

IT GRC-based IT internal control framework

Young Rok Yu*, Seong Chae Seo**, Byung Ki Kim**

**CAS Inc., Seoul Korea*

*** Department of Computer Science, Chonnam National University, Korea*

yryu@casit.co.kr, seseo@jnu.ac.kr, bgkim@jnu.ac.kr

Abstract—Recently personal information leakage and computer hacking occur constantly. The majority of the incidents are caused by the negligence of IT internal control. It is practically impossible to prevent all the security incidents caused by the insider. However, an Automated IT internal control system - considered about administrative, technical and physical internal control reinforcement for precaution and rapid response against the incident in the early stage - can reduce the security threat considerably. The object of this paper to present an IT internal control framework with enterprise-wide perspective embraced administrative, technical and physical internal control reinforcement.

Index Terms—IT GRC, IT Internal Control, Governance, Risk Management, Compliance

I. INTRODUCTION

Recently personal information leakage and computer hacking occur constantly. The majority of the incidents are caused by the negligence of IT internal control. Authorities had established some regulations and standard criteria for IT internal control enhancement but companies need a solution for IT internal control for themselves.

Following the internal control improvement strategy issue report of finance IT[1] published by Financial Security Agency in 2011, 60 percent of the security accidents are caused by insider and large companies are more vulnerable about insider threats.

According to CERT USA in 2009, representative insider security incidents types are as follows:

- IT Sabotage by system administrator who has dissatisfaction about their work or company and a special privileged user (45%).
- Theft or modification aimed at monetary profit by a user who has legitimate system access privileges in working hours (44%).
- Theft or modification aimed at business profit by the person in charge.

Server/Network shut down and delete data by Ex-Gucci America employee in April, 2010 is for a typical example of insider security incident. Gucci America estimated the damage at \$200,000. The majority reason of this incident is poor access

control. Another example is Bank of America confidential information leakage. This incident caused by ex-program developer.

Organization which audits accounting internally are doing IT internal control using risk management, regulation and testing in IT fields. However, it is usually just a formality. Organization is using an information security program for control and response efficiently for increasing security treats of inside of the organization, but the program used very limited area of internal control. That is organization make an effort to reinforce the internal control, but it is insufficient enterprise-wide internal control framework which can maintain administrative, technical and physical ways at one point.

It is practically impossible to prevent all the security incidents caused by the insider. However, an Automated IT internal control system - considered about administrative, technical and physical internal control reinforcement for precaution and rapid response against the incident in the early stage - can reduce the security threat considerably. For reduce the security treats, it need to build an IT internal control framework embrace administrative, technical, physical internal control reinforcement.

This research present an embracing administrative, technical and physical internal control reinforcement IT internal control framework based on IT GRC(Governance, Risk management, Compliance). Governance defines administrative plans such as polish management, IT audit and response security incidents. Risk management defines technical and physical plans such as access control, server vulnerability, personal information access, information leakage component. Compliance defines Control Self Assessment (CSA) and compliance component such as personal information level evaluation.

This framework is an unified IT internal control framework which satisfied personal information access record archiving and privacy internal control system in Privacy Security Act Korea and inside data leakage prevention in industrial Technology Security law and differentiated from integrated log management, security management, or ESM.

II. RELATED RESEARCH

A. IT GRC

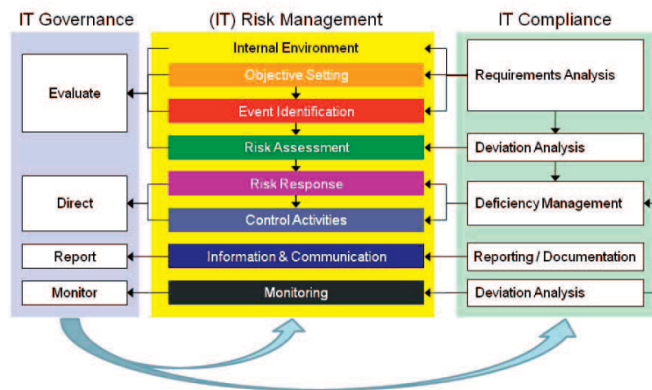
IT GRC consists of Governance, Risk and Compliance. IT Governance is composed of leadership, organizational structure and the process that IT supports and extends the organization's strategies and objectives [2]. In the current field of internal control framework, research such as Polish Management, IT Audit is not satisfactory.

IT Risk is a business risk associated with IT use, ownership, operation, involvement, influence and adoption. It is classified in a variety of ways, such as IT benefits / value realization, IT program and project delivery, IT operations and service delivery [3]. However, the implementation of Risk IT framework is rather weak to accommodate the COSO ERM (Enterprise Risk Management).

IT Compliance means domestic and foreign IT related laws and regulations. Financial IT security compliance framework in accordance with the law and the nature of the standard is classified as a total of 19 financial, security related laws, security standards [4].

B. IT GRC Framework for Consideration

IT GRC process model is a combination of IT governance, Risk management and IT Compliance to proceed with the analysis and control [5]. The model IT governance, as shown in the figure below follows ISO/IEC 38500:2008[6]; risk management the COSO ERM framework [7]; finally, IT compliance generic model to follow.



[Figure 1] IT GRC process model

Gartner identifies four primary functions of enterprise-wide governance, risk, and compliance platforms: audit management, compliance management, risk management, and policy management [8].

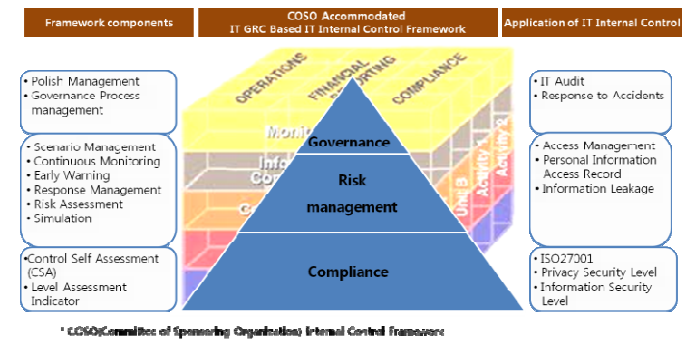
C. Information Security Control Activity

Jeong [9] has been studied empirically the moderating effects on organizational effectiveness of Information Security control activities (physical security, administrative security, technical security). He verified the impact on organizational

effectiveness of Information Security control activities (physical security, technical security, administrative security); and the result of verification, physical security, technical security, administrative security factors on organizational effectiveness has been revealed statistically significant.

III. IT INTERNAL CONTROL FRAMEWORK

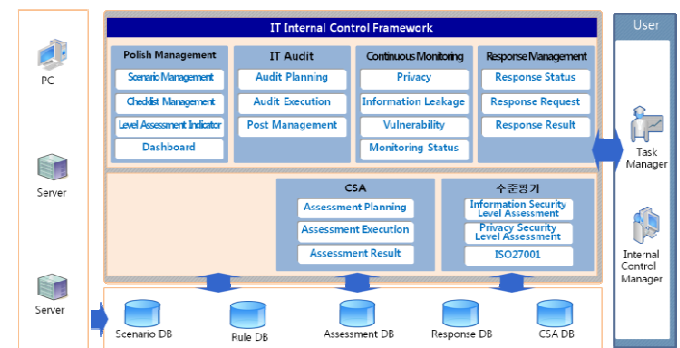
This chapter presents the components that comprise the IT internal control framework and internal control practices.



[Figure 2] IT GRC-based IT Internal Control Framework

A. Component Elements

This chapter defines the component needed in internal control, IT GRC perspective. From the perspective of IT Governance, polish management, IT Audit; IT Risk, continuous monitoring, response management, risk assessment; IT Compliance, CSA, level of assessment.



[Figure 3] IT Internal Control Framework Diagram

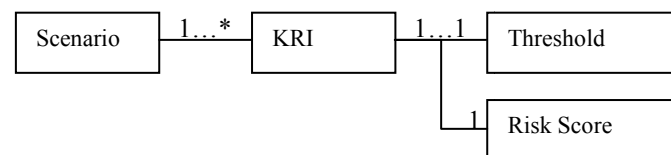
Polish management

Polish management administers an enterprise-wide policy needed to IT internal control. It consists of scenario management for IT Risk continuous monitoring and early warning, checklist management for CSA, management of the level assessment indicators for evaluation of the level such as Information Security Evaluation, dashboard that can determine the status of the overall internal control, law and regulations configuration management to manage internal control relevant law and regulations

Risk Scenario is a narrative about IT incidents that can impact on the business. To monitor the possible vulnerability, it collects personal information access record, DLP(Data

Leakage Protection), VPN(Virtual Private Network), access control and a variety of based security systems; and it creates a scenario where IT Risk on. For example, it pertains to large amounts of personal information that allowed non-IP access and download if the mail is sent.

All scenario defines specification for continuous monitoring, KRI (Key Risk Indicator) for measuring the risk. In one scenario, multiple KRI can be defined. This is the same principle as the one to measure various events. KRI manages risk score so that appropriate indicators of normal values, the caution, warning threshold, and corresponding risk can be assessed. From the existing scenario and the source data of scenario target, the user responds to changes in the business scenario generation, simulation and registration.



Threshold	max	min
normal		
caution		
warning		

Risk Score = (Finance+Media+Users) effect * weighting

Risk Level = {A, B, C, D, E}

[Figure 4] IT Risk Model

Checklist is the check item to manage IT Compliance across the enterprise self-check. It manages check contents, check items, detailed items, ratings, check intervals, importance, target institution.

Level of evaluation indicator manages indicators to diagnose internal and external IT Compliance level, including Information Security level diagnosis, Privacy Security level diagnosis. It manages diagnostic items, detailed diagnostic items, check point, judgment, improvement and measures, diagnostic results.

IT Audit

IT Audit manages the process for IT Audit. It consists of audit planning, audit execution and follow-up management. IT Audit utilizes continuous monitoring status to make Yearbook audit planning and proceed to perform audit preparation, audit execution, audit reports based on the audit plan, and perform disciplinary management of post based on the results of audit. By utilizing the status of IT Risk monitoring, it performs risk-based IT audit such as focused audit matters, inspired, auditable selection.

Continuous Monitoring

Continuous monitoring constantly monitor IT Risk scenarios that is subject to the IT internal control. IT Risk scenarios can be divided into personal information, information leakage vulnerability. Continuous monitoring can drill down statistics for each scenario and check the detailed information in the summary. If possible to take place of the vulnerability while

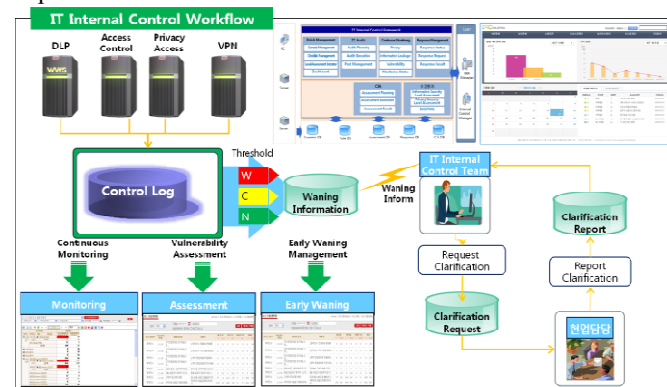
checking the details of the scenario, it can take advantage of the vulnerability and generate a list of vulnerabilities.

Response Management

By IT Risk scenarios, internal control personnel responses request, and it provides response personnel an opportunity to explain the reason rationally.

Risk Assessment

By assessing the degree of IT Risk Scenarios incurred into scenario-specific, personalized, organization, Risk Assessment is used as a reference or the strategy for future IT audit and improvement.



[Figure 5] IT Internal Control Workflow

CSA

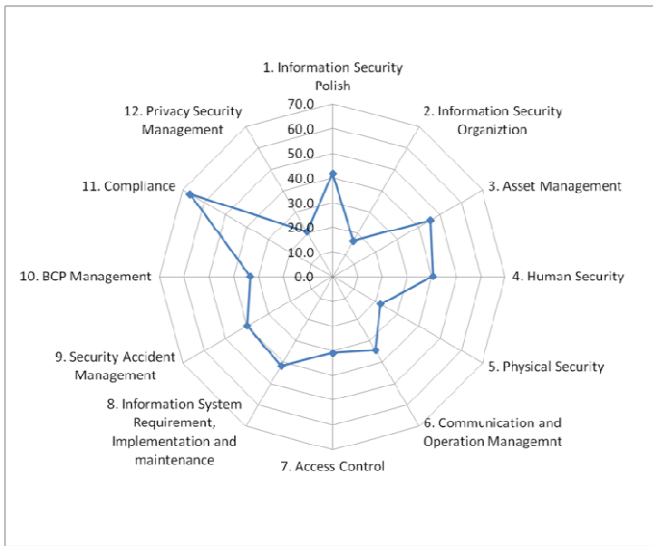
CSA plans, assesses the evaluation of the defined internal control checklist and compiles statistics to determine the level of awareness of the enterprise-wide internal control.

부서	3주		4주		1주		2주		4주		평균	
	이행	내용	이행	내용	이행	내용	이행	내용	이행	내용	이행	내용
IT운영팀	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
광남지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	5.00	0.00	1.25	0.00
광동지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
광서지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
고객서비스팀	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
광주지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
대구지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
대전지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
마케팅전략팀	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
부산지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
분당지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
수원지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
업무지원팀	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
원주지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
인천지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
울산지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
제주지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
준법감시부	0.00	0.00	0.00	0.00	3.75	2.31	5.00	1.50	0.00	0.00	2.91	1.27
중앙지점	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

[Figure 6] CSA result Example

Level Assessment

Level Assessment manages the current level based on the Information Security evaluation, Privacy evaluation defined at the level of the internal and external evaluation indicators.



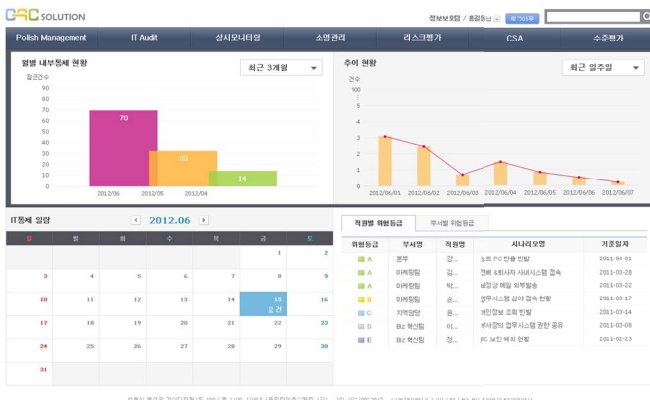
[Figure 7] G-ISMS(Government-ISMS) Level Assessment Example

B. IT Internal Control Instances

For internal control, IT Risk scenario consists of the personal information, information leakage and vulnerability. Personal scenario means to misuse the personal information in the record for access to personal information processing system. Information leakage scenario means a scenario where personal and confidential information can be leaked. Vulnerability scenario can cause internal vulnerabilities from right management and access control.

IV. RESULT AND DISCUSSION

Below is the example that implements IT security internal control system using IT internal control framework.



[Figure 8] IT GRC-based IT Security Internal Control Framework

Control for external attacks is being built, and internal control is being operated by DLP, VPN, access control; however, internal information leakage and IT Sabotage occurs consistently.

By utilizing IT internal control framework, possible vulnerability or early detection of vulnerability can be managed.

With the future security area, IT internal control zone can extend the area to IT strategy, build and operation.

V. SUMMARY AND CONCLUSION

Although there are already a variety of security-related solutions, the internal control system is required for responding to internal control issues, such as information leakage. Also, it needs to have integrated IT internal control system for systemizing it and set up a culture of internal control.

REFERENCES

- [1] S. H. Hong, "Strategy for Strengthen Financial IT Internal Control", Issue Report, vol. 2011-008, Financial Security Agency, 2011
- [2] Electronic Publication: "Cobit 5.0", at <http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx>
- [3] Electronic Publication: "Risk IT", at <http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx>
- [4] T. H. Kim, Y. T. Kim and J. M. Sung, "A Study on Financial IT Security Compliance Framework" in Proceedings of the Korea Information Processing.
- [5] N. Racz, A. Seufert, and E. Weippl, "A process model for integrated it governance, risk, and compliance management," in Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010), 2010, pp. 155-170
- [6] Electronic Publication: C. McClean, K. McNabb and A. Dill, "The GRC Technology Puzzle: Getting all the Pieces to Fit," 2009. Accessed 10 January, 2010, at <http://www.forrester.com/Research/Document/Excerpt/0,721,1,45772,00.html>
- [7] M. Rasmussen, "Hand in Hand," Business Trends Quarterly, vol. 2:2, May 2007, pp.44-46.
- [8] N. Racz, E. Weippl and A. Seufert, "Governance, Risk & Compliance (GRC) Software – An Exploratory Study of Software Vendor and Market Research Perspectives", 2011, Proceedings of the 44th Hawaii International Conference on System Sciences.
- [9] G. H. Jeong, S.R. Jeong, "The Effect of Information Protection Control Activities on Organizational Effectiveness : Mediating Effects of Information Application", Intelligence and Information Systems vol. 17:1. May 2011, pp. 71-90.



Young Rok Yu have completed a PhD in computer science from Chonnam National University in 2001. He received the MSc degree in computer science from Chonnam National University in 1998. He has worked for CAS Inc. in Seoul, Korea. His research interests are in GRC(Governance, Risk management, Compliance), software security, software engineering.



Seong Chae Seo received his PhD in computer science from Chonnam National University in 2006. He received the MSc degree in computer science from Chonnam National University in 1997. He is currently an post-doctoral researcher of computer science in the Chonnam National University in Gwangju, Korea. His research interests are in software analysis, software engineering, software quality, software security, software process, UML.



Byung Ki Kim received his PhD in mathematics from Chonbuk National University in 2000. He was chairman of Korea Information Process Science(KIPS) in 2007. He is currently a full professor of computer science in the Chonnam National University in Gwangju, Korea. His research interests are in software analysis, software engineering, software quality, software security, software process, software testing.