ISSN 2349-4506
Impact Factor: 2.785

Global Journal of Engineering Science and Research Management

MANAGEMENT OF INFORMATION SECURITY FROM DEVELOPMENT STAGE BY APPLYING COBIT GUIDELINES

Ashish Ukidve*, Ds S S Mantha, Milind Tadvalkar
* Principal, Vidyalankar Polytechnic, Mumbai, India
Ex-Chairman, AICTE,Professor, VJTI, Mumbai India
Director, Vidyalankar Dnyanapeeth Trust, Mumbai, India

DOI: 10.5281/zenodo.225177

KEYWORDS: The COBIT Framework COBIT domains, IT governance and information systems development,

ABSTRACT

COBIT is a collection of good processes and practices for IT governance. It offers the effective measures, indicators and activities for enterprise. COBIT has also been applied to many other governance, e.g. security governance, software process IT services management. Since COBIT is general-purpose, it requires expert knowledge for the implementation of each application. Although the guideline of security management are also published, we examined the contents of COBIT and defined a framework which specializes in information security engineering from the guideline. This paper presents the framework along with its application in development of information systems t. The framework effectively utilizes the COBIT-based security management and solves various subjects of security in the development.

INTRODUCTION

In business, information technology is an important success factor to drive customer's value for enterprises. Then the enterprises must understand the associated risks, such as increase in the regulatory compliance and critical dependence of many business processes on IT. Therefore, enterprises have to manage and optimize their all information assets i.e IT governance has become responsibility for enterprises.

However, it is difficult to get IT under control such that it deals with information a large organization needs. To solve this problem, the Information Systems Audit and Control Association (ISACA) and IT Governance Institute (ITGI) have proposed Control Objectives for Information and related Technology (COBIT). COBIT is a frame-work which provides processes, measures, indicators and best practices to maximize the benefits derived through IT utilization [7]. It enables clear policy development and good practice for IT governance through organizations.

COBIT can be widely applied to various purposes. ISACA and ITGI have clearly defined the mapping of COBIT against the other related standards, e.g., ISO/IEC 27002, ITIL (Information Technology Infrastructure Library), PMBOK (Project Management Body of Knowledge), and CMM (Capability Maturity Model). Moreover, they have provided the guideline of a COBIT application which is specialized in information security and governance. COBIT covers security in addition to all the other risks that can occur with the usage of IT.

It is important to understand that thorough knowledge and experience is required to utilize COBIT. In addition, the original purpose of COBIT is management through all the processes of IT introduction to business for the whole of an organization. Thus it is difficult to implement COBIT at each process (e.g., information systems development), because its applications are too wide. Even the contents of the above COBIT security baseline need to be understood thoroughly.

Therefore, we have carefully researched COBIT and proposed its effective utilization. Our major focus has been on the most important and difficult subject, i.e., management of security of information systems during development. In this paper, we improve the COBIT-based security baseline and provide a new draft framework which can support a project of information systems development in security management. The framework brings out the potential of COBIT and its effective application to the security management during development.

ISSN 2349-4506
Impact Factor: 2.785

Global Journal of Engineering Science and Research Management

THE COBIT FRAMEWORK

We herein show the structure and components of COBIT.

Table 1. The input/output of the process PO1

From	Inputs	Outputs	To
PO5	Cost-benefits reports	Strategic IT plan	PO2..PO6, PO8, PO9, AI1, DS1
PO9	Risk assessment	Tactical IT plans	PO2..PO6, PO9, AI1, DS1
PO10	Updated IT project portfolio	IT project portfolio	PO5, PO6, PO10, AI6
DS1	New/updated service requirement	IT service portfolio	PO5, PO6, PO9, DS1
...	...	...	...

COBIT domains

COBIT comprises of four domains referring to the management cycle [2].. Figure 1 shows the domains and the process flow having each domain name; PO (plan and organize), AI (acquire and implement), DS (deliver and support) and ME (monitor and evaluate).

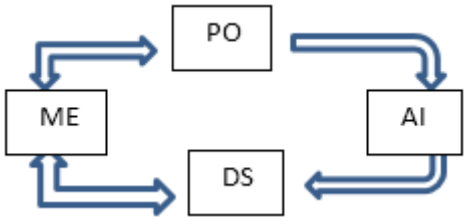

Figure 1. The management cycle and the COBIT domains

Each domain consists of many processes which define required activities for IT governance (Figure 2). PO comprises of 10, AI has 7, DS has 13 & ME has 4 processes

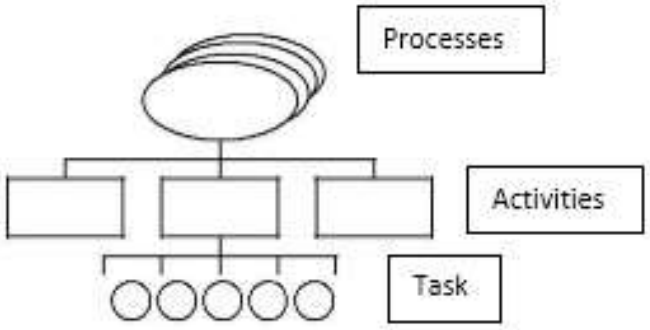

Figure 2. The hierarchical structure of COBIT

Moreover, one process is linked to the others via in-put/output relationship. The processes also provide control objectives and clearly define required activities and their responsible position of the organization in the process. Figure 3 shows the structure of PO and Table 1 shows of one of the processes in the domain in terms of input/output. The following is the process PO1 which describes "Define a Strategic IT Plan." PO1 has the six objectives from PO1.1 to PO1.6. PO1 also mentions that CIO and business executives have the responsibility of the first activity. Each process shows the responsibility of each activity in a table.

ISSN 2349-4506
Impact Factor: 2.785

Global Journal of Engineering Science and Research Management

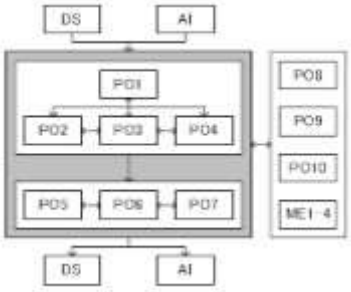

Figure 3. The structure of the domain PO.

PO-1 Define a Strategic IT Plan
IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities.

PO-1.1 Value Management of IT
Work with the business to ensure that the enterprise port-folio of IT-enabled investments contains programmes that have solid business cases.

Activities
1) Relate business goals to IT goals.
2) Identify critical dependencies and current performance.
3) Build an IT strategic plan.
4) Build IT implementation plans.
5) Analyze portfolios and manage project and service portfolios

The COBIT-based security management
ISACA and ITGI have published the document aligning COBIT and ISO/IEC 17799, which establishes guidelines or initiating, implementing, maintaining, and updating information security management in an organization [4]. The mapping describes the correspondence of the COBIT processes and the components of ISO/IEC 17799 [6]. After ISO/IEC 17799 was updated to ISO/IEC 27002 [5], the new mapping was published. These documents show the mapping of COBIT control objectives in tables (Table 2) with ISO/IEC 27002.

The security baseline [8] includes this mapping and offers a set of COBIT control objectives and activities required in security governance. The baseline defines security governance as "a subset of IT governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisation resources responsibly, and monitors the enterprise security programme." The baseline has 44 steps which are customized from the activities of COBIT for security governance.

Given below is an example, of the original description of DS11 -
DS11 Manage Data
To identifying data requirements.

DS11.1 Business Requirements for Data Management
Validate that all data expected for processing are received and processed completely, accurately and all output is delivered as per business requirements. Support restart and reprocessing activities.

Activities
1. Define data backup and retention requirements into procedures.
2. Define, maintain and implement procedures to manage the media library.
3. Define, maintain and implement procedures for secure disposal of media and equipment.
4. Back up data according to scheme.
5. Define, maintain and implement procedures for data restoration.

DS11 of the baseline describes "Ensure that all data remain complete, accurate and valid during entire processes." The activities are also modified as follows.

1) Subject data to a various controls to check for integrity during input, processing, storage and distribution. Ensure transaction authenticity and that they cannot be repudiated.
2) Distribute sensitive output only to authorized individuals.
3) Define requirement of archival, storage for input and output documents, data, and software. Ensure that they comply with user and legal requirements.
4) While in storage, check continuing integrity, accessibility and readability of the data.

Table 2. The mapping of the COBIT control objectives and the ISO/IEC 27002 components

COBIT control objective	ISO/IEC 27002 component
PO3.1 Technological direction planning	5.1.2 Review of the information security policy 14.1.1 Including information security in the process of business continuity management 14.1.5 Testing, maintaining and reassessing business continuity plans
PO3.2 Technology	–
infrastructure plan	
PO3.3 Monitor future	6.1.1 Commitment of Management to information
trends and regulations	security

Also, the baseline simplifies the original processes of the COBIT domains; DS in the baseline has only 6 out of the 13 original processes. Thus it is specialized for security governance.

However, the oversimplification makes strict security assurance difficult, since the baseline lacks some important processes. COBIT covers the whole of IT introduction to business but it provides less consideration to the information systems development process, which is an important part. It is necessary to carefully reconsider the set of the processes and activities.

APPLYING COBIT TO SECURITY MANAGEMENT IN INFORMATION SYSTEMS DEVELOPMENT STAGE

IT governance and information systems development

First we distinguish between IT governance, security governance and security management in Information systems development.

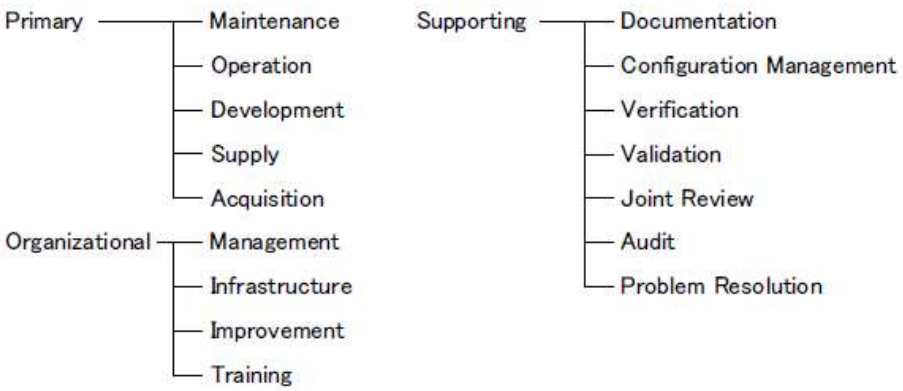

Figure 5. The classification of the lifecycle processes in ISO/IEC 12207 standard.

According to the above definition of security governance, IT governance includes it. IT governance widely deals with the whole of IT utilization on business, from business strategy planning to user education. Thus the development is merely a part of the activities of IT utilization. In COBIT, it corresponds to a part of the PO and AI domains. For example, requirements analysis is included in AI1 (Identify Automated Solutions) and design is included in AI2 (Acquire and Maintain Application Soft-ware). The security baseline partly includes such processes. This relationship is shown in Figure 4.

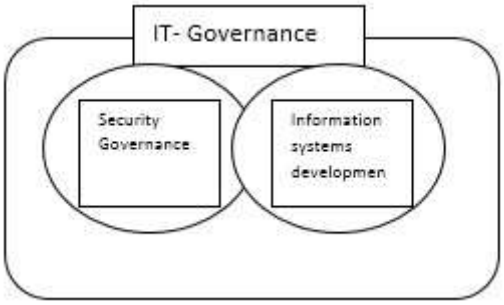

Fig 4. The relationship of IT governance and information systems development.

Partial application of COBIT security baseline is not sufficient for strict security assurance. Therefore, we propose a contrivance which can make up for the deficiency.

System development life cycle

To apply the COBIT-based security baseline to information systems development, we have first found the baseline's insufficiencies. As mentioned above, the baseline lacks the viewpoint of the development. Thus we have to clarify lack of activities for the development process.

There are some definitions of the systems development lifecycle [11]. ISO/IEC 12207 defines activities required in the development in the same way as COBIT. ISO/IEC 12207 classifies the activities under three categories (Figure 5). It also has the hierarchical structure like COBIT (Figure 6) and assigns a accountable role to each process. Each task has inputs and outputs, an activity is a detailed set of tasks, and a process is a set of interrelated activities, which transform inputs into outputs. These just correspond to the activities, processes and domains in COBIT (Figure 2). We build the new framework using this resemblance.

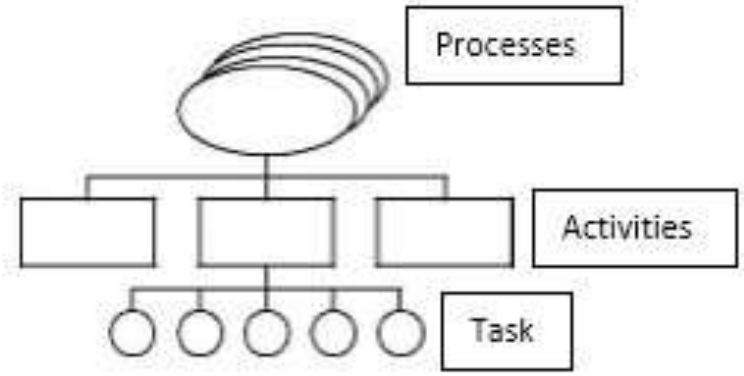

Fig 6. The hierarchical structure of ISO/IEC 12207.

Process definition

Secondly, we have found the correspondence of COBIT processes and ISO/IEC 12207 processes, thereby the security baseline's insufficiencies have been solved. The new framework consists of the activities in the security baseline and the additional activities in the original COBIT corresponding to ISO/IEC 12207.

Table 3. The role correspondence of the security engineering environment, ISO/IEC 12207 and COBIT

Security engineering environment	ISO/IEC 12207	COBIT
Designer	Acquirer, Supplier	Chief architect
Developer	Developer	Head development
User	Operator, User	Business process owner, Head operations
Maintainer	Maintainer, Employer of Supporting Processes	Compliance, Audit, Risk and Security
Administrator	Manager	CEO, CFO, CIO, Business executive, Head IT administration, PMO

With the correspondence, we must also change the CO-BIT processes for security management in information systems development. The guideline of such conversion for some processes is shown in the COBIT-based security base-line, e.g., PO1 'Define a Strategic IT Plan' is converted into 'Define the Security Strategy.' Except these processes, the target of the activities is corrected according to the tasks of ISO/IEC 12207. For instance, the first activity of PO10 (Manage Projects) may be corrected as follows -

"Define a security programme/portfolio management framework for information systems IT investments."

Role definition

COBIT defines the roles categorized for all processes as:

- Chief executive officer (CEO)
- Chief information officer (CIO)
- Chief financial officer (CFO)
- Business executives
- Business process owner
- Head operations
- Chief architect
- Head development
- Head IT administration (for large enterprises, the head of functions such as budgeting, human resources and internal control)
- The project management officer (PMO) or function
- Compliance, audit, risk and security (groups with control responsibilities but not operational IT responsibilities)

Similarly, ISO/IEC 12207 defines the following roles: Acquirer, Supplier, Manager, Operator, User, Developer, Maintainer and Employer of Supporting Processes. On the other hand, the security engineering environment including roles and processes is clearly defined in order to provide designers, developers, users, and maintainers with standard and consistent supports for design, development, implementation, operation, and maintenance of information systems with high security requirements [1]. Thus we defined Table 3 according to the resemblance of the processes. If the responsible role in each COBIT activity is replaced by Table 3, the activity can certainly change to an activity of the security management.

CONCLUSIONS

In this paper, we have applied the COBIT framework for IT governance to security management in information systems development. We have defined roles and activities in the security management as a framework by contrasting the COBIT-based security baseline, ISO/IEC 12207 and ISO/IEC 27002. Although our framework reduces the scope of COBIT from IT governance to security management in information systems development, it can effectively utilize processes, control objectives and activities defined in CO-BIT. Additionally, we have already defined components for documentation of information systems development based on ISO/IEC 12207 [10]. The components will be helpful for the activities of security management in our framework.

In the future, we must apply the framework to practical subjects and evaluate it. We are working on a complete documentation of our framework.

REFERENCES

1. Cheng, J., Goto, Y., Morimoto, S. and Horie, D., "A Security Engineering Environment Based on ISO/IEC Standards: Providing Standard, Formal, and Con-sistent Supports for Design, Development, Opera-tion, and Maintenance of Secure Information Sys-tems," Proceedings of the 2nd International Confer-ence on Information Security and Assurance, pp. 350-354, IEEE-CS, 2008.
2. B. Hopstaken and A. Kranendonk, Informatieplan-ning; puzzelen met beleid en plan, Kluwer, Deventer, 1991.
3. ISO/IEC 17799: 2005, Information Technology – Se-curity Techniques – Code of Practice for Information Security Management, 2005.
4. ISO/IEC 27002: 2005: Information Technology – Se-curity Techniques – Code of Practice for Information Security Management, 2005.
5. IT Governance Institute, Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit, 2008.
6. IT Governance Institute, COBIT 4.1, 2007.
7. IT Governance Institute, COBIT Security Baseline: An Information Survival Kit, 2nd Edition, 2007.
8. Morimoto, S., "Documentation Components of Soft-ware Development and their Management Based on International Standards," Proceeding of the 10th In-ternational Workshop on Learning Software Organi-zations (LSO 2008), 2008.
9. U.S. House of Representatives, Systems Development Life-Cycle Policy, 1999.