2012 INTERNATIONAL SYMPOSIUM ON INFORMATION TECHNOLOGY IN MEDICINE AND EDUCATION

Research on Risk Control System ITG-HRCM in IT Governance

YUAN Wei-hua
School of Computer Science and Technology
ShanDong Normal University; ShanDong JianZhu University
ShanDong, JiNan 250101
huahua_qingdao@126.com

WANG Hong[1], ZHANG Jian[2], QI Wen-jing[2]
1. ShanDong Normal University;
2. ShanDong JianZhu University
ShanDong JiNan 250101
wanghong106@163.com, zj.jn@126.com,
qiwj@hotmail.com

***Abstract*—In this paper, based on the preliminary research results K-PRS-ISMCS and PRS-ISMCS, a variety of risks existed in the process of IT governance are firstly analyzed; then a full-life cycle, multi-layered structure of IT risk governance ITG-HRCM (Hierarchical risk control model) integrated with ERMF and COBIT based on PRS-ISMCS is put forward with the description of the model function; thirdly a kind of improved risk quantization and calculation method is described; finally the work of experimental simulation is done to various risks in the process of IT governance, which proves that ITG-HRCM with its improved risk quantitative calculation method can meet the demand and expectations of information security objectives in IT governance.**

Keywords-Information Systems (IS); information security risk; risk management; IT Governance

I. INTRODUCTION

As one of the most powerful factors for promoting social development in the wave of Information Technology (IT) throughout the world，Information Technology has become an important engine of the world's economic growth. Information is one of the most valuable human resources as the leading role of information age. Economic development, social progress and national security are increasingly dependent on the possession and protection of information resources—a kind of essential strategic resource. As a result, the connotation of information security and information security risks is accordingly expanding [2]. However, "More attention is paid on implementation, and less is on risk; as well as more attention is attached on technology and less is on control", is a kind of common phenomenon present in the process of information technology of enterprises. Therefore, in order to prevent risks of information technology which must be controlled effectively and to improve the core competitiveness of enterprises, the construction of IT governance is extremely urgent. There are various risks existed in the process of IT governance, and the most important ones include risk of IT investment and security risks of information systems. One of the aims of the IT governance is to "increase the value of information systems to achieve organizations' business objectives by the balance of risks in information technology and information processes" [13]. The security of information systems could not be guaranteed if IT security risks can not be controlled, which will lead to an endless process of IT investment. Worse still, the sharp raise of the cost of IT investment will eventually lead to the failure of IT investment and even bring about irreparable damage to enterprises. Therefore, research on risk control system in IT governance is of great importance and is of far-reaching significance.

The overseas research on risk management of information security has a history of over 20 years, which started in recent years in our country [1]. Though great importance has been attached to the research of risk assessment by each field of our country, it still has broad research capabilities because of its existence in the stage of research and development. In this paper, based on the preliminary research results, the K-PRS-ISMCS (Knowledge based-Process Controlling Resources, Protecting, and Realization of Security Objectives-IS Management and Control System) and PRS-ISMCS (Process controlling, Resources, protecting and Security), a variety of risks existed in the process of IT governance are firstly analyzed; risk control model in IT governance based on PRS-ISMCS is then put forward with the description of the model function; thirdly a kind of improved risk quantization and calculation method is described; finally the work of experimental simulation is done to various risks in the process of IT governance. The experiment proved that ITG-HRCM with its improved risk quantitative calculation method can control various risks in the process of IT governance effectively, and can meet the demand and expectations of information security objectives in IT governance.

II. CONSTRUCTION OF RISK CONTROL MODEL ITG-HRCM IN IT GOVERNANC

A. Various Risks Existed in the Process of IT Governance

1) Risks of IT investment: the failure of perfect combination and the lack of effective implementation of deep-seated factors, such as future development strategy, core culture and organizational structure in the design and implementation of IT governance system will cause the application of IT technology system to bring about useless or negative impact to enterprises, and even cause risks of failure of the system.

2) Security risk of information systems: When information systems go wrong, stop running or lose some effective functions, activities in all fields influenced by the

978-1-4673-2108-2/12/$31.00 ©2012 IEEE

system will become insecure, thus resulting in great losses and even affecting the normal running of society.

B. Security Risk Management and Control Model of Information Systems PRS-ISMCS

PRS-ISMCS[2] is a kind of security risk analysis and evaluation model of Information systems designed and implemented in the project of "Research of dynamic analysis and quantitative assessment of security risks of Information systems based on statistical learning". As research object of PRS-ISMCS, a variety of potential security risks of Information Systems are analyzed based on method of life-cycle and are classified into the following sorts: technical risks, security risks, continuous risk and regulatory risk. Strategic objectives of corporate, management goal of information security and realization of objectives are linked together based on the classification of risks and the framework of "multi-directional cross-frame" is designed to analyze and recognize the mutual relations between them.

However with the deeply carrying out of IT governance, users are increasingly concerned about whether the precautions of risks can meet the security needs of enterprises. What's more, PRS-ISMCS is not suitable for the management of all risks, such as risks of IT investment in IT governance. As a result, the thought of internal control is utilized to carry out special and overall audit and to realize control of Information Systems in the research on Risk Control System in IT Governance to decrease risks caused by system failure.

C. Construction of Risk Control Model ITG-HRCM in IT Governance

In order to effectively control risks in the process of IT governance, based on PRS-ISMCS, using such international mainstream of IT control-related standards as ERMF (Internal Control-Integrated Framework) and COBIT (Control Objectives for Information and related Technology) for reference, a full-life cycle, multi-layered structure of IT risk governance ITG-HRCM is built, as shown in Figure 1, consisting of strategic objectives layer, auditing monitoring level, risk assessment and control layer and standard reference layer. In order to make the risk management of enterprise more abundantly, effectively, globally and objectively, various risks in IT governance of enterprise are studied in the multi-dimensional perspectives involving business strategy, goal-oriented and proactive risk response. Internal control mechanisms such as Audit of Information Systems are taken to strengthen the management and control of risks.

D. Model Description

ITG-HRCM (Hierarchical risk control model) is a full-life cycle, multi-layered structure of IT risk governance integrated with ERMF and COBIT, various risks of enterprise in IT governance are studied in perspectives of business strategy, goal-oriented and proactive risk response and so on. The four layers consisting of ITG-HRCM are as followings: Layer of strategic objectives, audit monitoring, risk assessment and control and standard reference.

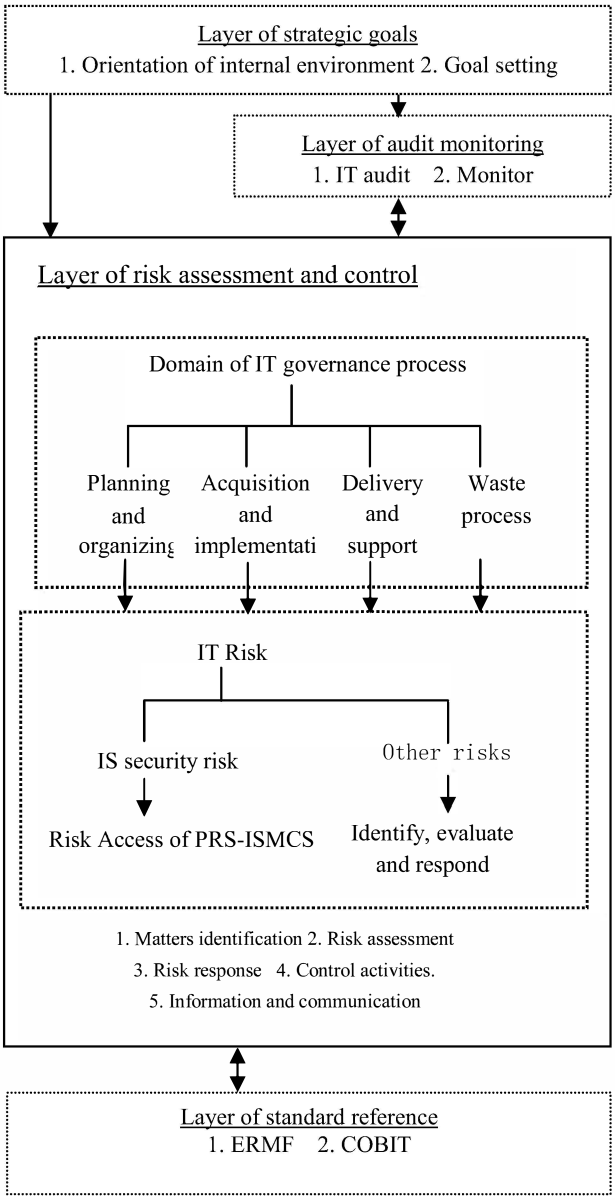
Layer of strategic goals
1. Orientation of internal environment 2. Goal setting
Layer of audit monitoring
1. IT audit 2. Monitor
Layer of risk assessment and control
Domain of IT governance process
Planning and organizing
Acquisition and implementati
Delivery and support
Waste process
IT Risk
IS security risk
Other risks
Risk Access of PRS-ISMCS
Identify, evaluate and respond
1. Matters identification 2. Risk assessment
3. Risk response 4. Control activities.
5. Information and communication
Layer of standard reference
1. ERMF 2. COBIT

Figure 1. Risk control model ITG-HRCM in IT governance.

1) Layer of strategic objectives

Layer of strategic objectives determines the needs of corporate business objectives by analysis of corporate strategy, business, competitive environment and technological development. Main activities belonging to this layer are orientation of internal environment and goal setting.

2) Layer of audit monitoring

Whether or not precautions of risks could meet security objectives of enterprises is judged by ways of audit, through such process of review and monitoring of information systems, to reduce risks of the system and to achieve security objectives.

3) Layer of risk assessment and control

As the third layer in ITG-HRCM model, layer of risk assessment and control is carry out the work of risk control in IT governance under the guidance of the first layer—strategic objectives, and which is also audit object of the second Layer—audit monitoring. Main activities belonging to this layer are matters identification, risk assessment, risk response, control activities, information and communication [4].

4) Layer of standard reference

This layer involves a set of various international standards using as reference for risk management and control in the Hierarchical risk control model, such as ERMF（Internal Control—Integrated Framework）of COSO, and COBIT(Control Objectives for Information and related Technology) of Information System Audit and Control Association and IT Governance Institute.

E. Characteristics of Model ITG-HRCM

1) Framework of hierarchical architecture

ITG-HRCM is a multi-layered structure of risk control and management in IT governance, including strategic objectives layer, auditing monitoring level, risk assessment and control layer and standard reference layer. Informationization of enterprise is characterized by management of multi-level, complicated process, difficult control of architecture of personnel and technology and so on. The architecture of the organization is usually made up of layers of decision-making, management and controlling [7], as a result the hierarchy of risk control model is chosen to make better and more efficient management of the various risks in the IT governance.

2) The combination of ERMF and COBIT

According to the characteristics of ERMF and COBIT, ITG-HRCM maximizs the advantages of the two theories to find a good meeting point for them. In the process of the building of hierarchical risk control model ITG-HRCM, activities carried out in each level are base on the eight elements (internal environment, objective setting, issues identification, risk assessment, risk response, control activities, information and communication and monitoring) of the theoretical framework ERMF of COSO [4]. While the application of control objectives in IT process is evaluated from three aspects comprised of reliability, safety and efficacy, with the audit of risks in IT governance on the line of the audit guide of COBIT [3].

3) Risk control of full life-cycle

ITG-HRCM divides the whole process of IT governance into four process domains according to characteristics of life-cycle of information systems: domain of planning and organizing process, access and implementation process, delivery and support process, and waste process. Risk control in IT governance begins with start-up phase of enterprise informationization, using proactive risk response strategies to minimized risks in all stages of IT governance in accordance with strategic objectives of corporate for risk control and IT audit, which is one of the most important parts in the whole process of IT governance.

4) Risk assessment of Information System is done by PRS-ISMCS

Risks in the whole life-cycle of the domains of Information System in IT governance are divided into two categories: security risks of information system and other risks, of which the former is the most important. If risks from information system could not be controlled effectively, they might be transformed into manage risks or strategic risks of enterprises [12]. Risks of Information Systems are dealt with by the three-dimensional security system model PRS-ISMCS from the project of "research of dynamic analysis and quantitative assessment of security risks of Information systems based on statistical learning", which can not only effectively identify security risk of Information systems, but the application of PRS-ISMCS can verify its effectiveness.

III. QUANTIZATION AND CALCULATION OF RISKS OF ITG-HRCM

A. Finne's Conceptual Model of Risk

Methods of risk assessment of information security referable are mostly inherited from the traditional ideas of conceptual model proposed by Finne, in which the risks and size of the loss were evaluated from the following areas: the vulnerabilities of information systems, possible attack, and loss of information assets [5]. The model is expressed as equation (1). Finne's view can be interpreted from the aspect of technology: risk is a potential degree of the possibility of loss and the size of potential loss that the body of threat makes use of the vulnerability of assets to destroy the enterprise which is determined by the possibility of occurrence of risk incidents and its impact.

$$R=F(A,V,T) \quad (1)$$

According to the conceptual framework of the three-factor risk model proposed by Yates, that risk is made up of potential losses, its size and uncertainty, Finne's conceptual model is scientific and rational, however it is confronted with many problems in practice [11]:

- Because information assets are far different from monetary assets, evaluation and potential loss are hard to measure.
- Sometimes the value of information assets is of relative meaning—information that one institution thinks very important, may become worthless when evaluated by another organization. Consequently, assessment of risk of information security based on simple assignment of the information assets may not be very convincing.

B. Quantization and Calculation of Risks of ITG-HRCM

In the IT management, more attention is paid on the actual loss caused by risks due to various threats utilizing vulnerabilities. In order to overcome the problems in Finne's conceptual model and to improve the effect of risk quantification of ITG-HRCM, the following improvements are done to quantification of key risk elements.

1) Quantification of key risk elements

Suppose a collection of assets for A = {a1, a2, a3, ...}, a vulnerability set of asset of a1∈A the Va = {v11, v12, v13, ...}; a collection of threat Ta1 = {t11, t12 , t13 ......}; a collection of security events, Ea1 = {e11, e12, e13 ......}; a collection of security measures Sa1 = {s11, s12, s13 ......};

the definition of risk vector of asset A for RA = {<a1, v11, t11, e11, s11>, <a1, v12, t12, e12, s12,>, <a1, v13, t13, e13, s13> ......}

2) Calculation of loss of risks

P(ti) represents the probability of occurrence of threat under a certain confidence level

C(ei) represents the maximum possible cost caused by a kind of event ei.

fi represents the amount of vulnerability, reflecting the possibility of weak points exploited by some threat with range [0, 1]. The value of fi is decided through the historical data of experience by experts.

P(ti)*fi reflects the actual likelihood of threat.

As to asset a, the corresponding weight vector is designed, Wa = {w1a, w2a, w3a ......}, the value is also obtained through the historical data of experience by experts.

R represents actual loss cause by the potential risk, and its value can be expressed and calculated as equation (2):

$$Ri = a_i \times w_i \times \sum_{t_i \in T_a} P(t_i) \times f_i \times \sum_{e_i \in E_a} C(e_i) \qquad (2)$$

IV. SIMULATION EXPERIMENT

Information system of a government is divided into two parts: intranet and extranet. Physical isolation was used between them for security reasons. Topology of Extranet portal of the government is shown in Figure 2.

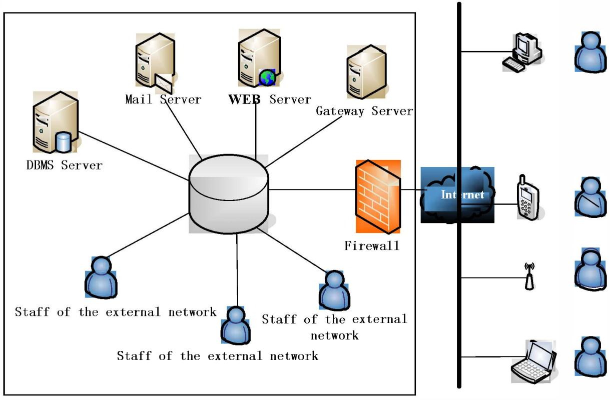
Mail Server
WEB Server
Gateway Server
DBMS Server
Firewall
Internet
Staff of the external network
Staff of the external network
Staff of the external network

Figure 2. Extranet topology of the government.

The portal is open to the public, including functions such as administrative affairs, online services and interactive participation. The whole information system has been in stable operation and maintenance phase of the life-cycle. The daily visits of the portal were comparatively large, and work of risk assessment was done in the phase mentioned above. There were approximately 7545228 visits recorded for about three months, among which about 350256 pieces of anomalies records, with its daily distribution shown in Figure 3.

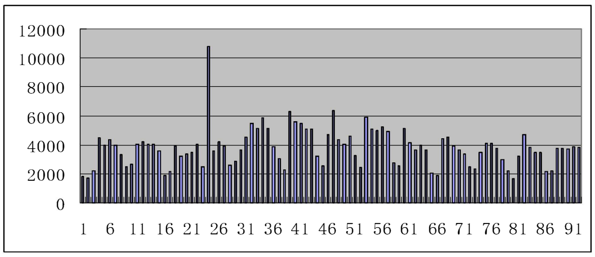

Figure 3. Daily distribution of anomalies records

According to the evaluation results of our implementation of ITG-HRCM, different types of threats against the WEB server and the corresponding impact of VI value were obtained and part of assessment result was shown in table 1.

TABLE I. TYPES OF THREATS AGAINST THE WEB SERVER AND THE CORRESPONDING IMPACT OF VI VALUE

ID name	Threats	Vulnerabilities utilized by Threats	vi	Risk level
......				
A 4 WEB Server	T11	V11（0.5）	0.3	Maintenance error
	T12	V15（0.3） V16（0.5）	0.3	System overload
	T13	V12（0.7） V13（0.1） V14（0.5）	0.7	Unauthorized access to system resources
	T14	V15（0.3） V16（0.5） V17（0.1）	0.5	Propagation of network virus
	T15	V12（0.7） V13（0.1） V14（0.5） V17（0.1）	0.7	Backdoor attack of Trojan horse
......				

According to formula (2), value of risk ri is calculated as follows (table 2):

TABLE II. VALUE OF RISK RI

Ti	p(Ti)	ai*p(ei)	wi	C(ei)	Ri
......					
T11	31.01%	1561	0.10	3	145.22
T12	4.70%	100	0.50	25	58.75
T13	20.97%	872	0.10	35	640.0
T14	28.01%	690	0.30	15	869.71
T15	15.30%	583	0.50	21	936.59
......					

V. Conclusion

After the establishment of risk control model ITG-HRCM in IT Governance, decision makers of risk management will be able to fully grasp present safety situation of the information systems. Management system of information security can be set up by ways of risk analysis and decision, as well as the construction of risk control model based on the life –cycle of information system. When risk of organization is not within the safety threshold of security management policy settings, appropriate security solutions are developed to make control and management of security risk under the acceptable range. Experiments show that, ITG-HRCM and its quantification and calculation methods of the risk can effectively control the various risks in the process of IT governance and can meet the requirements and expectations of security objectives in IT management.

References

[1] Yuan Wei-hua, Zhang Jian, Qi Wen-jing, “Research on Risk Management and Control System for Information Security K-PRS-ISMCS Based on Knowledge Management”, International Symposium on IT in Medicine and Education(ITME 2011), IEEE Press, Dec. 2011, pp. 31-35.

[2] Zhang Jian, Yuan Wei-hua, XU Jun-li, “Research on Security Management System PRS-ISMCS of Information System”, The International Conference on E-Business and E-Government(ICEE 2011), , IEEE Press, Dec. 2011, pp. 2505-2510.

[3] COBIT 4.0. Control Objectives for Information and related Technology, Version 4.

[4] Internal Control-Integrated Framework. COSO, 2004.

[5] Huang Jing-wen, “Study on Knowledge Based Risk Assessment for Information Security” ［D］, Donghua University, 2008.

[6] Sun Lei, “Research on Student Management Based on Knowledge Management” ［D］, Hei Long Jiang University, 2010.5.

[7] Liao Nian-dong, “Research on the Dynamic Risk Assessment Model of Information Security” ［D］,Beijing Jiaotong University, 2009.9.

[8] Huang Qin, Zhang Yue-Qin, Liu Li-Liang, “The research on Risk Evaluation Method of Modularization and Hierarchy of Information Security”, Computer Science, 2007, Vol.34 No10.

[9] GouDa-peng, “Research on Quantitative Methods of Information Security Risk Assessment” [D], HaErBing GongCheng University, 2009.

[10] James J.Jiang, Gray Klein.Software, “Development Risk to Project Effectiveness”, The Journal of Systems and Software.2000 (8):3-10.

[11] Du Mei, “Research and Application of Knowledge Management in teaching resources” [D], Beijing JiaoTong University of Posts and telecommunications, 2010.6

[12] Chen Guang, “Research on Method of Information System Information Security Risk Management” [D], National University of Defense Technology, 2006.

[13] Qiao Li-ping, “Study on IT governance of enterprise and method information system risk control”, 2003.

[14] Randall C.Reid, Stephen A. Floyd, “Extending the Risk Analysis Model to Include Market-Insurance”, Computers&Security, 2001(4), pp. 331-339.