 5, generic scorecards have been created for the enterprise and IT as a whole. It suggests that business- and industry-specific key performance indicators (KPIs) should be added; and cascades of scorecards should be built for numerous IT personnel and disciplines, including IT service management, project and portfolio management, quality management, security management, etc. (ISACA, 2012).

BSC Focus of this Study

As elaborated above, previous studies mentioning BSC and COBIT focus on the alignment of business and IT goals. They exemplify how BSC can be effectively used to define IT goals and metrics that are closely linked to business strategies. The COBIT-BSC model in this study differentiates from previous studies in that it aims to provide a simple view of the structure of COBIT control objectives and its relations to popular frameworks, such as ITIL and ISO27000. The model categorizes 34 control objectives in COBIT 4.1 into five general groups, which are inspired by the four perspectives presented in BSC. However, the model merely uses the four views of BSC; there is no further discussion on other BSC related concepts, such as defining goals, measures, etc. Therefore, it is only a structural analysis of COBIT control objectives.

The COBIT-BSC model is a combination of theory and practice. It is created during the final phase of the case study, as more practical insights are collected from experienced IT professionals and auditors. The model aims to provide a simple way of viewing COBIT control objectives and helps organizations capture its essence quickly. To some extent, it shortens the lengthy study of complicated concepts in COBIT. It shows clearly how COBIT relates to ISO27001 and ITIL, making it easier for management to understand the distinctive value COBIT. The benefits of using this model are summarized in the following aspects:

- Provides an easier way of understanding the relations and internal links between each control objectives in COBIT;
- Provides a start point for organizations to implement COBIT framework based on existing IT processes and policies;

- Simplify the process of evaluating and prioritizing each control objectives during COBIT implementation;
- Gives an overview of the relations between other IT frameworks with COBIT and helps to capture the essences of each of these frameworks;
- Helps organizations quickly identify strengths and weaknesses of their IT processes and governance frameworks

Chapter 9 - Summary & Discussions

Value of this Study

This study reviews the current studies on COBIT and other IT governance frameworks. It summarizes the theoretical values and weaknesses identified by previous researchers. Based on the case study, the actual usage of the tools and methods in COBIT are revealed that although there are many tools introduced in COBIT, such as Performance Goals, Metrics, Control Practices, RACI Charts, etc., organizations are more interested in the Maturity Model, which is easy to understand and be quantified. The COBIT has more practical values in providing consistent IT audit process and assisting proactive IT process improvement. These practical insights will add more knowledge to COBIT studies.

In line with literature reviews, some practical problems of COBIT are identified, such as complicated concepts and structure, lack of implementation guidance and proven benefits, confusion with other IT standards. We also analyze and classified the structural problems of COBIT control objectives in details. In addition, a COBIT-BSC model is proposed to illustrate a simple way of structuring COBIT control objectives. This method is different from the usage of BSC in previous studies which focus on IT-business alignment.

This study summarizes many findings from previous studies on COBIT and contributes much practical knowledge through the case study. It will help organizations to understand the practical problems and values of COBIT, so that they can take advantage of it as well as other IT control frameworks for better IT governance.

Limitations and Recommendations

The following are some limitations of this research and recommendations of future work:

First of all, due to the scale of this study, the amount of data collected is very limited and is not rigorously validated under different contexts. Conclusions are drawn based on analysis available resources and the reality of the company. It is necessary to collect more inputs and criticisms from more IT practitioners and COBIT experts. Besides, it also bears the innate drawbacks of case study research methodology that the data collected cannot necessarily be generalised to the wider population. The implementation of IT governance frameworks might vary a lot regarding a series of factors, such as the size, industry, strategy, IT maturity level of an organization. Thus, further studies are in great need to test the validity of this study in a broader range of contexts.

Secondly, the main purpose of this study is to explore the practicability of COBIT framework. Some practical problems of COBIT adoption and implementation are identified by the case study. Because of the scarce recourses and inadequate academic studies on COBIT5, this research is limited to COBIT 4.1. Since a large part of COBIT 5 refers back to COBIT 4.1 and most organizations are using it, this research is still valuable. However, further analysis is needed to examine whether COBIT 5 provides new solutions for the practical problems identified in this study.

Thirdly, the proposed COBIT-BSC model only illustrates a simple view COBIT control objective based on BSC perspectives. It aims to help management quickly understand COBIT and its relation to ISO27001 and ITIL. It is not a scrupulous result and does not mean to be complete as the full goal cascade table or detailed mappings. Still, the validity of categorizing each control objectives needs further discussions.

References

Ahuja, S. (2009). Integration of COBIT, Balanced Scorecard and SSE-CMM as a strategic Information Security Management (ISM) framework. *Proceedings of the Fourth International Workshop on Business/IT Alignment & Interoperability.*

Anthes, G. (2004). *Quality Model Mania*. Retrieved 2013, from ComputerWorld: http://www.computerworld.com/s/article/90797/Model_Mania

Bowen, P., Rohde, F., & Cheung, M.-Y. D. (2007). Enhancing IT governance practices: A model and case study of an organization's efforts. *International Journal of Accounting Information Systems* .

Buzina, M. (2011). *Is COBIT practical enough for real world usage?* Retrieved 2012, from http://buzina.wordpress.com/2011/08/30/is-cobit-practical-enough-for-real-world-usage/

Colbert, J., & Bowen, P. (1996). A Comparison of Internal Controls:COBIT, SAC, COSO and SAS 55/78. *IS Audit and Control Journal* .

Council, C. (2007). Implications for the Future of COBIT Systems in Higher Education. *Information Systems Control Journal* .

Cram, A. (2007). The IT Balanced Scorecard Revisited. *Information Systems Control Journal* .

HARDY, G. (2006). *Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges.* Information Security Technical Report.

ISACA. (2012). *COBIT Document.* Retrieved 2013, from http://www.isaca.org: http://www.isaca.org/COBIT/Documents/Compare-with-4.1.pdf

ITGI. (2008). *Aligning CobiT4.1, ITIL V3 and ISO/IEC27002 for Business Benefit.* IT Governance Institute, www.itgi.org.

ITGI. (2007). *COBIT 4.1.* IT Governance Institute, www.itgi.org.

ITGI. (2006). *Global Status Report on the Governance of Enterprise IT (GEIT)—2006.* IT Governance Institute, www.itgi.org.

ITGI. (2011). *Global Status Report on the Governance of Enterprise IT (GEIT)—2011.* IT Governance Institute, www.itgi.org.

Kaplan, B., & Duchon, D. (1998). Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. *MIS Quarterly* , pp. 571 -587.

McDonough, S., & McDonough, J. (1997). *Research Methods as part of English Language Teacher Education?* Hodder Arnold.

Nicho, M. (2008). Information Technology Audit: Systems.

Oliver, D. (2003). A Selective Approach to COBIT:A Top-down Approach. *Information Systems Control Journal* .

Ridley, G., Young, J., & Carroll, P. (2004). *COBIT and its Utilization: A framework from the literature.* Proceedings of the 37th Hawaii International Conference on System Sciences.

Robinson, N. (2005). IT Excellence Starts with Governance. *Journal of Investment Compliance* , 45-49.

Rouyet-Ruiz, J.-I. (2008). 0 COBIT as a Tool for IT Governance: between Auditing and IT Governance. *UPGRADE* .

Sallé, M., & Rosenthal, S. (2004). *Formulating and Implementing an HP IT program strategy using CobiT and HP ITSM.* Retrieved 2013, from HP Technical Reports: http://www.hpl.hp.com/techreports/2004/HPL-2004-179.html

Simonsson, M., Johnson, P., & Wijkström, H. (2007). Model Based IT Governance Maturity Assessments With COBIT. *the 15th European Conference on Information Systems.* Switzerland.

Spremic, M. (2012). Measuring IT Governance Performance: a. *International Journal of Mathematics and Computer in Simulation* .

Symons, C. (2006). *COBIT Versus Other Frameworks: A Road Map To.* Forrester Research.

Van Bruggen, R., & Van Grembergen, W. (1997). Measuring and improving corporate information technology. *Proceedings of the Fourth European Conference on the,* (pp. 163-171). Delft.

Van Grembergen, W., & De Haes, S. (2005). Measuring and Improving IT Governance Through the Balanced Scorecard. *Information Systems Control Journal* .

Van Grembergen, W., De Haes, S., & Amelinckx, I. (2003). Using COBIT and the Balanced Scorecard as Instruments for Service Level Management. *Information Systems Control Journal* .

Van Grembergen, W., Saull, R., & De Haes, S. (2003). Linking the IT Balanced Scorecard to. *Journal of Information Technology Case and Application Research* .

Van Maanen, J. (1979). *Qualitative methodology.* Sage.

von Solms, B. (2005). Information Security governance: COBIT or. *Computers & Security* , pp. 99-104.

Webb, P., Polland, C., & Ridley, G. (2006). Attempting to Define IT Governance: Wisdom or Folly. *Proceedings of the 39th Annual Hawaii International conference on System Sciences.* IEEE Computer Society.

Williams, P. (2006, September). *A helping hand with IT governance*. Retrieved 2012, from Computer Weekly: http://www.computerweekly.com/opinion/A-helping-hand-with-IT-governance

Yin, R. (1994). *Case Study Research: Design and Methods.* Sage.

Appendix A-Questionnaires

Questionnaire 1
Topic: IT Governance
Participants: IT Managers

1. Is there an IT plan in your department that defines IT goals aligned with related business objectives and priorities?

- o Yes
- o No

2. How well do you think the processes of IT functions are organized in your department?

- o Well defined and organized; we have clear process structure, roles, responsibilities and supervision, and all people are well informed of that;
- o Partially defined and organized; we have only defined critical processes and roles, limited people are informed of their responsibilities and supervision.
- o Not defined and poorly organized; we don't have clear process structure, separation of duties, or supervision.

3. In your opinion, which statement relates most closely to the current IT performance in your department?

- o IT performance significantly underperforms compared to our expectations
- o IT performance somewhat underperforms compared to our expectations
- o IT performs in line with our expectations
- o IT performance somewhat outperforms our expectations
- o IT performance significantly outperforms our expectations

4. Have your department defined measurable objectives for your IT processes?

- o Yes, we have defined measurable objectives for all our IT processes.
- o Yes, but we have only defined measurable objectives for critical IT processes.
- o No, we haven't define any measurable objectives for our IT processes

5. Do your department have any scorecards, reports or documents that assess current process performance?

- ○ Yes, we have performance reports for all our IT processes, and most of them are generated automatically and regularly.
- ○ Yes, but we only have performance reports for important IT processes, and most of them are generated automatically and regularly.
- ○ Yes, but we only have performance reports for important IT processes, and most of them are generated manually only when they are required.
- ○ No, we don't have performance reports for our IT processes.

6. Do you review or verify current process performance against agreed-upon targets?

- ○ Yes, we regularly review our performance to meet targeted objectives.
- ○ Yes, but we only review our performance when increasing problems are identified.
- ○ No, we don't review our performance.

7. How do you think IT governance/ control are performed in your department?

- ○ Controls and measurements are in place for all our processes and they are well executed
- ○ Controls and measurements are only in place for critical processes, and they are partially executed
- ○ We don't have formal controls and measurements for our processes

8. Which statement do you think relates most closely to the general perception of IT control in your department?

- ○ We do not think our IT control is an issue for our department.
- ○ We understand IT control is an issue but are just starting to assess what needs to be done.
- ○ We are well aware that IT control is important and we have a number of ad hoc measures in place.
- ○ We have well-defined IT control measures and processes in place.
- ○ We have well-functioning IT control processes and a performance measuring system in place.

- ○ Our IT control processes are continuously optimised based on performance measuring.

Questionnaire 2
Topic: IT Governance Framework
Participants: IT Managers

1. Do you use or refer to any framework for IT governance/ IT performance control?

- ○ Yes
- ○ No

2. What IT governance framework(s) do you use or you are considering using in the future? (multiple choice)

- ○ COSO(Integrated Framework of internal Control from Committee of Sponsoring Organisations of the Treadway Commission)
- ○ COBIT (Control Objectives for Information and related Technologies)
- ○ ITIL(IT Infrastructure Library)
- ○ ISO/IEC 17799(Code of Practice for Information Security Management)
- ○ FIPS PUB 200(Federal Information Processing Standards)
- ○ PRINCE2(Projects in Controlled Environments)
- ○ CMMI(Capability Maturity Model Integration)
- ○ Others (please specify)

3. What are the motivations and objectives of your department using these frameworks?

- ○ Improve alignment between IT and business
- ○ Comply with internal/ external audit requirements
- ○ Improve IT maturity level
- ○ Benchmark best IT control practices
- ○ Identify internal control weaknesses
- ○ Formalize control processes
- ○ Reduce control costs
- ○ Others (please specify)

4. Do you think it is easy to understand basic methodologies of these frameworks?

- ○ Yes, they are very clear and easy to understand
- ○ Not really, as it requires intensive study to understand basic concepts and structures
- ○ No, it is very difficult to understand basic concepts and structures even after careful study

5. How do you think these IT governance frameworks?

- ○ The frameworks are very beneficial and applicable.
- ○ The frameworks are beneficial but not applicable for all circumstances.
- ○ The frameworks are theoretically beneficial but too generic for practical use.
- ○ The frameworks are not beneficial as they are too generic to adapt to our existing control mechanism.

6. How do you use IT governance frameworks?

- ○ We follow the guidelines and practices strictly as a whole, and use them as benchmarks.
- ○ We only select a few guidelines and practices related to our processes and follow them literally.
- ○ We do not follow the guidelines and practices literally, but only use them as references to get inspirations, then adapt or customize them to our existing control mechanism.
- ○ We create our own control mechanism without referring to any framework.

------If Q1=No, answer 7-8

7. As you mentioned that you don’t use or refer to any IT governance framework, how do you create your own IT governance/control mechanism in your department? (Please specify)

18. How do you define control metrics or measurements based on your IT processes? (Please specify)

Questionnaire 3
Topic: COBIT Framework
Participants: IT Managers, Team Leaders

1. Do you think it is easy to understand basic methodologies in COBIT?

- o Yes, they are very clear and easy to understand
- o Not really, as it requires intensive study to understand basic concepts and structures
- o No, it is very difficult to understand basic concepts and structures even after careful study

2. How do you think COBIT framework in general?

- o The framework is very beneficial for improving our IT controls and very applicable to our current processes.
- o The framework seems beneficial but we don't know how to apply it.
- o The framework is not very beneficial, because it is too generic to adapt to our existing processes.

3. Do you think the control objectives cover all your IT processes?

- o Yes, they cover all our IT processes
- o No, but they cover most part of our IT processes
- o No, they only cover a small part of our IT processes

4. How do you think the degree of relevancy and effectiveness of control objectives?

- o They are highly relevant to our control processes, correctly reflect our main concerns and effectively reveal some critical control issues.
- o They are relevant to some of our control processes, reflect part of our concerns and reveal some control issues, but not very critical ones.
- o They are not very relevant to our control processes, only reflect a small part of our concerns, most of them are irrelevant; and few control issues are revealed.

5. Do you find it is easy to map your current IT processes into the processes in COBIT?

- ○ Yes, it is easy to map our IT processes into COBIT, no or little extra effort is required.
- ○ Not really, only after carefully study and fully understanding of the processes, can we map our IT processes into COBIT.
- ○ No, it is very difficult to map our IT processes into COBIT even after careful study, because they are too generic, great effort are needed to adapt them to our current IT processes

6. Do you think maturity level can properly assess your current process performance, do you think the results are credible?

- ○ It can correctly reflect our current IT performance, and the results are agreed by most assessors, so we think they are credible.
- ○ It can reflect our current IT performance, though the results differ among assessors, we still think they are credible.
- ○ It cannot correctly reflect our current IT performance; the results vary a lot by different assessors, so we don't think they are very credible.

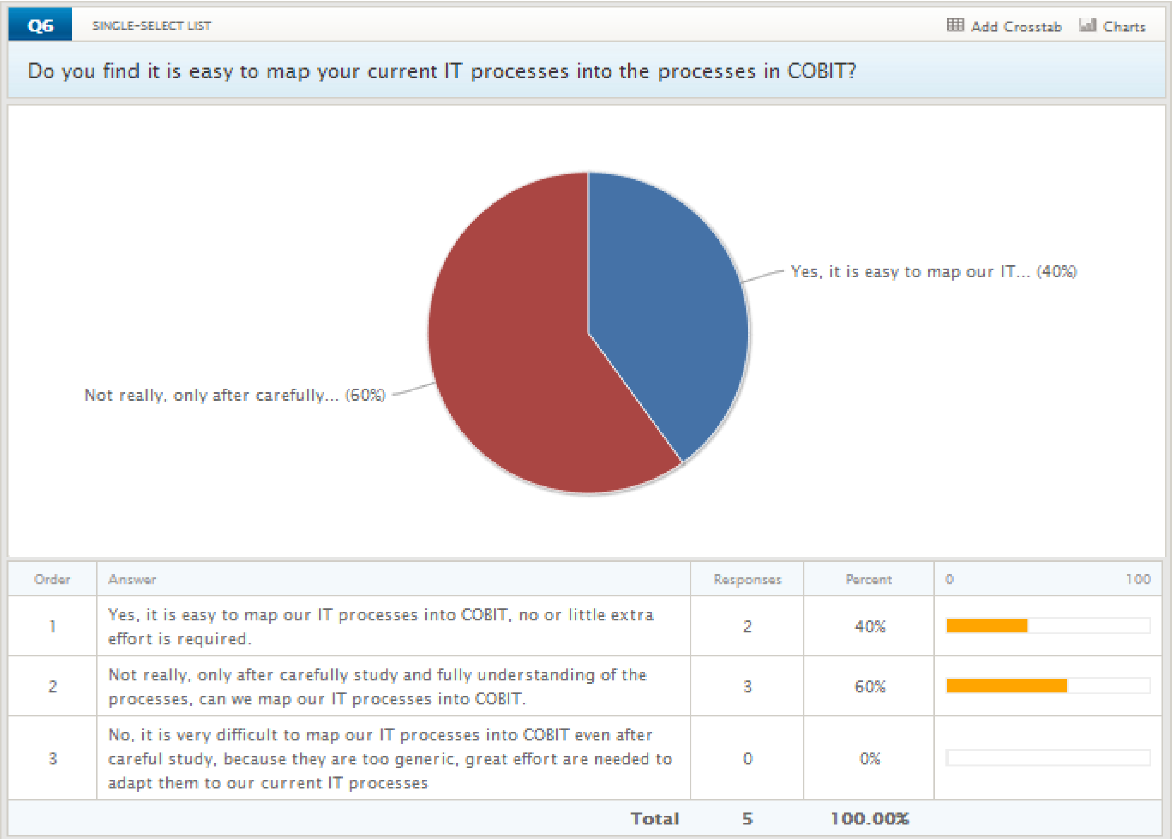
7. Do you think it is easy to set target performance level based on Maturity Model scales?

- ○ Yes, we can easily decide the target levels for each process based the description of different maturity levels; it is easy to link them to our IT goals and needs.
- ○ Not really, we are not sure which level is optimal for each process as the description of different maturity levels do not directly link to our concerns.
- ○ No, one scale is not very distinguishable from the other, it's hard to set desired performance based on these scales;

8. Do you think the best practices are helpful in developing action plans for improving your IT control capability and processes performance?

- ○ Yes, best practices are very practical and applicable
- ○ Not really, best practices are generally good but they are hard to implement
- ○ No, best practices are too generic to apply; great adaption efforts are needed

All the survey results are available from the on-line tool. The following figure is an illustration of the results.


Q6
SINGLE-SELECT LIST
Add Crosstab
Charts
Yes, it is easy to map our IT... (40%)
Not really, only after carefully... (60%)

Do you find it is easy to map your current IT processes into the processes in COBIT?

Order	Answer	Responses	Percent	0 100
1	Yes, it is easy to map our IT processes into COBIT, no or little extra effort is required.	2	40%	
2	Not really, only after carefully study and fully understanding of the processes, can we map our IT processes into COBIT.	3	60%	
3	No, it is very difficult to map our IT processes into COBIT even after careful study, because they are too generic, great effort are needed to adapt them to our current IT processes	0	0%	
	Total	**5**	**100.00%**	

Figure 16: on-line survey results

Appendix B-Maturity Evaluation

High Level Assessment

Process Importance Scale

1	**inapplicable**
2	**can be useful**
3	**is useful**
4	**is desirable**
5	**a must**

Process Evaluation Form

PROCESS	Description	Importance
1. PLANNING & ORGANISATION		**(1-------5)**
PO1 Define a strategic IT plan	• defines IT goals and priorities based on business objectives •Align all IT resources with business strategy and priorities •Analyze and manage project and service portfolios	
PO2 Define the information architecture	• develop a corporate information architecture and data model • maintain a data dictionary to promote a common use of data throughout all IT applications	
PO3 Determine the technology direction	• creates a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer, such as systems architecture, technological direction, acquisition plans, standards, migration str	
PO4 Define the IT organisation and relationships	• Processes, administrative policies and procedures are in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, segregation of duties, and supervision	
PO5 Manage the IT Investment	• manage IT investment programmes, ensure effective use of IT resources • provides transparency and accountability into the total cost of ownership (TCO)	
PO6 Communicate management aims and directions	• articulate IT mission, service objectives, policies and procedures to stakeholders • ensures awareness and understanding of business and IT risks, objectives and direction and compliance with relevant laws and regulations	
PO7 Manage human resources	• follow defined practices supporting recruiting, training, evaluating performance, promoting and terminating IT workforce	
PO8 Manage quality	• provides clear quality requirements, procedures and policies • quality management system is developed and maintained by proven development and acquisition processes and standards	

PO9 Assess risks	• develop a risk management framework documenting a common and agreed-upon level of IT risks, mitigation strategies and residual risks	
PO10 Manage projects	• establishes an IT project management framework which includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, QA, a formal test plan, and testing and post-implementation review after	
2. ACQUISITION & IMPLEMENTATION		**Importance**
AI1 Identify Automated Solutions	• analysis of new application or function before acquisition or creation	
AI2 Acquire and maintain application software	• Align application development with business requirements and standards	
AI3 Acquire and maintain technology infrastructure	• develop processes for the acquisition, implementation and upgrade of the technology infrastructure • ensures that there is ongoing technological support for business applications	
AI4 Enable operation and use	• provide documentation and manuals for users and IT • provide training to ensure the proper use and operation of applications and infrastructure	
AI5 Procure IT resources	• Procure IT resources, including people, hardware, software and services • develop procedures for procurement, selection of vendors, setup of contractual arrangements, the acquisition itself	
AI6 Manage changes	• formally manage and control all changes, including emergency maintenance, patches for infrastructure and applications within the production	
AI7 Install and accredit solutions and changes	• tests new systems in a dedicated environment with relevant test data • define rollout and migration instructions • release planning, actual promotion to production, and post-implementation review	
3. SERVICE DELIVERY MANAGEMENT		**Importance**

DS1 Define and manage service levels	• provide documented definition IT services of and agreement on service levels • monitor and timely report to stakeholders on the accomplishment of service level	
DS2 Manage third party services	• clearly define the roles, responsibilities and expectations in third-party agreements • review and monitor such agreements for effectiveness and compliance	
DS3 Manage performance and capacity	• periodically review current performance and capacity of IT resources • forecast future needs based on workload, storage and contingency requirements	
DS4 Ensure continuous service	• develop, maintain and test IT continuity plans • utilize offsite backup storage and provide periodic continuity plan training	
DS5 Ensure systems security	• establish and maintain IT security roles and responsibilities, policies, standards, and procedures • perform security monitor and periodic test and implement corrective actions	
DS6 Identify and allocate costs	• build and operate a fair IT costs allocating system to capture, allocate and report IT costs to the users of services	
DS7 Educate and train users	• identify training needs of internal and external users • define and execute effective training and measure the results	
DS8 Manage Service Desk and Incidents	• develop a well-designed and well-executed service desk and incident management process including incident registration, escalation, trend and root cause analysis, and resolution	
DS9 Manage the configuration	• establish and maintain an accurate and complete configuration repository • collect initial configuration information, establish baselines, verify and audit configuration information, and update the configuration repository as needed	
DS10 Manage problems	• identify, classify and resolve problems based on root cause analysis • formulate recommendations for improvement, maintain problem records and review the status of corrective actions	
DS11 Manage data	• identify data requirements, establish effective procedures to manage the media library, backup and recovery of data, and proper disposal of media	

DS12 Manage the Physical Environment	• define physical site requirements, select appropriate facilities, design effective processes for monitoring environmental factors and managing physical access	
DS13 Manage operations	• define operating policies and procedures for effective management of scheduled processing • protect sensitive output, monitor infrastructure performance and ensure preventive maintenance of hardware	
4. MONITORING & CONTROL		**Importance**
M1 Monitor and Evaluate IT Performance	• define relevant performance indicators, systematically and timely report performance, and promptly act upon deviations	
M2 Monitor and Evaluate Internal Control	• monitor and report control exceptions, results of self-assessments and third-party reviews to ensure effective and efficient operations	
M3 Ensure Compliance With External Requirements	• comply with laws, regulations and contractual requirements by identifying compliance requirements, optimizing and evaluating responses, obtaining assurance and integrating IT's compliance reporting with business	
M4 Establishment of an IT Governance Framework	• define organizational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives	

Table 9: Process Evaluation Form

Results from 7 IT Managers

PROCESS	**M1**	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**AVG.**
AI6 Manage changes	5				5	5	4	**4.75**
PO1 Define a strategic IT plan	4	5	5	5	5	5	4	**4.71**
DS13 Manage operations	5	5		5	5	4	4	**4.67**
DS8 Manage Service Desk and Incidents	4				5	5	4	**4.50**
PO10 Manage projects	5	5	5	3	5	5	3	**4.43**
DS5 Ensure systems security	4	4		5	4	5	4	**4.33**
PO7 Manage human resources	5	5	5	5	3	4	3	**4.29**
AI4 Enable operation and use	4	5	5	4	5	4	3	**4.29**
AI2 Acquire and maintain application software	4	5	5	3	5	4	4	**4.29**
AI1 Identify Automated Solutions	4	4	5	3	5	5	4	**4.29**

DS10 Manage problems	4				5	4	4	**4.25**
M1 Monitor and Evaluate IT Performance	4	5		4	5	4	3	**4.17**
M3 Ensure Compliance With External Requirements	5	4		4	4	5	3	**4.17**
DS4 Ensure continuous service	5	5		5	3	3	4	**4.17**
PO6 Communicate management aims and directions	5	5	4	4	2	4	4	**4.00**
PO8 Manage quality	5	5	4	3	2	5	4	**4.00**
PO9 Assess risks	4	5	4	4	4	3	4	**4.00**
AI3 Acquire and maintain technology infrastructure	4	4	3	4	5	4	4	**4.00**
M2 Monitor and Evaluate Internal Control	4	4		3	5	4	4	**4.00**
PO2 Define the information architecture	4	5	4	3	2	5	4	**3.86**
PO5 Manage the IT Investment	5	2	4	4	4	4	4	**3.86**
PO4 Define the IT organisation and relationships	4	3	4	3	5	4	4	**3.86**
AI5 Procure IT resources	3	3	5	3	5	4	4	**3.86**
DS12 Manage the Physical Environment	4	4		4	4	4	3	**3.83**
DS2 Manage third party services	5	5		2	2	5	4	**3.83**
DS11 Manage data	4	4		4	3	4	4	**3.83**
M4 Establishment of an IT Governance Framework	3	3		3	5	5	4	**3.83**
DS9 Manage the configuration	3				5	4	3	**3.75**
DS3 Manage performance and capacity	4				3	4	4	**3.75**
DS7 Educate and train users	4	5		3	4	3	3	**3.67**
AI7 Install and accredit solutions and changes	4				2	5	3	**3.50**
DS1 Define and manage service levels	4				3	4	3	**3.50**
PO3 Determine the technology direction	5	3	3	4	1	4	4	**3.43**
DS6 Identify and allocate costs	4				2	4	3	**3.25**

Table 10: high level assessment results

Low Level Assessment

Maturity Level Scale

Score	**Level**	
0	**non existing**	processes are not applied at all
1	**initial ad hoc**	processes are ad hoc and disorganized
2	**repeatable intuitive**	processes follow a regular pattern
3	**defined process**	processes are documented and communicated
4	**managed and measurable**	processes are monitored and measured
5	**optimized**	best practices are followed and automated

Maturity Assessment Form

POCESS	SUB-CONTRROL OBJECTIVES	DESCRIPTION	CURRENT SCORE
PO3-Define the information technology direction	PO3.2 - Technology Infrastructure Plan	Create and maintain infrastructure plan	
	PO3.3 - Monitor Future Trends and Regulations	Monitor technology evolution.	
AI3-Acquire and Maintain Technology Infrastructure	AI3.1 - Technological Infrastructure Acquisition Plan	Define acquisition procedure/process.	
	AI3.3 - Infrastructure Maintenance	Develop a strategy and plan for infrastructure maintenance.	
DS2-Manage third party services	DS2.1 - Identification of All Supplier Relationships	Identify and categorise third-party service relationships.	
	DS2.2 - Supplier Relationship Management	Define and document supplier management processes. Establish supplier evaluation and selection policies and procedures.	
	DS2.3 - Supplier Risk Management	Identify, assess and mitigate supplier risks.	
	DS2.4 - Supplier Performance Monitoring	Monitor supplier service delivery. Evaluate long-term goals of the service relationship for all stakeholders	
DS3-Manage performance and capacity	DS3.2 - Current Performance and Capacity	Review current IT resource performance and capacity.	
	DS3.3 - Future Performance and Capacity	Conduct IT resource performance and capacity forecasting. Conduct gap analysis to identify IT resource mismatch.	
	DS3.5 - Monitoring and Reporting	Continuously monitor and report the availability, performance and capacity of IT resources.	
DS4 - Ensure Continuous Service	DS4.2 - IT Continuity Plans	Develop and maintain IT continuity plans.	
	DS4.3 - Critical IT Resources	Identify and categorise IT resources based on recovery objectives.	
	DS4.5 - Testing of the IT Continuity Plan	Regularly test IT continuity plans.	
	DS4.8 - Service Recovery and Resumption	Plan IT services recovery and resumption.	

	DS4.10 - Post-Resumption Review	Establish procedures for conducting post-resumption reviews.	
DS5-Ensure systems security	DS5.4 - User Account Management	Periodically review and validate user access rights and privileges.	
	DS5.5 - Security Testing, Surveillance and Monitoring	Conduct regular vulnerability assessments.	
	DS5.6 - Security Incident Definition	Clearly define characteristics of potential and actual security incidents.	
	DS5.10 - Network Security	Implement and maintain technical and procedural controls to protect information flows across networks.	
DS7-Educate and train users	DS7.1 Identification of Education and Training Needs	Identify and characterise users' training needs.	
	DS7.2 - Delivery of Training and Education	Build a training programme. Conduct awareness, education and training activities.	
	DS7.3 - Evaluation of Training Received	Perform training evaluation. Identify and evaluate best training delivery methods and tools.	
DS12-Manage the physical environment	DS12.2 - Physical Security Measures	Define the required level of physical protection.	
	DS12.3 - Physical Access	Define and implement procedures for physical access authorisation and maintenance.	
	DS12.5 - Physical Facilities Management	Manage the physical environment (including maintaining, monitoring and reporting).	
DS13-Manage ICS operations	DS13.1 - Operations Procedures and Instructions	Create/modify operations procedures (including manuals, checklists, shift planning, handover documentation and escalation procedures).	
	DS13.2 - Job Scheduling	Schedule workload and batch jobs. Apply fixes or changes to the schedule and infrastructure.	
	DS13.3 - IT Infrastructrure Monitoring	Monitor infrastructure and processing, and resolve problems.	
	DS13.5 - Preventive Maintenance for Hardware	Schedule and perform preventive maintenance.	

ME1 - Monitor and Evaluate IT Performance	ME1.2 - Definition and collection of Monitoring Data	Identify and collect measureable objectives that support the business objectives.	
	ME1.3 - Monitoring Method	Create scorecards.	
	ME1.4 - Performance Assessment	Assess performance.	
	ME1.5 - Board and Executive Reporting	Report performance.	
	ME1.6 - Remedial Actions	Identify and monitor performance improvement actions	

Table 11: maturity assessment form

Results of maturity evaluation

Process	Infra	Communication	OES	Windows
DS4 Continuous Service	2.4	3.2	2.6	1.9
DS13 Operations	2.5	0.8	3.3	2.3
DS5 Systems security	2.2	0.3	2.5	2.5
ME1 Monitor	2.6	1	3.2	2.5
DS7 Train users	1.3	1.3	1.1	1.4
DS2 Third party	2.6	3.3	2.4	2.6
DS12 Physical environment	2.3	0	1.8	3.6
DS3 Performance&capacity	3.1	4.2	3	2.6
PO3 Technology direction	2.2	3.3	2.1	1.7
AI3 Acquire Infrastructure	2.5	2.8	2.6	2.2

Table 12: maturity evaluation results