CSCanada
Management Science and Engineering
Vol. 8, No. 3, 2014, pp. 11-16
DOI: 10.3968/5520

ISSN 1913-0341 [Print]
ISSN 1913-035X [Online]
www.cscanada.net
www.cscanada.org

Research on Building Baseline of IT Risk Control and Its Application in IT Risks Management

YANG Feng[a],*

[a]Ph. D., Associate Professor, Key Laboratory of Technology and Security on Electronic Commerce, School of Information, Guizhou University of Finance and Economics, Guiyang, China.
*Corresponding author.

Received 12 June 2014; accepted 26 August 2014
Published online 15 September 2014

Abstract
Based on ERM of COSO and IT life-cycle theory, this paper analyzed enterprise's IT risk management needs and its environment, provided the definition of baseline IT risk control, proposed the framework and models of constructing IT risk control baseline in enterprises, and finally discussed its elements and construction methods of IT risk control baseline. Applying the baseline model of IT risk control into IT risk management works of enterprises, it will be a powerful tool and means for the enterprise IT risk management.

Key words: IT risk management; Baseline of IT risk control; Risk environment; Risk control

Yang, F. (2014). Research on Building Baseline of IT Risk Control and Its Application in IT Risks Management. *Management Science and Engineering*, *8*(3), 11-16. Available from: URL: http://www.cscanada.net/index.php/mse/article/view/5520
DOI: http://dx.doi.org/10.3968/5520

INTRODUCTION
Science and technology make humans face great risks when they bring progress and prosperity to human civilization. Information technology works in this way as well. With the application of information technology or information system in enterprises, the operation of daily business suffers great uncertainty and insecurity when the enterprises are enjoying the revolution and a sharp increase in productivity brought by information technology. It can be said like this: With the further development and application of information technology in varied fields, information security has become a strategic problem that enterprises, governments at all levels and even the whole world are confronted with currently. It has become an important part of national comprehensive security.

Based on ERM of COSO and IT life-cycle theory, this paper analyzed enterprise's IT risk management needs and its environment, provided the definition of baseline IT risk control, proposed the framework and models of constructing IT risk control baseline in enterprises, and finally discussed its elements and construction methods of IT risk control baseline. The baseline model of IT risk control was applied into IT risk management of enterprises. Through the management of IT risk control baseline, the management of organizational IT risk can be realized, and its process and difficulty level can be simplified and regulated with the expectation of improving IT risk management efficiency. It is expected that a consistent, comparable and reproducible evaluation result of IT risk and its valid control is constructed. And this evaluation result is made as a powerful tool, which is used to enhance the stability of IT system in enterprises and reduce various threats and risks to it.

1. REVIEW OF LITERATURES AND THEORETICAL RESEARCHES
This section reviews some researches and applications of baseline in software engineering, information security, information security risk and other fields.

Ma (2005) summarizes the characteristics of modern science and technology risk; Yang (2010) proposes that information and technology risk of commercial bank is difficult to measure, easy to spread and rather influential compared with other risks.

As to the risks brought by new technology, i.e., technology risks, the famous scholar Starr (1965) in

Psychological risk area present a well-known question "How safe is safe enough". He uses Risk-Benefit Analysis to calculate risk value. (Starr, 1969)

Liu (2000) thinks that the information system security baseline is the minimum guarantee of information system, or in other words, the basic security requirement of this information system. Information security system has to make a balance between the security cost and the security risks it can stand. Thus, security baseline is the reasonable dividing line of this balance. Li and Wang (2009) propose that security baseline is the basic requirement of security. They design a security baseline model aiming at business system with American FISMA as references. Sang (2007) studies the protection of telecommunication system security from perspectives of security baseline and hierarchy protection. Lü (2006) proposes security classification management and fundamental baseline strategy of e-government system; she also defines FBL (IA Fundamental Baseline) and EBL (IA Enhanced Baseline). In order to deal with network security problems of communication network in fundamental management, Ma (2011) proposes to formulate communication network security baseline of operation business, which is then combined with business and application carried by network elements. They together enhance the operation condition of communication network.

From the previous literature review and research findings, it can be seen that the baseline concept and technology are mainly used in the process management of software development, especially software configuration management process as well as the application of information security management.

Based on the previous research findings of others, this thesis applies the baseline concept and technology in IT risk management process. Based on ERM of COSO and IT life-cycle theory, the process of IT risk management is regulated and simplified. The thesis aims at realizing the management of organizational IT risk through the management of IT risk control baseline. The assessment of IT risk control baseline can facilitate the assessment of IT risk, that is to say, the purpose of constructing IT risk control baseline and assessing IT risk control baseline is to establish a minimum strategy set and workload, which are used to satisfy the basic requirements of organizational risk management, i.e., the minimum standards and references of IT risk management.

2. BASELINE AND IT RISK CONTROL BASELINE

2.1 The Connotation and Basic Attributes of Baseline

Baseline can be defined as a standard measurement or fact against which other measurements or facts are compared. Its concept and technology are widely used in Surveying and mapping, Geodesy, Marine engineering, Aviation science[1], Biology, Medical science, Botany, Pesticide science, Software engineering, Information security and other fields.

Baseline is a normal term in software engineering. It is often encountered in software configuration management, IT project management, rational unified process (RUP), Microsoft Solution Framework (MSF), and there are some derived terms, such as, baseline promotion, baseline tendency, baseline audit, etc.. To be specific, baseline is the work auditing and results at certain stage in software project development process. It is a label or snapshot of work pieces or phased achievements at certain time in the storage reservoir. Baseline is also a data set which is data static inspection when the snapshot is established. It is a stable version of software document, source code as well as software development configuration, preserving the software development findings at the current stage. It provides a formal standard or reference which the development of software projects is based on, enhancing the development and management of software projects.

Snapshot is defined by SNIA as[2]: a completely available copy in certain data set. It includes the mapping of corresponding data at specific point of time. It can be a duplicate of the data it implies, or even a replicate.

Snapshot technology has a very wide range of applications, such as, as a backup source or data mining source, as a checkpoint of preserving application programs, or even as a method of replicating data (Liu, 2009, August 5).

In software project development management, the construction and application of baseline have to combine three main factors: reproducibility, traceability and report.

Reproducibility refers to the ability to return in time and re-generate the version given by the software development system; or the ability to re-generate the development environment at early stage in the project development process.

Traceability refers to establish the inheritance relationships between work pieces of software development projects. The purpose is to ensure the following factors: demand analysis, systematic planning, design of system outline and detailed planning, can satisfy the requirements of projects development, implementation of project code, system up line, systematic implementation, system maintenance and other work.

Report is used to compare the content of different baselines. Baseline comparison can benefit debugging and then generate instructions.

In the process of software development, the significance of baseline is to catalog work for different

[1] Baidupedia. Baseline. Retrieved 2011, August 5 from http://baike.baidu.com/view/350200.htm
[2] Baidupedia. Snapshot. Retrieved 2011, August 5 from http://baike.baidu.com/view/677611.htm

stages explicitly. The continuous work is classified into different stages at these points, and the present work can be reviewed and confirmed, which can guide the future work.

Using baseline as basis and tool to manage the software development process is a fundamental method of software engineering management, and meanwhile an efficient method in practical work. The baseline efficient management can greatly facilitate software development and contribute a lot to the success of software development projects.

The systematic baseline management of the software development process can guarantee continuity, consistency and verifiability of output at different stages. Software versions can be controlled by controlling the versions of baseline; the alternation of software development can be controlled by controlling the alternation of baseline; and the management of software development can be realized through baseline management (Lu, 2011), with the promotion of software development quality and the in-time completion of software products as expectations.

At the stage of software project development, the baseline can be set as development baseline, testing baseline and issuance baseline according to the time sequence of project development. Thus, the efficient and orderly work at development stage can be guaranteed. Development baseline refers to project-level baseline established by the project development team in development process. It is mainly used in demand analysis, software planning, software design, code compiling, etc.. Testing baseline is established by the project development team with the purpose of testing various software products. Issuance baseline is promulgated by the project development team. It is corresponding to the verified configuration set of software products at each stage, and it is reference baseline of the subsequent development stage. Another concept is still held by some others: Issuance baseline is established after the testing work of testing personnel. It is an achievements set of software products which includes *Readme.text, User Manual, User Instructions, Installation and Configuration Manual of Software Products, Quality Report of Software Products,* and installation package of products, etc..

2.2 IT Risk Control Baseline and IT Risk Control Baseline Management

IT risk control baseline refers to the bottom line of risk control ability of an enterprise in IT application activity. IT system has to satisfy the basic requirements of enterprise information security and IT risk management. IT risk control baseline is the fundamental ability requirement, and it is the lowest requirement for enterprises to control their practical risks.

In *The Information Technology Management Guidance of Commercial Bank*, information technology risk is defined by China Bank Regulatory Commission as the operation, law and reputation risks resulted by natural and human factors, technique leak and management defect when information technology is applied in commercial bank operation process[3], in other words, the possibility of IT system risks and the negative impacts on enterprises.

The smooth and safe operation of IT system has to make a balance between risk cost and the risk it can stand. The IT risk management and control baseline are just the critical line of this dynamic balance.

IT risk management not only focuses on IT technology risk, IT investment risk, IT project risk, but also focuses on IT operation risk, IT management risk, etc,. Thus, IT risk control management can be divided into IT technology control baseline, IT investment risk control baseline, IT project risk control baseline, IT operation risk control baseline and IT management risk control baseline.

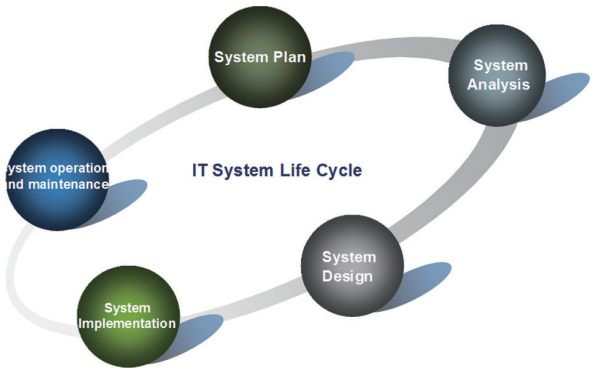

Figure 1
IT System Life Cycle

IT projects have the characteristics of high technological content, long cycle, numerous departments, uncertainty, etc.. Thus, the IT projects which are divided into several stages can facilitate risk management (Wang, Zhang, Lu, & Chen, 2005). According to the life cycle theory, IT system has to pass through project establishment, development, operation. With the alternation of its environment, maintenance and modification are necessary. And it will be substituted by the new system if it is not qualified (Lu, 2011). IT system includes five stages: IT system plan, IT system analysis, IT system implementation, IT system operation and maintenance (Figure 1). Therefore, in IT system life cycle, with the further development of IT system projects, a series of IT risk management control baselines can be constructed from IT risk management angle. Such as, IT system plan risk control baseline, IT system analysis control baseline, IT system design risk control baseline, IT system implementation control baseline and IT operation and maintenance risk control baseline (see Figure 2).

[3] China Banking Regulatory Commission. (2009, June 1). Guidelines on the Risk Management of Commercial Banks' Information Technology. Retrieved 2011, August 5 from http://www.cbrc.gov.cn/chinese/home/jsp/docView.jsp?docID=20090601FC296F80D3957B65FFFA9EDA836D7300

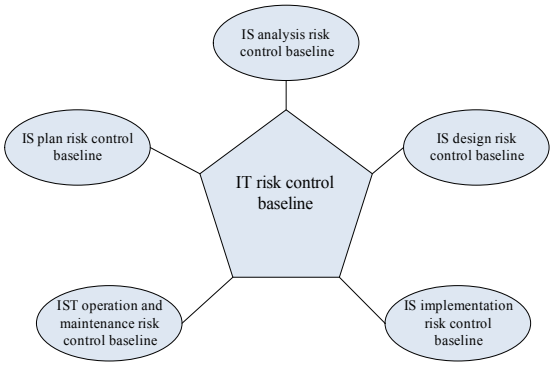

Figure 2
IT Risk Control Baseline Based on IT System Life Cycle Theory

Different organizations and enterprises have different criterion upon the categorizations of IT risks. Thus, the classification of IT risk control baseline has many different manifestations according to some disciplines, which are beneficial to the IT risk management of enterprises and organizations.

The significance of constructing IT risk control baseline is that it aims to regulate and standardize the process of IT risk management and control. Through the analysis of IT system risk management environment and its needs, constructing IT risk control baseline in enterprises can satisfy the lowest requirements of IT risk management. Through the management of IT risk control baseline, the management and supervision of IT risk process can be realized; the process and difficulty can be simplified and regulated. Meanwhile, the performance of an enterprise's IT risk management can be enhanced, getting a consistent, comparable and repeatable IT risk evaluation result. The evaluation result will be a powerful tool to manage IT risks in enterprises, which can improve the stable operation of IT system and reduce the possibilities of suffering various risks.

Then, how to design an IT risk control baseline model which can both suitable for the environment and satisfy the development requirements?

Based on ERM integrated framework, in the following part this paper analyzes the construction model of IT risk control baseline of IT system operation and maintenance stage.

3. CONSTRUCTION MODEL OF IT RISK CONTROL BASELINE BASED ON ERM INTEGRATED FRAMEWORK.

3.1 The Theme and Core Significance of COSO's ERM

COSO is *The Committee of Sponsoring Organizations of The National Commission of Fraudulent Financial Reporting,* or *Committee of Sponsoring Organizations of the Treadway Commission.* In September 2004, based on *Internal Control——Integrated Framework* published by COSO and the requirements about reports in *Sarbanes-Oxley Act,* the researching findings about risk management were included at the same time, the *Enterprise Risk Management – Integrated Framework* was promulgated (see Figure 3). The aim of it is to offer a comprehensive application guideline upon a unified system of term and concept for all the enterprises worldwide[4].

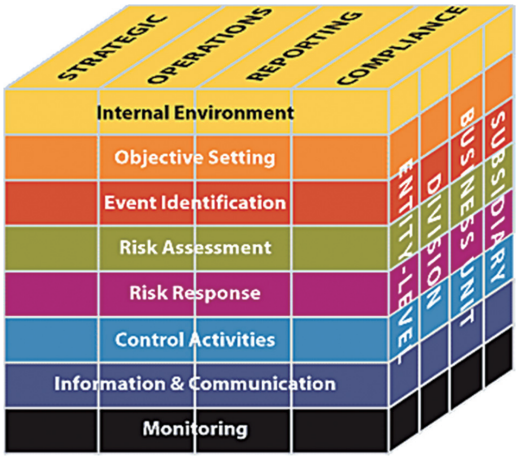

Figure 3
Risk Management Framework of Enterprises—The Components of COSO

The framework consists of 8 factors: internal environment, objective setting, events identification, risk assessment, risk response, control activities, information communication and monitoring.

The framework has 4 targets: strategic target, operation target, report target and regulated target.

The definition of "risk" given by ERM integrated framework of COSO: Risk refers to the possibility of negative effects an event will bring the target realization." This definition stresses the negative effects of risks, while expresses the positive effects of events with "opportunities".

The definition of "enterprises risk management" given by ERM integrated framework of COSO: Enterprises risk management is a process which is exerted by the board of directors, management level and other personnel. It is applied in strategy formulating and it runs through the enterprise, aiming to recognize the potential events that may influence the subject, manage risks and make it within the risk capacity and guarantee the realization of subject's target. (Fang & Wang, 2008)

3.2 The Construction of IT Risk Control Baseline Based on ERM Integrated Framework of COSO

Based on the definitions of risk and risk management given by ERM integrated framework of COSO, the eight

[4] Baidupedia COSO. Retrieved 2011, August 6 from http://baike.baidu.com/view/1050747.htm

factors of enterprises risk management process, as well as the features of IT risk management field, the thesis gives IT risk control baseline model and operable methods and steps for enterprises.

The construction of risk control baseline of IT system consists of the following aspects:

3.2.1 The Internal Environment Analysis of IT System in Enterprises

The internal environment includes the keynote of the enterprise, which influences the risk awareness. The realization of the target relies on the internal environment of the IT system, which includes:

* The government of IT, IT organization structure, characters and responsibilities.
* The guiding principle and target of IT risk control, as well as the IT strategies of achieving this.
* IT ability, and the comprehension of IT resources and knowledge.
* IT system, information flow and decision making process.
* The relationship with internal stakeholders, and their perceptions and values.
* The IT risk management culture of enterprises.
* The IT risk management standards, guidance and models adopted by enterprises, etc..

3.2.2 The Collection of Related Information on IT Risk Management

The collection of related information on IT risk management refers to systematically collect all the related risk management information on all target systems. The information is the basis of organizing IT system risk management analysis and determining risk target. The collected information includes:

a) Information assets,

b) The construction of IT infrastructures

* IT risk management system;
* The construction of IT risk management organizations;
* Related disciplines and regulations;
* IT risk events happened in the past;
* high level IT system risk management target.

There are many methods to acquire the information. Such as, questionnaire, gauge, brainstorming, symposium, and communication between IT risk managers and IT system users. The work is quite complicated, but a very important work step.

3.2.3 The Target Setting of IT System Risk Management

The goal setting of IT system risk management, the strategy target of an enterprise, as well as the ability of IT system to support business strategic target realization, all these are prerequisites for managers to recognize the potential factors which influence the achievement of organizational business target. The IT risk managers should adopt proper programs to design IT system goal, ensuring the goal can support and suitable for the theme, and can be consistent with risk capacity.

3.2.4 The Recognition of IT Risk Factors and the Extraction of Key IT Risk Factors

Organizations should recognize IT system risk sources, the scope of risk influence, related events and potential results.

The purpose of IT system risk recognition is to establish a comprehensive risk list based on IT risk events. These events will hinder, degrade and delay the target realization. And in this process, the most important is to recognize IT system risks thoroughly.

* IT system planning stage: The risks confronted in this stage is management risks, technology and planning risks, as well as team construction and coordination risks.
* IT system analysis stage: The risks confronted in this stage are planning risks, technology risks, and progress risks and demanding risks.
* IT system designing stage: The risks in this stage are technology risks, progress risks and quality risks.
* IT system risk implementation risks: The risks in this stage are planning risks, technology risks, management risks and expenditure risks.
* IT operation and maintenance stage: The risks in this stage are mainly management risks, operation risks, technology risks, expenditure risks, market risks and credibility risks.

3.2.5 The Ascertainment of IT System Risk View

The risk view can analyze the IT risk influence resulted by the combination of IT system and business process. The ascertainment of risk view refers to it analyzes IT system and the above constructed business system risks from perspective of IT risk, thus providing a macro IT system risk view for those managers and high-level decision makers. It includes:

* The characters and security responsibilities in IT system;
* The integration level of IT system and business system;
* The risky degree of information flow in IT system.

3.2.6 The Definition and Ascertainment of IT Risk Control Baseline

IT risk control baseline refers to the basic risk manage and control baseline of an IT system (includes information assets, service process, organization of personnel, management rules, etc.), i.e., the degree IT system can satisfy the fundamental requirements of IT security and risk management.

The ascertainment of IT risk control baseline is the consensus of IT risk management stakeholders on its integrity, scope and content representation. This can guarantee the efficiency and rationality of the construction of IT risk control baseline, satisfying the requirements of IT risk management.

The definition and ascertainment of IT risk control baseline include the following several parts:

* The IT risk management target has to be ensured and satisfied.

* All the related aspects of IT system risk control baseline haveto be made certain. It includes: IT technology risk control baseline, IT investment risk control baseline, IT project risk control baseline, IT operation risk control baseline, IT management control baseline, etc..

* The consensus on IT risk controls baseline of IT risk management stakeholders can be achieved.

* IT risk control baseline can satisfy daily IT risk management requirements in enterprises, enhancing the IT risk management performance.

CONCLUSION

Based on ERM of COSO and IT life-cycle theory, this paper analyzed enterprise's IT risk management needs and its environment, provided the definition of baseline IT risk control, proposed the framework and models of constructing IT risk control baseline in enterprises, and finally discussed its elements and construction methods of IT risk control baseline. The baseline model of IT risk control was applied into IT risk management of enterprises and became a powerful tool of enterprises' IT risk management. The limitation of this thesis is a lack of empirical verification and quantification of IT risk control baseline. How to exactly construct IT risk control baseline of an enterprise, and make it quantified and verified, and how to apply it in practical IT risk management work and improve its efficiency will be an issue worthy of being discussed.

REFERENCES

Fang, H. X., & Wang, H. (2008). *Enterprise risk management — Integrated framework*. Dalian, China: Dongbei University of Finance & Economics Press.

Li, C., & Wang, W. (2009). The application of security baseline control in risk management process. *Network Security Technology & Application*, (9), 4-7.

Liu, A. G. (2009, August 5). A review of snapshot technology development. Retrieved 2011, August 5 from http://blog.csdn.net/liuben/article/details/4494555

Liu, T. (2000). Research of building security baseline of complicated information system. *Chinese Journal of Management Science,* (8), 636-644.

Lu, J. Y. (2011). *Information system risk management.* Beijing China: Tsinghua University Press.

Lü, X. (2006). Security classification methods and baseline guarantee strategy of e-government information system. *Netinfo Security,* (9), 34-36.

Ma, G. Y., & Shen, J. (2011). How to better serve the function of communication network as security baseline. *Telecommunications Technology,* (5), 11-14.

Ma, Y. (2005). Technological development and technological risk management. *Forum on Science and Technology in China,* (1), 33-36.

Sang, Z.Q. (2007). Security baseline and hierarchy protection of telecommunication operating enterprises. *Telecommunications Network Technology*, (9), 4-7.

Starr, C. (1969). Social benefit versus technological risk. *Science, 165,* 1232-1238.

Wang, Y. C., Zhang, J. L., Lu, X. Y., & Chen, Y. (2005). Risk Identification of IT projects during total life cycle. *Chinese Journal of Management, S2* (9), 5-9.

Yang, T. (2010). The commercial bank's information technology risk and the prevention. *Finance Forum,* (11), 66-70.

Yang, T. (2010). Study on the information technology risk in the commercial bank of China. *Information Security and Technology*, (06), 66-70.