Journal of Economics, Business and Management, Vol. 1, No. 4, November 2013

An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model

Shengnan Zhang and Hans Le Fever

***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. A pilot COBIT program within an IT department was carried out to collect primary data. The actual usage of COBIT tools is analyzed and compared to their theoretical design. Practical problems of COBIT framework are identified. A COBIT-BSC model is proposed to illustrate a simple way of structuring COBIT control objectives. This study will contribute some practical insights to COBIT framework and help organizations take advantage of COBIT as well as other IT control frameworks.**

***Index Terms*—COBIT, IT Governance, balanced scorecard, control frameworks, IT standards, ISO27000, ITIL, IT audit.**

I. Introduction

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 [1]. 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 [2]. A number of IT governance frameworks, such as ITIL, COBIT, ISO17799 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 [3] 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 [4] that the usage of COBIT decreased from 14% in 2008 to 12.9% in 2010. This trend proves the conclusion that COBIT is not as easily implemented as originally estimated [5]. 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.

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 was carried out to gather primary data. Practical problems and value for adopting and implementing COBIT framework are identified A COBIT-BSC model is proposed to illustrate a simple way of structuring COBIT control objective based on five views in Balanced Scorecard (BSC). It provides an overview for management to understand COBIT and its relation to other popular IT standards.

II. IT Governance Framework

A. 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" [6]. 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

Manuscript received March 3, 2013; revised May 14, 2013.

S. Zhang is with Leiden University, Verlengde Wassenaarseweg 16H Oegstgeest, 2342BG, the Netherlands (e-mail: Sophie112zsn@gmail.com).

H. LeFever is with Leiden Institute of Advanced Computer Science, Postbus 9512, 2300 RA Leiden (e-mail: h.t.le.fever@umail.leidenuniv.nl).

performance [7].

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 [8].

B. IT Control Framework

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. There are three categories of control frameworks [9]:

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';

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.

C. 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 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.

D. 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.

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.

E. COBIT

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. COBIT 5 is developed by consolidating and integrating the COBIT 4.1, Val IT (a collection of management practices and techniques for evaluating and managing investment in business change and innovation) and Risk IT (a framework launched by ISACA aiming to integrate the management of IT risk into the overall Enterprise Risk Management) into one single business framework [10].

1) 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 (*Effectiveness Efficiency, Confidentiality, Integrity, Availability, Compliance, Reliability*), IT resources (*People, Applications, Technology, Facilities, Data*) and IT processes form the three main dimensions of COBIT conceptual framework.

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: Plan and Organise, AI: Acquire and Implement, DS: Deliver and Support and ME: Monitor and Evaluate*) plus a process number and a control objective number. COBIT 4.1 has 34 high level processes that cover 222 control objectives.

COBIT presents IT activities in a hierarchical structure from the highest domain level to IT processes and to the lowest level of IT activities.

2) 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.

III. COBIT Reviews

Despite the fact that COBIT is becoming an influential framework for IT control and governance, study on COBIT literature and utilization [11] reveals that there is relatively little academic literature that has been published investigating the utilization of COBIT. Some researchers [12] 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. There are also many other weaknesses, such as the lacks of guidance, complex structures. The number of case studies on COBIT is very limited.

In order to fill this gap and add more practical insights on COBIT, this research explore the actual usage of COBIT in an IT department at a international company. The following part is the summary of the main findings.

A. Actual Usage COBIT Tools

The fundamental tools introduced in COBIT are *Performance Goals& Metrics* (enabling IT performance to be measured), *RACI Charts* (identifying who are Responsible, Accountable, Consulted, or Informed for specific IT process), and *Maturity Model*(assisting in benchmarking and decision-making for process improvements).

1) 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. Secondly, the various measurements and metrics do not make much sense for real IT management. It is pointed out [13] 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. 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?

2) 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.

3) 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.

However, it should be noticed that companies must customize an efficient method to measure their maturity levels. The description of Maturity Model in COBIT 4.1 is still complicated.

B. Practical Problems of COBIT

1) 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*:explains how COBIT organizes IT governance, management and control objectives and good practices by IT domains and processes, and links them to business requirements; *Control Objectives:* provides generic good practice management objectives for IT processes; *Management Guidelines*: offers tools to help assign responsibility, measure performance, and benchmark and address gaps in capability;*Maturity Model*: provides profiles of IT processes describing possible current and future states.

It 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. 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.

2) 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 more matured IT standards like ISO27000 and ITIL, the value of COBIT is hard to perceive. There are no proven statistics or studies confirming its claimed advantages. 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. Management are still dubious about COBIT and 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.

IV. New COBIT-BSC Model

A. Grouping COBIT Control Objectives

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. Therefore we are inspired to find an easier way for organizations to capture the essence of COBIT and its relations to other popular IT standards.

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 [14] and more practical analysis. We notice that the driving factor for ISO27001 certification is mainly to satisfy and assure customers and stakeholders. Besides, 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 that are covered by ITIL are easy to be identified as most of them share same terms. After excluding above control objectives, the remaining ones fall into three categories: high-level IT strategies, IT Financial issues and Learning and Training.

B. Fitting into Balanced Scorecard

It is interesting to notice that these five categories fit well into the views in Balanced Scorecard (BSC). BSC is first developed by Kaplan and Norton [15] 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.

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 1 illustrates this model.

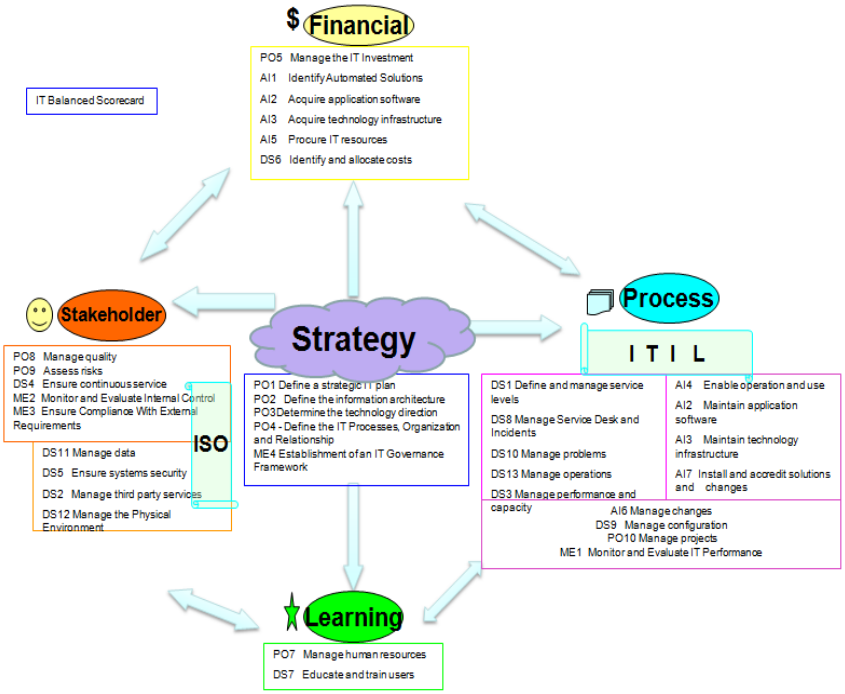

Fig. 1. COBIT-BSC model.

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 user

V. Conclusions and Discussions

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. 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. In order to solve these problems, a COBIT-BSC model is proposed to illustrate a simple way of structuring COBIT control objectives.

Due to the scale of this study, the amount of data collected is limited. Conclusions are drawn based on analysis available resources. It is necessary to collect more inputs and criticisms from more IT practitioners and COBIT experts. Besides, the proposed COBIT-BSC model only illustrates a simple view of 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. Still, the validity of categorizing each control objectives needs further discussions.

References

[1] ITGI. (2007). *COBIT 4.1*. IT Governance Institute. [Online]. Available: www.itgi.org

[2] W. Van Grembergen and S. De Haes, "Measuring and improving IT governance through the balanced scorecard," *Information Systems Control Journal*, vol. 2, no. 1, pp. 35-42, 2005.

[3] M. Simonsson, P. Johnson, and H. Wijkström, "Model based it governance maturity assessments with COBIT," *the 15th European Conference on Information Systems.* Switzerland, 2007.

[4] ITGI. (2011). *Global Status Report on the Governance of Enterprise IT (GEIT)—2011*. IT Governance Institute. [Online]. Available: www.itgi.org

[5] ITGI. (2006). *Global Status Report on the Governance of Enterprise IT (GEIT)—2006.* IT Governance Institute. [Online]. Available: www.itgi.org

[6] P. Webb, C. Polland, and G. Ridley, "Attempting to Define IT Governance: Wisdom or Folly," *Proceedings of the 39th Annual Hawaii International conference on System Sciences*, pp. 194a-194a, vol. 8, IEEE Computer Society, 2006.

[7] ITGI. (2007). *COBIT 4.1*. IT Governance Institute. [Online]. Available: www.itgi.org

[8] M. Spremic, "Measuring IT Governance Performance," *International Journal of Mathematics and Computer in Simulation*, 2012.

[9] M. Nicho, "Information technology audit: systems alignment and effectiveness measures," Thesis of Doctor of Philosophy, AUT University, Auckland, 2008.

[10] ISACA. (2012). *COBIT Document.* Retrieved 2013. [Online]. Available: http://www.isaca.org/COBIT/Documents/Compare-with-4.1.pdf

[11] G. Ridley, J. Young, and P. Carroll, "COBIT and its Utilization: A framework from the literature," in *Proc. the 37th Hawaii International Conference on System Sciences*, vol. 8, pp. 1-8, 2004.

[12] M. Simonsson, P. Johnson, and H. Wijkström, "Model based IT governance maturity assessments with COBIT," *The 15th European Conference on Information Systems*, vol. 34, 2007.

[13] M. Buzina. (2011). *Is COBIT practical enough for real world usage?* [Online]. Available: http:// buzina.wordpress.com /2011/08/30/ is-cobit-practical-enough-for-real-world-usage/

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

[15] B. Kaplan and D. Duchon, "Combining qualitative and quantitative methods in information systems research: a case study," *MIS Quarterly*, pp. 571 -587, 1988.

Shengnan Zhang is a master graduate of Leiden University, the Netherlands. Her master thesis topic is on IT governance frameworks. She conducted her research by a COBIT pilot project at an IT department of an international company. This paper is based on the findings of her master thesis. She obtained 9 (out of 10) for her thesis defense is honored with Cum Laude for her graduation.

Her bachelor thesis, *Dynamic Scoring Model in University Students' Comprehensive Evaluation System*, was published by Advances in Artificial Intelligence (ISSN 2160-147X) at the 2011 International Conference on Management Science and Engineering (MSE 2011, 417).

Hans Le Fever is the programme director M.Sc. ICT in Business of Leiden University. He obtained a PhD in experimental physics at Leiden and worked at Shell for 22 years in a variety of planning and IT Management functions. Since 2003 he is an independent consultant serving Dutch (multinational) companies in the area of innovation and managing IT. His recent focus is on early stage Venture development in Life Sciences, Bio-Based Economy and IT. He has shared his knowledge at various academic institutions, business seminars and in-company programmes.

His publication includes: Living Lab: Innovation through Pastiche (a research linking disparate and discorded ontology). In: P. Cunningham & M. Cunningham (Eds.), *eChallenges e-2012 Conference Proceedings*, IIMC International Information Management Corporation (2012)