Received: 06 April 2021 | Accepted: 06 May 2021
DOI: 10.52898/ijif.2021.2

ORIGINAL ARTICLE

Partial Implementation of COBIT and Possible Risks

Yunus Emre GÜRBÜZ
Zübeyir ERGENEKON

Abstract
COBIT is one of the most adopted IT audit framework in the world. Some companies think to implement COBIT partially, not all process of COBIT. In this paper, we are going to give some tips to implement COBIT partially in an effective way. We also analyze the holistic approach of COBIT and show some examples about partially implementing which destroy the 'holistic approach'.

Examples are given from COBIT's PO (Plan and Organise) domain and a combined working process (such as Incident management and change management). Our study will be a guide for sectors that are considering to partially address COBIT, such as the insurance industry.

Keywords
Information Technologies, Insurance

JEL Classification
G22, M15

Authors Notes:
Correspondence
Neova Insurance, Head of Internat Audit,
ORCID: 0000-0003-2355-1852,
gurbuzyunus@gmail.com

Neova Insurance, IT Auditor,
ORCID: 0000-0003-4747-9402,
zubeyirergenekon@gmail.com

1. INTRODUCTION

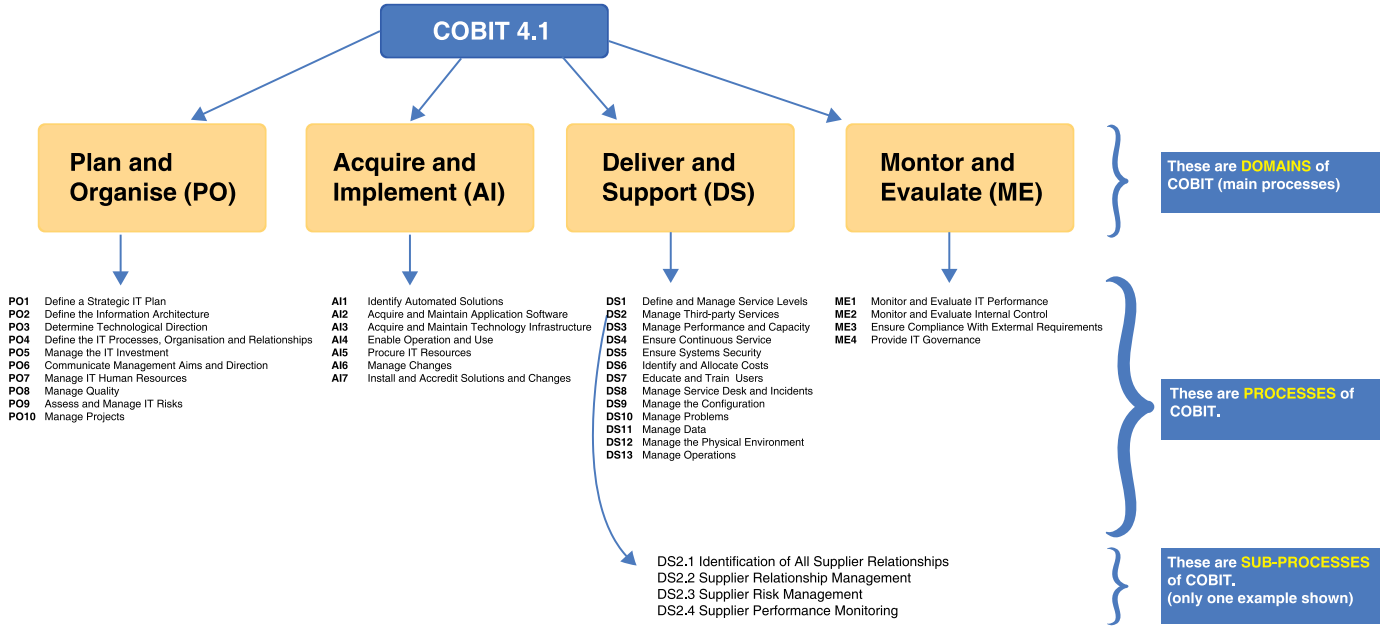
COBIT (Control Objectives for Information and Related Technology) is recognized as a set of best practices for IT management and audit worldwide. The first COBIT version was released in 1996 and currently the latest version is COBIT 2019. COBIT is published by an independent, non-profit organization, which is called ISACA and based in America.

In this paper we will make our comments on COBIT 4.1 version. Our comments maybe are appropriate for other versions of COBIT (COBIT 5 or COBIT 2019) but we have not tested for other versions. Because even though the versions change, the logic of COBIT and many processes remain the same.

COBIT is used in many countries and in many sectors such as finance, telecommunication, energy and insurance for IT audit and governance. But since this is not the subject of our article, we are not going into details. Those who want a detail can see detailed information at ISACA (COBIT Global Regulatory and Legislative Recognition, ISACA, 2014).

In COBIT 4.1, there are 34 processes of 4 main processes and 210 audit criteria related to these processes. You can see the domains (main processes), processes and sub-processes of COBIT at the Table 1 below.

Table 1. COBIT processes



The increasing importance of information systems has led to an increase in audit and management perception on information systems. In response to this increasing demand, we were met the best practices such as COBIT, ITIL, IS0 27001. While ITIL aims to increase the quality of IT services within IT unit, COBIT aims IT to work in line with the company's strategic goals. ISO 27001 is a standard that deals with data security. The working principles of COBIT and ITIL are in line with the universal data security principles on which ISO 27001 is based.

At this point, we face a new problem. This is how to implement applications such as COBIT and ITIL in business life. Therefore, the value of research and studies on the implementation of standards has increased. In some countries, insurance companies are not as financially rich and not enough regulated as banks; In this case, sectors such as insurance have difficulty in implementing information governance practices such as COBIT. The primary implementation problem is the partial implementation of the COBIT framework, which is difficult to fully implement. Because COBIT is comprehensive and complex, it makes it difficult to fully implement, and it requires serious effort and cost to fully implement. However, examples and case studies at the point of application and partial application are very few. Üvey (2013) also points to this difficulty. Uzunay (2007) stated that COBIT emphasizes the activities that businesses need to do in order to be successful but is not interested in how to do these activities. One reason for the implementation challenge is that COBIT is in this open structure. In this study, we will consider whether COBIT may be implemented partially or not.

2. LITERATURE REVIEW

Zhang and Fever (2013) have written an article on the adaptation of COBIT to BSC (Balance Scorecard). Although the study is not a completely partial application, it sets an example in terms of handling the COBIT processes in different groups. However, Zhang et al. (2013) stated that there was a lack of guidance on the implementation and customization of COBIT and that ISACA presented very few case studies on this subject. Moeller et al. (2013) wrote articles on the sustainability of COBIT 5.

Anomah and Aduamoah (2018) stated in their study that the implementation guidelines for COBIT 5 could not provide guidance on customization. They developed a model for an audit tool with customizing the COBIT 5.

Bartens et al. (2015) have written an article about Using Expert Views for Selective Implementation of COBIT 5. Considering the scarcity of studies on the partial implementation point, we can say that this article is important.

Ana Claudia Martins Amorim (2018) stated in her study that pre-implementation lessons and practical examples for COBIT were scarce and emphasized that due to the complexity, formal implementation guidance was abandoned, and partial implementation was made.

Efe (2013) stated in his study that full compliance to COBIT of regional development agencies may not be possible for but conceptually COBIT can provide a reliable basis for e-government and e-governance requirement of regional development agencies.

As can be seen in the literature review above, there are very few studies and examples regarding the implementation and customization of COBIT, we could not find a study that deals with the partial implementation that we especially focused on.

3. METHODS

3.1. Risks of Implementing COBIT Partially

COBIT is designed to provide integrated IT governance from planning to monitoring. If we select some processes in COBIT and ignore others, we will prevent efficient IT governance and negative results may occur which we present some examples below. In this context, there is a need to identify situations in which processes work with each other and with the overall COBIT system.

However, it is not easy for each company to implement all processes of the COBIT framework at once. This process requires serious labor, money and time. In addition, some companies may not need to implement all COBIT processes due to their business scope.

Therefore, partial implementation of COBIT should be carried out with great care. The COBIT processes to be implement cannot be randomly selected. For this reason, we need to examine the processes of COBIT and how the processes are related to each other so that we can apply COBIT partially without disrupting the integrated and holistic perspective of COBIT. Unfortunately, we have not enough resources, studies and documents to implement COBIT partially. Despite I contact ISACA for this problem, I have not got enough and satisfying answer.

We must clearly say that companies considering partial implementation should analyze well the interdependence and relationship of the processes they have chosen. It should be taken into consideration which processes provide data input / output to which processes and a method that will not harm COBIT's holistic perspective should be chosen. This is possible by understanding the interrelationships of processes and calculating what will be lost when a process is not implemented. Therefore, in our article, we have provided examples of what processes that are not implemented can cause. At this point, the "COBIT Quick start" approach, which we have included in the following pages of the article, offers a good methodology for partial implementation. COBIT Quick Start version has preferred a partial application method by making a reduction in COBIT sub-processes, not in COBIT processes.

COBIT management guidelines describe the interrelations of processes (IT Govarnance Institute, 2007). In this way, we can understand what processes a process provides input and what processes process a process can benefit from (Table 2).

Table 2. Interrelations of PO9 with other COBIT process

From	Imputs
P01	Strategic and tactical IT plans, IT service portfolia
P010	Project risk management plan
DS2	Supplier risks
DS4	Contingency test results
DS5	Security threats and vulnerabilities
ME1	Historical risk trends and events
ME4	Enterprise appetite for IT risks

Outputs	To						
Risk assessment	P01	DS4	DS5	DS12	ME4		
Risk reporting	ME4						
IT-related risk management guidelines	P06						
IT-related risk emedial action plans	P04	AI6					

In Table 2, we can see for PO9 interrelations with other processes. PO1, PO10, DS2, DS4, DS5, ME1, ME4 processes provide data for the PO9 process. In the same way, in the "output" section we can see, for which processes PO9 provides information to. These are PO1, ME4, PO6, PO4.

Examples of sub-processes that may pose a risk if not implemented together are as follows:

3.2. Occurring Risks When We Do Not Implement PO2

Related Processes: DS11 Manage Data (PO2.3 Data Classification Scheme provides essential data for DS11)

The PO2 process of COBIT aim to define information architecture. PO2.3 which is a sub-process of PO2 is about classification of data. PO2 provides a schema to be classified according to the criticality and sensitivity of corporate data. For example, the data can be classified according to the need of the organization in the form of 'public, confidential, top secret' and so on. With this structure which is classify the data; information such as data ownership details, appropriate security levels and protection controls, data retention and destruction criteria are kept. These data are needed for the correct implementation of operations such as access controls, archiving and encryption.

The DS11 process includes arrangements related to Data Management. If we don't have information about the classification of the data, we can't talk about the data management being healthy. Data not classified by criticality and sensitivity may cause many problems. Similarly, the sub-process DS 11.4 includes the information of disposal of data. However, the strategic and supportive data that will be the source of disposal operation information is in the process of PO2.3.

In the short words, we cannot effective and efficient data management without classifying the data. Because of ignoring PO2, we may face with problems with data operations such as protection controls, authorization, data storage and destruction criteria. These two processes of COBIT are a good example of how random selection should not be made when implementing COBIT processes. COBIT refers that there are data inputs from PO2 to implement DS11 in the implementation manual (Table 3). This confirms what we have described above.

Table 3. Data Inputs from Other COBIT processes to DS11 process

From	Inputs
P02	Data dictionary; assigned data classifications
AI4	User, operational, support, technical and administration manuals
DS1	OLAs
DS4	Backup storage and protection plan
DS5	IT security plan and policies

Source: IT Governance Institute, COBIT 4.1 Management Guidelines 2007, (online) www.isaca.org, retrieved date 09.08.2018

3.3. Occurring Risks When We Do Not Implement PO3

Related Process: PO3.3 -> Monitor Future Trends and Regulations

PO3 is about determining technological route. The PO3.3 sub-process of this process is concerned with monitoring future trends and regulations and monitors and enforces trends in technological processes. It is important to follow the trends of change and technology with an institutional structure. Otherwise, such values may vary depending on personal policies and competencies.

3.4. Occurring Risks When We Do Not Implement PO5

Related Process: PO5.4 -> Cost Management

Because of the companies are being technological oriented nowadays, IT costs are raising. PO5 of COBIT process present some useful information about cost management. It includes the assessment of the potential effects and the determination of such deviations in the event of a deviation in the budget.

Because of ignoring PO5, we cannot determine the deviations of IT budget and how to affect this to projects. However, cost management is necessary for PO1. We need cost management information in strategic and tactical IT plans.

3.5. Occurring Risk When We Do Not Implement Integrated Processes

We gave some examples above about interrelated processes when you can see with analyzing COBIT processes with care. But some of the COBIT processes are directly interrelated together. COBIT implementation guides point these processes directly. In this chapter we try to give a meaningful example about interrelated process directly.

Incident management, problem management, configuration management, capacity management and availability management are directly integrated with each other. (COBIT DS8.2 and DS10.4 points this direct relationship.)

Incident management tracks the incidents and events. In case of need, some incidents escalate to problem management. If an incident and problem need a software or hardware change, we track this record with change management process. We associate the incidents and problems with configuration items. With the reports of incident and problem management we can obtain capacity needs. Strategic decisions can be acquired from configuration management reports for availability management. To summarize, all this critic processes are interrelated with each other. So, we cannot think ignoring to implement some of these processes.

We need to know what services and works are related with the configuration item. If we stop or change configuration item, what should do we need to do for service continuity? The DS9 process provides some useful data to DS8, DS10 and AI6 processes for the purpose of business continuity.

3.6. Occurring Risks When We Do Not Implement PO7.5 and PO4.13

Related Process: PO7.4 -> Personel Training

PO7.5 -> Dependence Upon Individuals and PO4.13 Key IT Personnel

PO7 process is about management of human resources. PO7.4 sub-process is giving useful advices for personnel training. Education must be provided when an employee hired and other times. IT employee's information, talents and awareness of security are staying up to date with educations. Qualified employees play a large role in the realization of the company's targets. If the training practice does not become a corporate value, the qualifications of employees can be lost over time.

PO7.5 is a sub-process of PO7 which is foreseeing process not to only hold by an employee. As you can guess, information and talents which are holding only by one employee contains major risks for companies. "Key IT personnel" process highlights that critical job functions should not be undertaken by one employee. For the reason of PO4.13 is same line with PO7.5, these processes should be assessed together.

3.7. COBIT 5, COBIT 2019 and Flexibility of Implementing

All COBIT frameworks have their own structure and dynamics even though they are similar in basic. However, companies are insufficient to respond to updated versions of COBIT at the same speed. Altering a development that covers all parts of an organization is a tremendous event.

ISACA emphasizes that COBIT 5 is flexible and can be customized. The clarity of this flexibility in practical

business life is not obvious. On the other hand, the situation of COBIT 2019 is a separate subject of study in terms of partial implementation.

As a result, there is not enough knowledge, source, case analysis and industry experiences related to partial implementation of COBIT. We think that ISACA should seriously consider the partial implementation of COBIT.

3.8. Cobit Quickstart Version

COBIT Quickstart is the recommended version of COBIT for SMEs. At the same time COBIT Quickstart version gives a well thought and designed way to the companies who thinks to implement COBIT partially. In COBIT Quickstart version, the COBIT processes implemented generally. We mean that processes like po1, ds1, po4 are chosen generally and decrease the sub-processes like po1.4, ds4.5 etc. You can see this difference in the Table 4. This is very intelligent and elegant choice. Thus, we do not lose the holistic approach of COBIT. Ignoring to implement COBIT processes could lead to major risks.

Table 4. Comparison for COBIT and COBIT Quickstart

	COBIT	COBIT Quicktart
Domains (Main Processes)	4	4
Processes	34	32
Sub-processes	210	59

Source: IT Govarnance Institute, COBIT Quickstart Framework, second edition, 2007, p.14.

Some companies want to use some COBIT processes to increase their level. But especially for the SME's this is not a practical way for every time. Because you need tremendous work, money and effort to apply COBIT completely. You need additional software, culture change and time. Thus, COBIT Quickstart's way is the best way to implement COBIT partially. We do not defense that you should go with the same line with COBIT Quickstart. You should follow the COBIT Quickstart's thought, mind and choosing techniques.

Some of companies do not want to track an extra way and they want to follow a tested way. In this situation implementing COBIT Quickstart is a good way for some companies. But is COBIT Quickstart fit for our company? How do we know that? You can use these tests for answering this question. With "Stay in the blue zone" and "Watch the heat" tests, you can analyze whether COBIT Quickstart is fit for your company.

4. DISCUSSION

Because of COBIT implementation completely is a huge job and effort, this is not suitable for every company. SMEs can choose for them which they really need and meaningful for themselves. They should determine their risks and they should consider these risks when they are choosing processes. In the process choosing, companies must consider the subject of prevention of COBIT holistic view.

They should choose 34 principal process completely and choose other sub-processes to their needs. They must protect the processes of COBIT completely. They can reduce sub-processes that they think to implement. Ignoring principal processes is not a good way and give damage to the COBIT's mechanism. Sub-processes which are related each other should be searched. They should consider what all sub-processes are intended at.

In the COBIT partially implementation plan and process selection, companies must understand holistic IT governance concept what COBIT offer.

In our study, we have theoretically discussed the risks of partial implementation, it will be useful to conduct research on a business that performs partial implementation. However, further versions of COBIT should also be taken into account and it would be useful to consider further COBIT processes. Also Examples from other COBIT processes can also be reproduced. In this study, as an example, the risk assessment of 5 processes in partial implementation is discussed. As we mentioned earlier, the situation of COBIT 2019 and COBIT 5 is a separate subject of study in terms of partial implementation. However, this study can give an

idea or methodological example for analyzing the risks in different areas for the cases of separating the part from the whole.

Swallowing a drug by dividing it may not harm but using a medicament by removing a component in the drug can seriously damage the structure.

REFERENCES

Amorim A. C. M. (2018). Using Scrum for Implementing IT Governance with COBIT 5 [Master thesis, Instituto Superior Técnico].

Anomah S., Aduamoah M. (2018). Proposed Analytical Procedure for The Customization and Implementation of COBIT 5. EDPACS, 57:3.15-34, DOI: 10.1080/07366981.2018.1433933.

COBIT Global Regulatory and Legislative Recognition [Fact sheet]. ISACA. https://www.isaca.org/COBIT/Documents/Recognition-table.pdf

Bartens Y., S. De Haes, Y. Lamoen, F. Schulte and S. Voss., (2015). On the Way to a Minimum Baseline in IT Governance: Using Expert Views for Selective Implementation of COBIT 5. 48th Hawaii International Conference on System Sciences, Kauai. 4554-4563, doi: 10.1109/HICSS.2015.543.

Efe A. (2013). COBIT 5 Framework as a model for the Regional Development Agencies In Turkey. International Journal of eBusiness and eGovernment Studies Vol.5, No.1.

IT Govarnance Institute, (2007). COBIT® 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models.

Moeller, B. & Erek, K. & Loeser, F. & Zarnekow, Ruediger. (2013). How Sustainable is COBIT 5? Insights from Theoretical Analysis and Empirical Survey Data [Conference presentation]. 19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime. 3.

Uzunay, Vildan, (2007). COBIT (Control Objectives for Information ve related Technology). [Vocational Qualification Thesis].

Üvey, M. Cüneyt (2018). Orkestra Şefiniz: COBIT. ISACA. https://www.isaca.org/Knowledge-Center/cobit/Documents/COBITarticle-turkish.pdf

Zhang S. & Fever, H. L, (2013). An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model. Journal of Economics, Business and Management, Vol. 1, No. 4, 391-395. DOI: 10.7763/JOEBM.2013.V1.84

How to cite this article: Gürbüz, Y. E. & Ergenekon, Z. (2021). Partial Implementation of COBIT and Possible Risks. International Journal of Insurance and Finance, 1(1), 9-15. https://doi.org/10.52898/ijif.2021.2