International Symposium on Advances in Science and Technology
Bandar-Abbas | Iran
7-8 March 2013
7th SASTech
Persian Gulf
Hosted by:
Hormozgan University
Organised by:
Khavaran Institute of Higher Education

Proposing a Method for Measuring the confidentiality of Enterprise Architecture Based On COBIT

Marzieh Moheb,shiraz university,student
m.moheb598@gmail.com

Sayed Raouf Khayami,sanati shiraz university,professor
khayami@sutech.ac.ir

Paper Reference Number: 07-04-0414

Name of the Presenter: Marzieh Moheb

Abstract

As the enterprise is being matured and trying to develop IT governance, the recognition of technical and managerial dimensions of the enterprise as well as development and assessment of Enterprise Architecture (EA) plan is becoming one the important issues. Recently various papers focus on EA assessment, offering different methodologies. Since one of main goals of developing the EA plan is IT governance, the implementation of well-suited plans can be used as a powerful tool in IT management decisions. It implies that the EA assessment model according to this view is considerable. This model follows assessment process based on different information criteria that are effective in developing the good and qualified EA plan. In this research, we try to offer critical indicators for assessing the EA plan with concern to confidentiality as one of the information criteria from the perspective of IT governance. These indicators are based on one of the IT service management frameworks, named COBIT[1]. The result of this research is an assessment method, consisting of the critical confidentiality indicators, the method of indicator's measurement and the layer of assessment for each indicator according to EA plan structure.

Key words: Enterprise Architecture, Enterprise Architecture, Enterprise Architecture criteria, IT governance, Confidentiality

1. Introduction

Information technology benefits make the enterprise increase the use of this capability. Optimum use of information technology requires the accurate knowledge in various aspect of enterprise. This knowledge helps the enterprise to have dynamism and agility, make informed decisions and change rapidly against internal and external drivers.

During the last decade, enterprise architecture (EA) has grown into an established approach for holistic management of information systems and other IT services in an organization(

[1] control objectives for information and related technology

Johnson P& Johansson E,2007). The EA solution gives the comprehensive understanding in different organizational dimensions such as strategy, process, knowledge, products, services and information infrastructure and the strategic relationships between them. It uses the output to identify and analyze the As-is state, offer the To-Be state according to enterprise strategic goals and finally show the roadmap in order to migrate from As-is to To-Be state (Razavi ,2009).

Due to the variation of enterprise activities, level of maturity, rapid development of technology tools and high implementation cost, analyzing the EA plan based on enterprise current situation, goals, strengths and weaknesses, threats and opportunities seems to be imperative.

In recent years the assessment concept has been considered and Valuable research in this regard has been provided. These researches classified in to two groups of qualitative and quantitative assessment. Qualitative assessment that will be discussed in this research is based on representing the quality attributes and providing the mechanism for measuring the level of quality. The selected mechanism is different based on assessment methodologies. Since the EA describes all aspect of enterprise in IT perspective, the implementation of well-suited plans can be used as a powerful tool in IT management decisions and IT governance. It implies that the most significant feature of an acceptable EA plan is IT governance establishment according to business goals. In this paper we propose a method for qualitative assessment of confidentiality as one of the quality attributes based on IT governance view. To this aim we utilize COBIT framework, which is comprised of 34 high-level control objectives and 318 detailed control objectives that have been designed to help businesses maintain effective control over IT and ensure that the enterprise’s IT sustains and extends the organization’s strategies and objectives as well ,That is the exact meaning of IT governance. The next section describes this framework in more details. To identify the confidentiality indicators, we study COBIT process model and control objectives. The next step will be redefining identified indicators according to EA scope. In order to make the method applicable, we show how to measure the indicators and determine the related layers of an EA plan for measuring each indicator.

The outline of this paper is as follows. Section 2 Introduces the COBIT IT service management framework and its characteristics and defines confidentiality attribute from EA perspective. Section 3 is devoted to the explanation of the method in step by step manner. Finally in section 4 we have paper conclusion.

2.Data and Material

In this section, first, the COBIT framework will be introduced and then we will define confidentiality attribute in EA scope.

2.1. COBIT framework

Control Objectives for Information and Related Technologies (COBIT) is an international standard, prescribing IT governance (Harryparshad ,2011), which was initially intended to be used by organizations for benchmarking; subsequently it has been used for internal and external auditing of systems (Tuttle and Vandervelde, 2007). This framework incorporates business and IT goals in its monitoring of the information metric system (Radovanovi, et al, 2010) with the main characteristics of being business-focused, process-oriented, controls-based and measurement-driven.

- **business-focused**

Business orientation is the main theme of COBIT. It is designed not only to be employed by IT service providers, users and auditors, but also, and more important, to provide comprehensive guidance for management and business process owners. Managing and controlling information are at the heart of the COBIT framework and help ensure alignment to business requirements. To satisfy business objectives, information needs to conform to certain control criteria, which COBIT refers to as business requirements for information. Based on the broader quality, fiduciary and security requirements, seven distinct, certainly overlapping, information criteria are defined as follows.

- **Effectiveness** deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- **Efficiency** concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Confidentiality** concerns the protection of sensitive information from unauthorized disclosure.
- **Integrity** relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- **Availability** relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- **Compliance** deals with complying with the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies.
- **Reliability** relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities

- **Process-oriented**

To govern IT effectively, it is important to appreciate the activities and risks within IT that need to be managed. They are usually ordered into the responsibility domains of plan, build, run and monitor. COBIT defines IT activities in a generic process model within four domains these domain are called:

- **Plan and Organise (PO:** Provides direction to solution delivery (AI) and service delivery (DS).
- **Acquire and Implement (AI):** Provides the solutions and passes them to be turned into services.
- **Deliver and Support (DS):** Receives the solutions and makes them usable for end users.
- **Monitor and Evaluate (ME**) :Monitors all processes to ensure that the direction provided is followed.

- **Controls-based**

COBIT defines control objectives for all 34 processes, as well as overarching process and application controls. Control is defined as the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

- **Measurement-driven**

A basic need for every enterprise is to understand the status of its own IT systems and decide what level of management and control the enterprise should provide. Enterprises need to measure where they are and where improvement is required, and implement a management tool kit to monitor this improvement. COBIT deals with these issues by providing:

- **Maturity models** to enable benchmarking and identification of necessary capability improvements
- **Performance goals and metrics** for the IT processes, demonstrating how processes meet business and IT goals and are used for
- measuring internal process performance based on balanced scorecard principles
- **Activity goals** for enabling effective process performance (ITGI, 2007).

2.2. Confidentiality information criteria

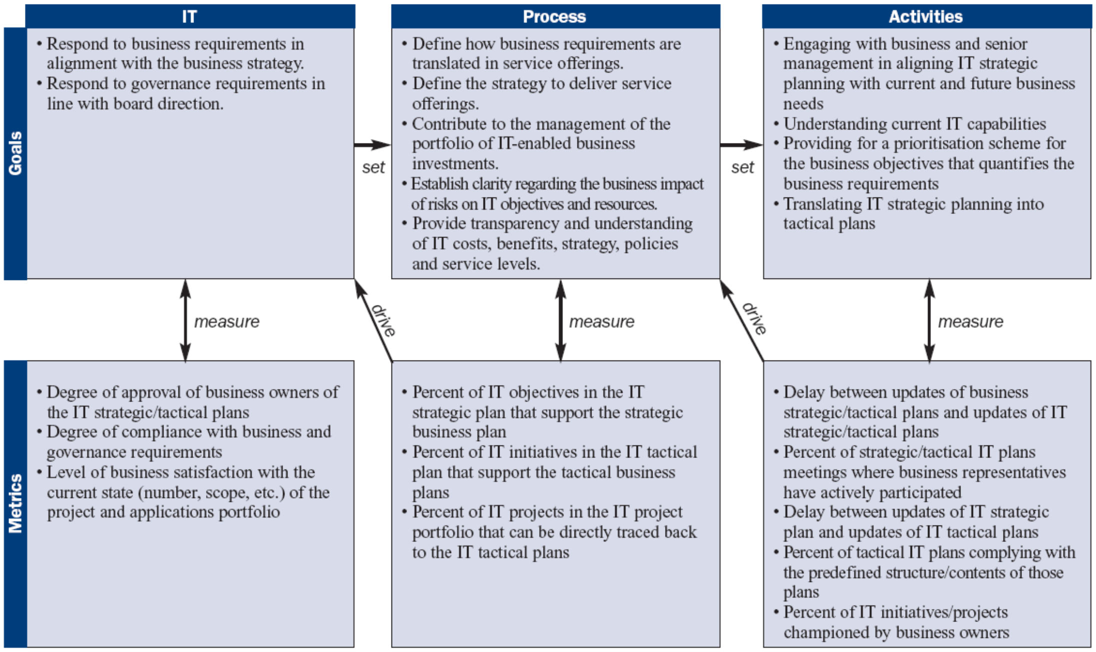
As defined in COBIT, confidentiality concerns the protection of sensitive information from unauthorized disclosure. Managing confidentiality across an enterprise has become a major concern of businesses and governments. As networks extend our ability to communicate widely, they expose us to hackers, business competitors, disgruntled co-workers, and other predators with vandalistic or larcenous intent (Allen W, 2011) A successful worm attack within an enterprise network can be substantially more devastating to most companies compare to larger internet [3]. Obviously, according to the importance of this information criterion, a well-defined EA plan should consider the security strategies and key factors in order to ensure the managerial board and other stakeholders of this concept. In the next section we will propose a method to assess the EA plan confidentiality from based on COBIT framework.

3. Assessment framework

In this section we propose the assessment framework in 3 main steps as follows.

3.1. Identify COBIT confidentiality indicators

As noted in section 2.1 COBIT framework defines 34 processes in a generic process model within four domains. Each process is identified by a two-character domain reference (PO, AI, DS and ME) plus a process number. To assess these processes, this framework offers assessment indicators in 3 levels of IT managerial, process and activities figure 1 shows the indicators offered for PO1, the first process in plan and Organize domain.



Goals – IT:
- Respond to business requirements in alignment with the business strategy.
- Respond to governance requirements in line with board direction.

Goals – Process:
- Define how business requirements are translated in service offerings.
- Define the strategy to deliver service offerings.
- Contribute to the management of the portfolio of IT-enabled business investments.
- Establish clarity regarding the business impact of risks on IT objectives and resources.
- Provide transparency and understanding of IT costs, benefits, strategy, policies and service levels.

Goals – Activities:
- Engaging with business and senior management in aligning IT strategic planning with current and future business needs
- Understanding current IT capabilities
- Providing for a prioritisation scheme for the business objectives that quantifies the business requirements
- Translating IT strategic planning into tactical plans

Metrics – IT:
- Degree of approval of business owners of the IT strategic/tactical plans
- Degree of compliance with business and governance requirements
- Level of business satisfaction with the current state (number, scope, etc.) of the project and applications portfolio

Metrics – Process:
- Percent of IT objectives in the IT strategic plan that support the strategic business plan
- Percent of IT initiatives in the IT tactical plan that support the tactical business plans
- Percent of IT projects in the IT project portfolio that can be directly traced back to the IT tactical plans

Metrics – Activities:
- Delay between updates of business strategic/tactical plans and updates of IT strategic/tactical plans
- Percent of strategic/tactical IT plans meetings where business representatives have actively participated
- Delay between updates of IT strategic plan and updates of IT tactical plans
- Percent of tactical IT plans complying with the predefined structure/contents of those plans
- Percent of IT initiatives/projects championed by business owners

Figure 1: po1 indicators ITGI(2007)

According to COBIT classification each information criterion, such as integrity or confidentiality, is mapped to a number of processes based on its definition. This mapping is shown by way of P to indicate primary relationship and S to indicate secondary. For instance PO1 is mapped to effectiveness and efficiency information criteria in primary relationship. Figure 2 shows this mapping.

In this research, to identify the key indicators of confidentiality we study all the COBIT processes and their structure to extract the processes mapped to this information criterion. The extraction processes are shown in table 1.

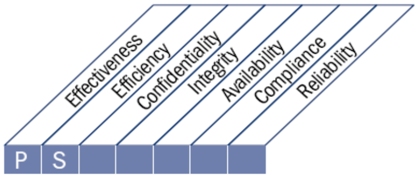


Figure2: po1 mapping to information criteria ITGI(2007)

Po2-S	Po9-p	DS1-S
DS2-S	DS5-P	DS12-P
ME1-S	ME2-S	ME4-S

Table1.The COBIT processes mapped to confidentiality information criterion

According to 9 extraction processes, we identify the defined indicators for each process. These indicators are basic indicators for EA plan assessment. Table 2 shows some of these basic indicators.

Rows	Indicators
1	• Frequency and review of the type of security events to be monitored
2	• Number and type of obsolete accounts
3	• Number of unauthorized IP addresses, ports and traffic types denied
4	• Percent of cryptographic keys compromised and revoked۳
5	• Percent of satisfaction of the information model users (e.g., is the data dictionary user-friendly?)
6	• Percent of redundant/duplicate data elements

7	• Percent of satisfaction of the information model users (e.g., is the data dictionary user-friendly?)

Table2. Some COBIT indicators mapped to confidentiality information criterion

3.2. Redefining confidentiality indicators

According to comprehensive characteristics of EA plan, the identified indicators should be overviewed based on EA dimension. To achieve this, we categorize the extraction indicators into 3 groups as follows:

- **Group 1**consists of the indicators don’t need to redefine.
- **Group 2** should be redefined to use.
- **Group 3** can’t be used in assessment

Based on this categorization, we use the basic indicators in group 1 without any change, redefine second group indicators and omit the third group. The output of this section is shown in table 3.

3.3. Determining the measurement method

In this section we determine the measurement method for finalized indicator (section 2). As shown in table 3, there are different types of indicators to measure. Some of them determine the absence or presence of a feature, plan or mechanism. In this case, the numeric system will be binary and the value is 0 or 1.The other type shows the percent of

rows	Indicators	Studied layer	Numeric system	Measurement method	Ideal situation
1	Existing the security logs mechanisms at the information systems level	infrastructure	binary	Check if exist	1
2	Existing the comprehensive security plan in EA plan	strategy	binary	Check if exist	1
3	Percent of data bases with the security logs mechanisms	infrastructure	binary	Counting the data bases which have the mechanism	1
4	Percent of servers with fire wall mechanism	infrastructure	decimal	Counting the servers which have the mechanism	The most
5	Percent of information systems with encryption tools	infrastructure	decimal	Counting the systems which have the mechanism	The most
6	Percent of information systems with authentication mechanism	infrastructure	decimal	Counting the systems which have the mechanism	The most
7	Existing a physical security plan and mechanism in EA plan	infrastructure	binary	Check if exist	1
8	Percent of information systems with intrusion detection tool	infrastructure	decimal	Counting the systems which have the mechanism	The most
9	Percent of data elements that are as the part of the enterprise data model	data	decimal	Check the ERD diagram	The most
10	Percent of applications are complying with the	application	decimal	Check the ERD diagram	The most

	information architecture				
11	existing a data model in EA plan	data	binary	Check if exist	1
12	Percent of redundant/duplicate data elements	data	decimal	Check the entities-information systems contrast matrix	The less
13	Percent of IT budget spent on risk management (assessment and mitigation) activities	IT management	decimal	Check the budget list	relative
14	Percent of identified IT events used in risk assessments	IT management	decimal	Check the risk management plan	The most
15	existing a risk analyze action plan for critical IT risks	IT management	binary	Check the risk management plan	1
16	Percent of critical IT objectives covered by risk assessment	IT management	decimal	Check the business-IT goal contrast matrix and risk management plan	The most

Table3: Confidentiality indicators and the measurement method

an object which have or not have a special characteristics, consequently the numeric system will be decimal and the value Varies from zero to one hundred. To propose the applicable method for EA assessment, we specify the related layers to study, the numeric system and ideal situation for each indicator

4. Results and Analysis

As the complexity of the modern large enterprises increases, new system engineering and architecture challenges emerge to help the stakeholders capturing the whole dimension and identifying the key aspects of the enterprise (Ludwig M& Farcet N, 2010). In fact the enterprise needs to identify its whole dimension in order to fulfill the missions and satisfy its objectives. In order to provide such support, enterprise architecture models should be amenable to analyses of various properties, as e.g. the level of enterprise confidentiality (Johnson P& Lagerstr¨om R, 2006). Although the importance of enterprise architecture has been recognized, hardly any attention has been paid to the analysis of their quantitative properties (Iacob M & Jonkers H , 2004). Also as one of the main goals of enterprise architecture is to establish IT governance, analyzing the EA plan in this view is too much important. In this research we propose a method to assess confidentiality information criterion in it governance view based on COBIT.

The benefit of this method is that it is based on one of the best IT service management frameworks provides good practices across a domain and process framework and also presents activities in a manageable and logical structure strongly focusing on IT assessment concept. Designing and defining of sufficient indicators in different view point increases the accuracy of assessment process. As mentioned these indicators are based on COBIT framework and the result of benchmarking various researches in EA assessment concept. More importantly, as we identify the measurement method, related layers and ideal situation for each indicator, their value doesn't only depend on assessment team's experience, but also it is relay on technical decisions. Consequently, the assessment's result is fair and more reliable.

References

Allen W (2011) Creating a Culture of Enterprise Cyber security, BatteauWayne State *University International Journal of Business Anthropology vol. 2*(2)

Edward W.N & Berrnroider,Milen Ivanov(2011) IT project management control and the Control Objectives for IT and related Technology (CobiT) framework,*Elsevier Journal of Project Management*, *, Pages 325–336*

Harryparshad N.(2011)Best Practices for Implementing Multiple Concurrent IT Frameworks (CMMI, ITIL, Six-Sigma, CobiT and Pmbok) *master design in business leadership,university of south africa*

Iacob M & Jonkers H (2004), Quantitative Analysis of Enterprise Architectures, *Telematica Instituut, P.O. Box 589, 7500 AN Enschede, the NetherlandsE-mail: {MariaEugenia.Iacob,* Henk.Jonkers}@telin.nl

IT Governance Institute (2007)CobiT 4.1, *IT Governance Institute, United States of America*,

Johnson P & Johansson E& Sommestad T & Ullberg J (2007), A Tool for Enterprise Architecture Analysis , *Department of Industrial Information and Control Systems*

Johnson P& Lagerstr¨om R& N¨arman P & Simonsson M ,(2006), Extended Influence Diagrams for Enterprise Architecture Analysis,*Royal Institute of Technology Stockholm, SwedenEmail:* {pj101, robertl, pern, martens}@ics.kth.se

Ludwig M& Farcet N (2010) , Evaluating Enterprise Architectures through Executable Models *Topics – Modeling and Simulation | C2 Architectures and Technologies THALES LAND & JOINT SYSTEMS Battlespace Transformation Center 160 Boulevard de Valmy 92704 Colombes CEDEX FRANCE +33(0)1 46 13 32 67 marie.ludwig@fr.thalesgroup*

Razavi Mahsa & Davoudi,Freidoon shams aliee,” (2009) A New Approach towards Enterprise ArchitectureAnalysis”,*International Conference on Enterprise Information Systems and` Web Technoligies(EISWT-09),Florida,USA,*

Shamsul S &Sharifi M & Masarat A (2008) Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations *IEEE*

Spafford G(2003)The Benefits of Standard IT Governance Frameworks *(www.itsmwatch.com/itil/article.php/2195051*

Tuttle, B. & Vandervelde, S.D.(2007)_. An empirical examination of CobiT as an internal control framework for information technology, *International Journal of Accounting Information Systems*, 8: 240-263.