2012 International Conference on Information and Network Technology (ICINT 2012)
IPCSIT vol. 37 (2012) © (2012) IACSIT Press, Singapore

A Novel Assessment Model for Managing Information Security Using COBIT

Usha Bala Varanasi, Sumit Gupta and Suvarna Kumar G [+]

MVGR College of Engineering, Dept of CSE, Vijayanagaram, Andhra Pradesh

Abstract. COBIT, Control Objectives for Information and related Technology. **Business continuity plan can be improved in an organization with the help of COBIT.** COBIT helps to mitigate risks and also judge when things go wrong. Big organizations that have complex, interdependent processes integrated in them faced lots of problems in transforming informal process into structured processes by establishing inter-departmental relationships to create a framework. Accordingly organizations adopted a structured manner such as frameworks or reference models like Cobit, Balanced Scorecard. This guarantees the completeness, accuracy, validity, authorization, segregation of duties within the organization along with the effectiveness of the organization. Cobit's analytical methods can be used to assess the organization quantitatively and for qualitative assessment we can utilize the Balanced Scorecard. In this paper we discuss the method of estimating organization's effectiveness and performance with Cobit and the implementation of Balanced Scorecard in an organization. And also focus on the advantages of Cobit and Balanced Scorecard that result in systems development, change management, business continuity, service level management, and security, computer operations that improve the ROI of that organization and promote the organization's profits with proper planning strategies of the Balanced Scorecard.

Keywords: information security, COBIT, information assurance, performance measurement, ISMS, quality management and assessment, balanced scorecard.

1. Introduction

Information Security and Management Systems (ISMS), is an approach that provides integrity, availability and confidentiality by reducing risks in an organization [1]. ISMS governs the information security effectively and deals with the security of both the information as well as the information asset. ISMS contain technical and organizational procedures that reach all levels of organization where the information can be managed. This ISMS is usually developed by the senior management that covers the whole management hierarchy and can be applied for a life cycle process. ISMS cannot be implemented to the policies outside the domain which is a major drawback. ISMS can be deployed by these seven steps that include organisational setup, asset identification, risk analysis, asset valuation, and selection of control set, operational testing and finalisation of the baseline control test [1, 2]. ISMS must refer to the standards and strategies to control information security system. It should meet the challenges outside the organizations by following security management measures such as risk management, actions, control and auditing actions.

COBIT is mainly used to identify the issues and setting up priorities for improvement in order to assess the control objectives in an organization. Cobit uses the maturity models to identify the performance of the enterprise, comparison of one organization with another, and as a path between 'as-is' and 'to-be' strategies. Cobit appeals to different users such as executive management, business management, IT management, Auditors [3].

[+] Corresponding author. Tel: + 0891-2561756.
E-mail address: kasibhattaushabala3@gmail.com.

Organizations' maturity levels can be measured by the guidelines, metrics and strategic planning of the Cobit framework. Organization's data gathering can be carried out by following a procedure that contains data gathering, analysis, research, brainstorming, documentation, refinement and presentation. The performance of the organization can be measured by using certain goals and metrics in three levels such as IT goals to measure business aspects, Process goals to measure the support to IT process and Activity goals to measure the requirements to carry out the process. Cobit can be implemented in any industry like small, medium and large organizations; for instance education, energy, financial services and government. It can be used to improve the information systems' efficiency either by improving the existing processes or by designing and implementing new processes that result in change management; which means that Cobit can be used to develop an IT policy framework when needed. Cobit is a logical structure that ensures the consensus of experts which focuses more on control than execution [3, 4]. Many versions of Cobit are available such as Cobit Quickstart can be implemented for small and medium enterprises, Cobit Online can be implemented for Internet users to customize their requirements. This framework maximizes benefits, minimises risks and serves as a link between the compliance and performance that can be carried out in different phases such as Plan and Organize, Acquire and Implement, Deliver and Support, Monitor and Evaluate, usually referred as high level control objectives[4].

Corporate Governance uses Cobit that addresses different management concerns relating to: limited IT knowledge to deliver business values, IT related concerns with priorities, IT risk factor management. Corporate Governance includes business process owners, managers, IT community, users and auditor (also known as evaluator) who conduct a study to generally accept the IT control processes. This study forms the basis for the Cobit in the organization. The actual study was done by ISACA, Information Systems Audit and Control Association which can be implemented by the professional auditors in an organization. Cobit can be used as an audit program development in an organization that needs substantial time to enhance the IT governance. It can also be used as IT governance framework with limited resources.

The Balanced Scorecard is a tool that permits on presenting the different areas of working of an organization in the shape, which gives exact information on the theme of observed object. It is simply a set of measures or ratios selected from different dimensions of effectiveness. Balanced Scorecard is mainly used to measure the effectiveness of an organization.

As a result we can say that Cobit and Balanced Scorecard are the best frameworks by which many organizations can be benefitted in achieving their goals.

2. COBIT

2.1. Objective

COBIT ensures the quality, fiduciary and security in an organization in order to balance requirements. COBIT is used for developing business continuity plan in an organization**.** COBIT can be used in an organization to link their enterprise-specific, operational and control requirements, policies and standards [5]. Due to the ever-changing technology and the usage of legacy systems without proper interactions between them the accustomed methods are unable to meet complex growth of industrial systems; thereby increasing the expenses of system failure. It ensures the integrity of information and also information system. It also links business goals to the IT goals. The main objective of this paper is to align the cobit framework with Balanced Scorecard in an organization. This merging is done mainly to overcome one of the disadvantages of Cobit which is "unable to predict (how) in the questionnaire". Cobit's implementation was to improve the efficiency of the information security services either by improving the existing process or designing and implementing new processes in order to achieve their goals [4, 6]. Cobit is a well-planned procedure that can be carried out in different phases. Cobit serves as a link between compliance and performance [7]. It is a top down approach that can be used to provide an assessment of the organization's current IT operations and to develop a strategy along with a plan.

- Data Sources: interviews, focus groups, documentations, observations
- Data Analysis: resources, financial and technological data
- Research Sources: COBIT, different vendors

- Development of plan and strategy

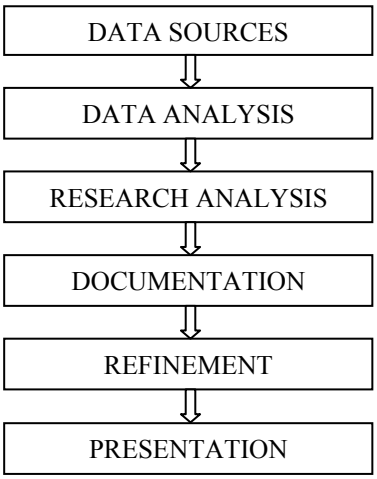

Fig. 1: Assessment of an organization

2.2. Approach of using COBIT

Cobit framework enables the organization to achieve the objective of growth thereby increasing business continuity. Cobit can be used as governance framework for IT which increases the success graph of the organization [8]. The main advantages of Cobit can be listed as forming strategies, developing audit plans, assessing and managing risks, managing application life cycle, policy formulation, outsourcing-catering opportunities for third parties and organization's security. The main metrics can be controlled are communication, quality, consistency, credibility and maturity.

3. Methodology

Cobit can be used to develop an IT policy framework from scratch which is more challenging for professional auditors. For instance, the organization should first acquire all the policies from IT and then it can be enhanced into a policy framework with the usage of Cobit [5, 9]. This new policy framework can control some areas like system security, configuration, data, operations and risks. These policy frameworks should prepare a questionnaire for which all the audit teams provide answers. Basing on these answers some constraints that are appropriate are redirected back to the original objectives. This establishes a link between control objectives and policy framework, which can be called as a policy. These policies can be verified by using risk control matrix based on "what? And why?" (Brainstorming) type of questions [10]. This enables to find gaps if any. These gaps can be filled by modifying the policies and can be made available to the public and the whole organization. The main use of this policy is to disclose the interested parties about a solution. This policy is a statement that supports business objectives.

This combined study can be used to analyze a comprehensive approach of an organization as follows:

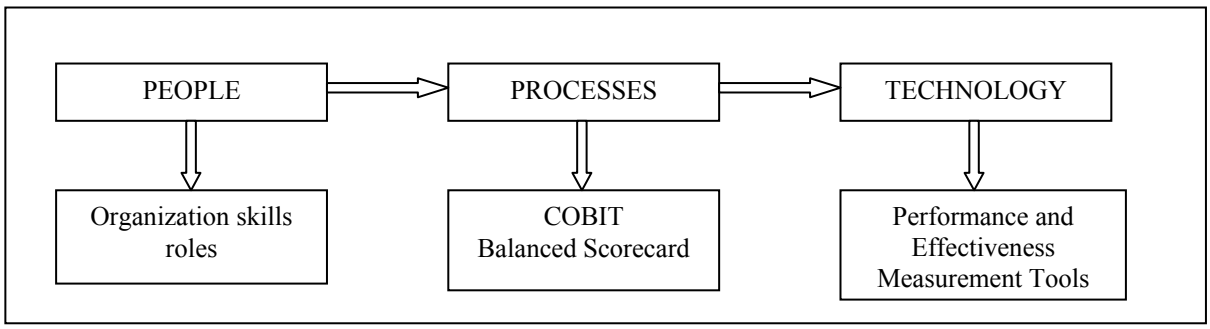

Fig. 2: Comprehensive approach for the summary of IT maturity

4. Balanced Scorecard

Balanced Scorecard is defined by Norton and Kaplan. Balanced Scorecard is an approach that is used to measure the effectiveness of an organization [11]. Effectiveness of an organization can be defined as an ability of a strategy in achieving planned aims. This effectiveness can be depicted using some dimensions such has financial, market, operational and development [12]. Balanced Scorecard converts traditional methods into defined initiatives or actions.

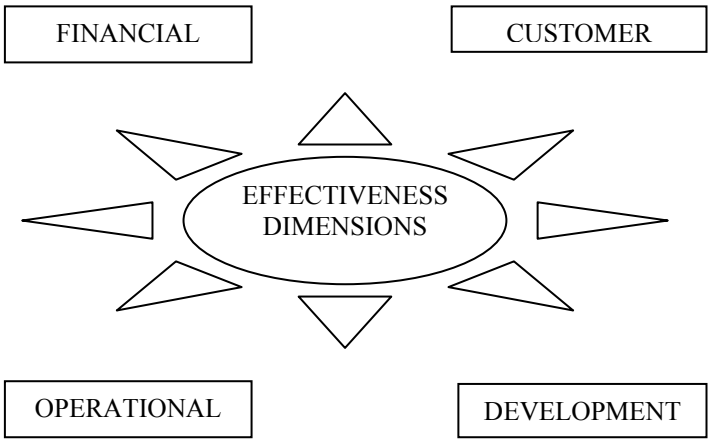

Fig. 3: Dimensions of effectiveness:

Balanced Scorecard is a major accomplishment of management in accounting to carry out performance evaluation judgement. It is a performance measurement tool that translates business goals into performance measures. Its main aim is to measure success against the strategy which is specially designed for the senior executives in an organization. Balanced Scorecard is simply a set of ratios selected from different dimensions of effectiveness. It is a tool that permits the different areas of working of an organization in the shape, which gives the exact information on the theme of the observed object [12].

Balanced Scorecard can be applied to IT which uses 3 layers that consist of mission, strategy and metrics.

- Mission: development opportunities for future needs
- Strategy: obtain control over objectives
- Metrics: development and implementation of IT metrics based on critical success factors

The Balanced Scorecard can be mainly used for construction of a strategy and its usage within the organization. This Balanced Scorecard can also be used for monitoring the strategy's implementation and its process of verification [10, 12]. It translates the strategies to all the teams, cells, individual workers of the organization. Balanced Scorecard analyzes the effect of the relationships among the processes within the organization. It anticipates the future based on the past references.

Balanced Scorecard is a base of the management system. It provides full information in relation to present and future state of the organization.

Our main idea is to merge Cobit with Balanced Scorecard to overcome one of the main disadvantages of the Balanced Scorecard which is careful selection of initiatives or actions by the executives.

5. Analysis

This model can be analyzed to align business strategies with IT strategies [1, 3, and 5]. Of all the domains of the COBIT framework, Deliver and Support (D&S) and Acquire and Implement (A&I) are the domains with the highest levels of importance and are treated as the basis for this combined framework. Cobit and Balanced Scorecard frameworks can be combined and can be depicted as follows:

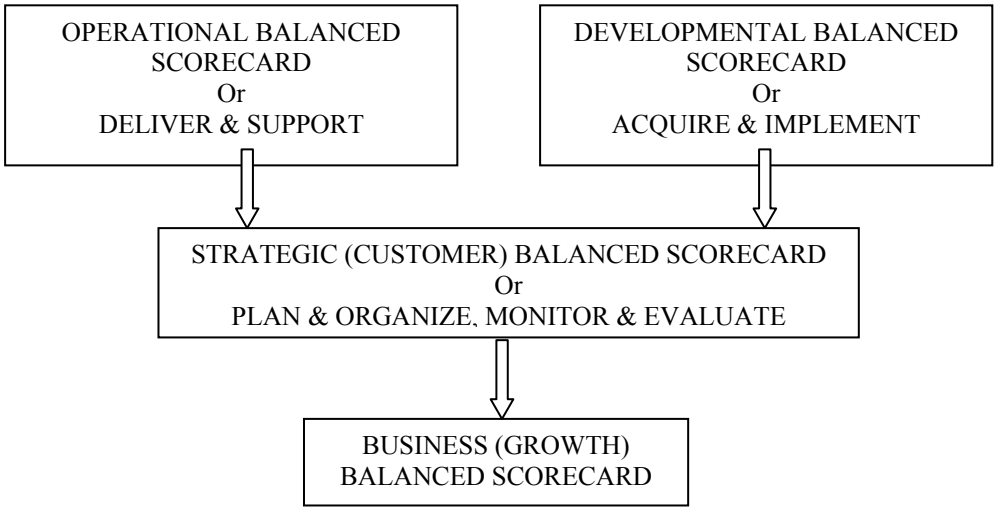

Fig. 4: Combined framework based on Balanced Scorecard and COBIT:

6. Conclusion

Measurement of performance and effectiveness of the organization are mainly concentrated which is a very important aspect of the information systems' assessment [1, 3]. This merging up of Cobit and Balanced Scorecard frameworks might result in dealing with (how) approach in Cobit as well as in choosing the best initiatives by the executives in Balanced Scorecard.

In this comprehensive approach Cobit is used to evaluate the current state of the organization and Balanced Scorecard is used to define the planning strategy. By merging of these two frameworks an organization's maturity levels can be assessed [3]. This process can be implemented to improve business continuity, reduce risks that tend to improve organizational behavior, and improve the system performance, organization's efficiency and effectiveness, security that results in improving the ROI of that organization.

7. References

[1] ISMS –Carnegie Mellon Copyright, Carnegie Mellon University, 2005-2011.

[2] ISMS- Knowing What to Secure-

[3] COBIT FOCUS, IT Organization Assessment- volume 1, January 2011.

[4] COBIT FOCUS, (Case study) Using COBIT Best Practices for developing BCP for an outsourcing company, by A Rafeq, CISA, CGEIT, CIA, FCA-Volume 2, April 2010.

[5] COBIT & its Utilization: A framework from the literature- Gail Ridley, Judy Young, Peter Carroll.

[6] Quantifying Criticality of Dependability- Related IT Organization Processes in Cobit- Tobias Goldschmidt, Adreas Dittrich and Miroslaw Malek.

[7] COBIT 4.1 Excerpt, IT Governance Institute.

[8] COBIT 4.1 Framework, IT Governance Institute.

[9] COBIT_STUDENT_BOOK, IT Governance Institute.

[10] IT Governance based on COBIT 4.1, A Management Guide, ISTM Library.

[11] R.Kaplan, D.Norton, The Balanced Scorecard, PWN, Warsaw 2001.

[12] K.Cholewicka-Gozdzik, The Balanced Scorecard- Tool of estimation the organization's effectiveness, Quality Problems, No 2 (2002) 6.