韓國IT서비스學會誌
第12卷 第4號
2013年 12月, pp.219-234
http://dx.doi.org/10.9716/KITS.2013.12.4.219

정보시스템 감리 프레임워크 개발 : 한국 전자정부의 RFID/USN 프로젝트 개발을 통해서*

김소정* · 구철모* · 고창은***

IS Audit Framework Development through e-Gov's RFID/USN Project in South Korea*

Sojung Kim* · Chulmo Koo* · Chang E. Koh***

■ Abstract ■

We introduced a framework of information systems audit methodology and applied to IS projects based on RFID/USN in six public organizations in South Korea. An analysis of five IS implementation projects shows the iterative technical specific risks are disclosed. The key 14 risk factors categorized into 4 classifications (Project Management, application, database, system architecture) which are based on the established IT audit framework in order to extend to the technology (RFID/USN) specific framework and apply to the other case as well. The implications of these findings for audit research and practice are discussed.

Keyword : Information Systems Audit, e-Government, South Korea, National Information Society Agency(NIA)

논문투고일 : 2013년 07월 26일 논문수정완료일 : 2013년 11월 28일 논문게재확정일 : 2013년 12월 03일

* The authors wish to thank Korean Information Agency(NIA) for its cooperation and support.

** 국립 싱가포르 대학교 경영대학, 정부기관조직 연구센터 연구원

*** 경희대학교 호텔관광대학 교수, 교신저자

**** 북 텍사스 주립대학교 경영대학 교수

1. Introduction

The use of IT in the public sector has significantly increased in many countries. The rapid and pervasive implementation of IT applications by public organizations in South Korea is worth noting and provides excellent cases to study. Thus we set out to explore IT development and management practices by public organizations in South Korea and found that surprisingly, knowledge managerial aspect of monitoring IT projects is often noticed, but has received far less rigorous analysis.

In the absence of a specific IT project monitor and control scheme, we developed a framework to be applied and tested for several projects. In this study, we developed new auditing framework for a projects encompassing specific technology namely, RFID (Radio Frequency Identification). Specifically, this study is to (1) analyze audit reports of RFID projects, (2) develop the auditing framework for RFID specific projects, and (3) apply the proposed framework to the target project. For the purpose of this, we choose RFID projects managed by Korean IT promoting authority, namly NIA (National Information society Agency) in South Korea as NIA has supported to implement e-governments projects which often utilize the emerging information technology such as USN (Ubiquitous Sensor Network) as well as RFID. Moreover, as a steward of e-government of South Korea, NIA has conducted auditing on those projects. Through the RFID/USN audit throughputs, NIA has provided that various types of best practices to contribute to a successful IS implementation, maintenance, and operation in public sectors. The objective of this study is to investigate the validity of the NIA through RFID/USN auditing projects. We analyzed RFID/USN IT projects, uncovered hidden problems, and articulated the critical risk factors and recommendations. Finally, this case study would be able to reduce potential risks as well as increase quality information to the future IS implementation.

2. Monitor and Control IT Projects

Organizations are increasingly aware of the potential role of information technology (IT) in supporting strategic business goals and maximizing overall returns [2] as well as the risks associated with the implementation of IT [15] They are investing a large amount of money on various IT projects, some of which do not return expected outcomes in terms of qualify software products delivered in time and with budget Blackburn et al. [5] This inevitable gap between the expectation and the reality with IT projects calls for the need for prudent IT audit methods to monitor the reliability and integrity of IT projects to ensure the maximum return and minimum risk.

The need for an effective auditing method is equally essential to public organizations as well as private ones [24]. For these public organizations ensuring the quality and integrity of the development, implementation and maintenance of IT projects are essential [24, 28]. Despite good intention of developers and users involved in IT projects, some projects end up with products with defects, sub-standard performance, inadequate operation and maintenance and inappropriate uses [18]. To eliminate or reduce such IT project maladies, organizations need to adopt an ef-

fective IT auditing method to monitor IT projects throughout the entire lifecycle of the project [28]. Numerous studies have investigated the quality and productivity of software development, but few have approached from a comprehensive IT auditing perspective Faraj and Sproull [9] Harter et al. [12]. Several systematic methods to monitor and control IT projects have been project such as the Control Objectives for Information and Related Technology (COBIT) developed by ISACA (Information Systems Audit and Control Association) and the Capability Maturity Model (CMM) developed by SEI (Software Engineering Institute). COBIT has provided the link to bridge the gaps between business risks, control needs and technical issues and showed good practices and activities across a domain and process framework. It emphasizes regulatory compliance, helps organizations control risks and increase the value of the IT project, enables to align IT with it's the business goals and simplifies implementation of the COBIT framework [15] Ridley et al. [20]. On the other hand, CMM was originally developed as a tool for objectively assessing the ability of government contractors' processes to perform a contracted software project. However, it has become a general model to aid in improving organizational business processes in diverse areas such as software engineering, system engineering, project management, software maintenance, risk management, system acquisition, information technologies Debreceny et al. [7]

3. NIA IT Audit Framework

IT audit has been highlighted in focusing on institutionalization because risks or possible reverse functions of IS have critical impact on decision-making capability, consequently the role of IT auditor in its capacity of controlling the risks of IS, is critical. However, the benefits of IT audit and critical success factors for IS audit have not been fully explained and empirically investigated yet in the theoretical literature.

The reasons why the IT audit has gained little attention in the academic literature may be, (1) it covers two different disciplines (software engineering and auditing) [28] and its pragmatic approach hinders research to extend the discussion on IT audit; (2) it has been regarded as only a part of accounting, giving researchers little chance to focus on the importance of IT auditing; and (3)the risk concerned in IT audit holds a multi-dimensional and subjective concept and this makes it difficult to evaluate the impact of IT audit Ellis et al.[8]. Moreover, IT auditors are supposed to judge the risks and report the influence, which makes it difficult to investigate the risks and IT auditing. This paper, will brifely introduce Korean IS audit framework developed by NIA and propose the complementary framwork for RFID specific projects.

3.1 NIA(National Information Agency)'s IS AUDIT

Under the perspective of IS audit by itself, it is widely recognized that IS audit activity contains the procedure of collecting evidence related to the defects and giving feedback about pros and cons Ellis et al. [8]. However, it is hard to make a consensus among auditors [27], and moreover, to find any significant difference for a technical or a judgmental knowledge between

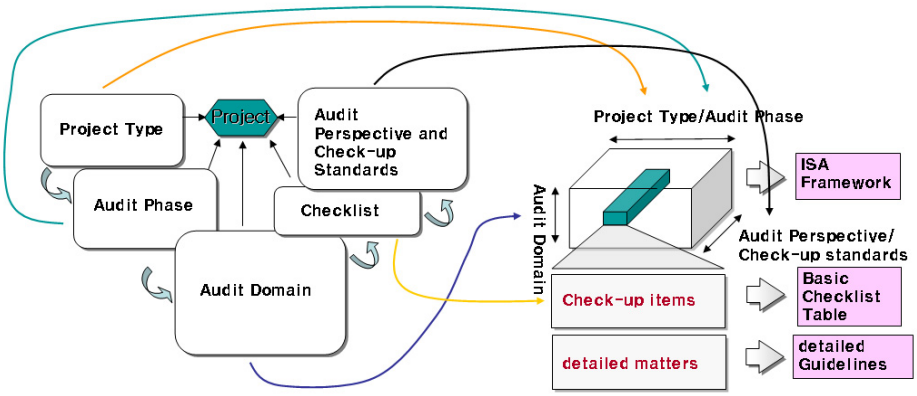
auditors and auditees responsible to software quality control and proper measures Grabski et al. [11]. Due to these drawbacks of the audit, Grabski et al. [11] insisted that IS audit should be carried out not only an internal audit that has an appropriate checklist to determine control weakness, but also an external audit that should be considered by public accounting firms (e.g., General Audit Standards compliance of public accounting firms) to ensure that all factors were addressed in all the audits.

For the importance of appropriate check lists in Information Systems Audit, NIA has developed NIA Information Systems Audit Framework (NIAF), which is well suited for the e-Gov situation. Even though the Information Systems Audit Framework was initially developed as a simple check list for auditing, it has been enhanced and refined with heuristic data based on the previous IS audit experience for more than 20 years in public sector of Korea. According to the NIA [14, 23] 46 expert groups have attended to establish and extend the NIAF including detailed ISA Guidelines. NIAF includes a chart that incorporates audit examination points by project type, audit times, and areas of the audit, based on the audit examination framework. Outlines and basic audit examination items are defined by each audit area and its structures [Figure 1]. The conceptual model [Figure 1] is used to execute audits through the framework [Figure 2], which composes of a check-up system based on project types/auditing phase depending on audit domain with a perspective of a basic check-up standard, to be flexibly applied to changes such as the emergence of new project types.

The NIAF construction includes the three major components (project type/audit phase, audit domain and audit perspective/check-up standards) :

Project type : A project can be classified as enterprise architecture construction, information strategy planning, system development, database construction, system operation or system maintenance. These categories are based on the life cycle of the IS implementation project in question.

Audit phase : This phase proposes adequate timing required for regular audits by referring to



[Figure 1] Relationship between Conceptual Model and NIAF

the methodologies used in audit cases previously performed. In the case of system development projects, the audit phases are classified, with methodology models commonly used for recent IS implementation projects, specifically into the structured-information engineering development model and the object-oriented component-based development model.

Audit domain : It enables consistent audits to be conducted by classifying the target objects of standardized units (areas) of audits into audit domains based on project type/audit phase. Audit domain consists of Project Management, Application, Database, and System Architecture

Audit perspective/check-up standards : In conducting an audit, a lack of consistency may result and this is due to different interpretations of auditor views based on their individual experiences and knowledge. Audit perspective was introduced to reduce the lack of audit consistency. With this concept, an auditor reports the target project from the viewpoint of the methodology and the procedure relevant for the target project.

NIA IS Audit Repository : After the audit execution procedure, certified auditor should submit the final audit report which including following factors.

- Project information : budget, period, type, phase, vendor (developer), acquirer
- Audit information : audit phase, period, auditors
- Used basic check items
- Score of each domain and result of each domain in brief
- Recommendation including type, time, importance, and related stakeholder
- The detailed report on findings including detected problems, points of improvements, and the snap shot showing status at audit time.

Audit results with above mentioned factors based on NIAF have been stored in NIA IS Audit repository. Some of the information of repository is analytic knowledge, including project information and basic check items. On the other hands, some of the information of repository is qualitative knowledge, which is hard to analysis but instinctive and useful to extract specific knowledge, including recommendation and retailed reports [23].

4. Research Methodology

4.1 Multiple-Case Study Research Design

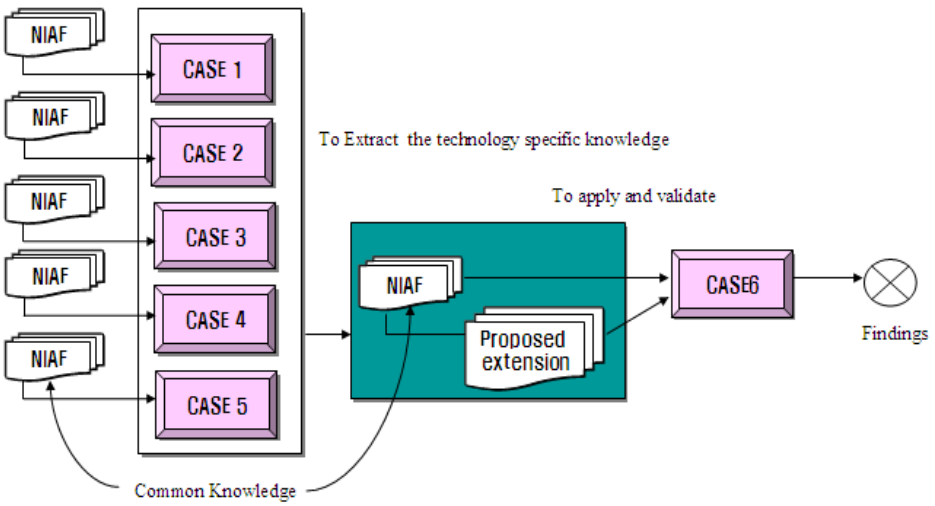
[30] suggests that a case study can be useful when a researcher explores a topic that has rarely been researched. Furthermore, the case method can be effective tool when trying to conceptualize or theorize a complex subject or behavior in a real world setting Benbast et al. [3]. The case method is also well suited to the study of IS implementation when the research is largely exploratory and it addresses the “how” and “why” questions Benbast et al. [3, 30]. We adopted the case method for this study for the following reasons : (1) Study of audit on e-Gov is still immature and there are few literatures on that research field; (2) It is useful to extract the practitioner’s knowledge from the case study rather than quantitative research; and (3) Our research questions include not only what but also many why and how question.

Our study is based on six cases. A multiple-case study can provide more detailed and sig-

nificant results than a single-case study [30]. Multiple-case studies can help researchers investigate complex relationships among numerous concepts and variables more effectively. Moreover, the multiple-case study provides a higher level of external validity and reliability than a single-case study [30]. In this research, multiple-cases are used, 6 cases of which were conducted and stored in repository of NIA , while the final 6th case was conducted after extracting knowledge from previous auditing. Extracted knowledge (proposed risk factors) from previous audit experience on e-Gov RFID/USN pilot IT implementation was applied to the target site and evaluated. Research model for case study is depicted in [Figure 2]. This is extension of previous research of [23] and similar to [14] work.

4.2 Validity and Reliability

Case study was criticized because it is difficult to conduct repeatedly and has possibility to distort the facts under the perception of researcher's subjective view. Repository, however, can solve the problem of lack of iteration in the case study because same kinds of cases of repository are used. NIAF, also, can be able to work out the problem of lack of objectivity because findings are refined based on the prepared NIAF which is established by external expert group. By using replication logic of the same examination protocol based on the NIAF in multiple case studies, the external validity of the information can be obtained. On the other hands, using multiple sources of evidence (software development artifacts, documents, interviews, observations, testing) based on the NIA audit methodology provides multiple measures of the same phenomenon in each case. This multiple measures develop a process of triangulation and make the construct more convince and accurate. To increase the reliability, all findings from each case were sent to both acquirer and implementer to make sure that the findings have no biased interpretation or judgment.



[Figure 2] Research Model for Case Study

4.3 Data Collection

The target cases are obtained at the NIA audit repository of previous auditing on e-Gov IT implementations. We screen them and choose the 6 RFID/USN projects for 2 years. Secondly, the 6 cases for the purpose of examining validity of the extracted risk knowledge are determined. The final case also fills the criteria and purpose of this research. Finally, we focus on the 6 projects that implemented for the e-Gov RFID/USN pilot projects as following <Table 1>.

4.4 Case Analysis

Analysis on the NIA Audit Repository for e-Gov RFID/USN Pilot Projects : This analysis includes three investigations on the cases. In the first investigation, examination on the face validity of recommendation items in the each audit result (each of the first six cases) was performed. According to audit methodology and NIAF, the recommendation holds the potential risks of the project and the proposed solution to control it for the success of the projects. Through the examination process of contents validity, we screened the recommendation items and deleted those items that contained trivial findings (e.g. the target project is predicted to miss the planned schedule), consequently, did not meet the NIAF protocol and criteria of the research as well. After examination on contents validity, we choose the recommendation items and the used basic check items as well, which are also analytic knowledge and easy to grasp from the repository as following <Table 2>.

Even though the contents of detailed reports on findings were more implicit than the analytic figure depicted in <Table 2>, <Table 3>, those have more meaningful and abundant information about the cases. Some of the potential risk items can be escalated repeatedly, which are also RFID/USN project specific. Those technique specific risk items, which would be used as check list items for the later auditing, were extracted by the second investigation analyzing on the implicit findings. The second investigation was

〈Table 1〉 RFID/USN Implementation Background Comparison

	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
Ownership	Gov	Semi-Gov	Gov	Gov	Province	Province
Implementer	SME	SME	LE	SME	SME	LE
Budget ($ million)	1.19	0.62	0.63	0.48	0.67	0.70
Duration (Months)	8	7	7	6	5	6
Number of Sites	5 sites	39 sites	N/A	N/A	9 sites	6 sites
RFID MW	Smart-Chain	Pavillion	Wave-Frame	URID	N/A	N/A

〈Table 2〉 Number of Used Basic Check Item

Audit Domain	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
Project Management	7	7	6	6	8	7
Application	6	5	7	6	6	5
Data Base	6	5	6	6	5	4
System Architecture	5	4	7	4	5	5

〈Table 3〉 Number of Recommendation

Audit Domain	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
Project Management	4	7	5	2	3	5
Application	2	4	4	3	4	4
Data Base	2	4	2	4	2	3
System Architecture	5	3	4	5	2	7

performed to classify each recommendation items to risk construct and weight the impact of the construct on the IT implementation success in each case.

Since we'd established no initial construct, constructs were revealed and refined with iterative and explorative approach. The final risk constructs, naturally, have the variance of their coverage, and, can be related to each other. The classification process also contained the assumption because it was conducted retrospectively not prospectively. To weight the impact of the risk construct on the target project, two kinds of measure were used, which are degree of emergency (DE, Degree of Emergency) holding upper, medium, and beyond) and degree of importance (DI, Degree of Importance; upper and beyond), respectively. Either of two index DE or DI is an indicator into the final IS audit report. For example, we set upper DE with beyond DI or medium DE with upper DI to medium impact on the success (**), upper DE with upper DI to strong impact (***), and medium DE with beyond DI or beyond DE with upper DI to weak impact (*).

After the coding process, we got the preliminary table illustrating the extent to which different factors proposed have affected the RFID/USN IT implementation. The preliminary table may contain very unusual situation of the case, and consequently, the factors related to less than 2 cases were deleted, then we got the cross case effect matrix in the second place as following <Table 4>.

From the analysis on the 5 cases, 14 risk factors in the four perceptions or domains (from project management and quality assurance to system architecture and security) were explored. Under the perception of project management and quality assurance of the project, sufficient preparing for IT operation (e.g. a plan to educate the operators) is a critical risk factor to all cases. Case 5 has a strong impact of that risk at the level of average of impact, since Case 5 has a short project period that may call for more effective effort than other cases. Alignment with performance target is also a critical factor. It is difficult to meet the performance requirement (non-functional requirement) since even though RFID/USN technique may be immature, acquirer (governmental organization) want their target performance to be obtained through the projects. Evidence also shows that management of multi-task has very a strong effect on the success in Case 1 and Case 2, while remain cases present no impact of it. One of the possible reasons is that Cases are related to the harbor distribution and hold more distant hosts than others and Case 2 holds many remote hosts at the level of average, so this feature of the two cases let the impact of simultaneous management of multi-sites strong.

〈Table 4〉 Cross Check Matrix

	Case 1	Case 2	Case 3	Case 4	Case 5
PM and QA Prepare sufficiently for operation		**	*	*	***
Consider alignment with performance target		**	*	*	***
Manage multi-site task simultaneously	***	***			
Application Must define and finish required task	**	*	***		***
Must align business process with RFID infra considering malfunction of RFID reader	*	***		*	
Consider usability	**		**		
Integration test problem		***		*	
Database Refine relative documents preparing for connection with heterogeneous system	**		*	*	*
Consider further data volume and tuning			*	**	
Consider tracibility		*			***
System Architecture and Security Manage test process and result	**	***	*	*	***
Consider tracibility and accessibility	*		***		*
RFID code type: private			*		
Wide problems with RFID middleware	*		*		

Note) *** : The impact of risk construct is very high, ** : medium, * : weak.

Under the perception of application systems, four factors were explored. First of all, evidence shows that finishing the defined requirement task is a very critical factor for all cases. IT implementation project holds the ambiguous outcome image at the level of average so that it causes requirement volatility and requirement uncertainty [17]. If it need to deal at the pilot project with USN technique, its uncertainty gets strong along with high technology uncertainty. For above mentioned reason, requirement management can be critical factors to the cases. Cases 4, however, also interestingly, present no effect of the requirement management. One of the possible reasons is that its project size is relatively small, so it has small project complexity to handle the requirement uncertainty effectively. Under the perception of database, 'to refine relative database artifacts (including system interface definition, naming rule) preparing for connection with heterogeneous system' is critical on the success of IT implementation. The RFID reader of the USN should sense the tag information real time and transfer the data to the other heterogeneous system, so that it is important to make the relevant artifacts to be clarified so as to operate the system effectively. Tuning the database with predicted data volume and obtaining the tracibility of the data is effective to the success, however, its effectiveness is different among the cases.

While the risk factors related to tune shows medium effect on Case 3 and Case 4 and no effect on case 2 and case 5, the risk factors re-

lated to traceability shows high effect on case 2 and case 5 and no effect on case 3 and case 4. This evidence shows that there may be a trade off between data tracibility and data tuning. One of the solutions to trace RFID project effectively is put the more information into the RFID tag. If the RFID tag holds much information, it can improve tracibility but its read/write speed also can be delayed and database should handle the huge amount of data calling for tuning. In other words, if there is a high possibility of lack in tracibility, there is a low possibility of low transaction speed, while there is a high possibility of slow transaction speed, there is a low possibility of difficulty in trace. Tracibility of data is evidently critical issue in the projects involving RFID/USN technique, however, it contains multi aspect and solution under the concept of tracibility, including data normalization, data type, relation attribute, and so on.

Under the system architecture and security, tracibility and accessibility is also explored risk factors as well. Most of all, management test with various scenarios is a very important factor effecting the success of project. All the cases stress the testing considering product type, climate, data volume, moving speed, building type, simultaneous perception, adhesion method, reader interference, direction oriented antenna, and so on. This means that reading rate is easily decreased sharply by the minor mistakes operator made or unexpected environment situation, so the test with various kinds of scenarios should be conducted. The second factor, however holding weak impact on success in the perception of system architecture domain, is related to RFID code policy. Acquirer, naturally, can choose their RFID code type, which is one of the public (EPC Gen2, or ISO/IEC Type C) or private type, and each choice has pros and cons. The governmental agency may prefer private (not international, but national) code type to management effectively contrary to the industry's preference.

The last risk factor is related to the RFID middleware including inter-operation, unskilled adaption, deficient operation manual, monitoring problem, and vulnerability. Even though only two cases present weak impact of RFID middleware risk on the success, its importance needs to gain attention due to the pattern of hazards which are widely spread. In addition to above mentioned risks, the other factors related to institutional concern or software development methodology were also found in the second investigation. These risk means that it is required to tune the relevant law or institution and tailor the traditional software development process (e.g. ISO/IEC 12207 or vendor's software development methodology) as well in order to implement successful IT

Application and Validation of Proposed Risk Items and NIAF : The proposed factors were applied for the final and 6th case. The body of NIA Audit knowledge, including basic check list, was also used for that case. In the middle of auditing on that case, auditors validated the RFID/USN technique specific audit knowledge and NIAF. This validation process ensures that the previous specific knowledge can be applied to IS system concerning same technology issues. The basic check items based on the NIAF were proposed to the target project.

During the auditing period, the proposed RFID/USN specific risk factors (14 risk items) and above illustrated 21 basic check items were con-

〈Table 5〉 Proposed Basic Check Items (Common Items)

Domain	Number of items	Proposed check items (example)
Project Management	7	◦ Adequacy of follow-up responses related to the proposal/contract/task concerned/project charter ◦ Applying to relevant software development methodology and standard ◦ Adequacy of quality assurance plan and activity ◦ Achievement of business target and quality target ◦ Presence of plans for technology transfer and education and adequacy of relevant activities ◦ Presence of operation team to be setup to maintain the implemented systems ◦ Adequacy of plan of trial operation
Application	5	◦ Consistency between implemented system and each task concerned ◦ Consistency between software development artifacts including analysis, design, implementation, and test holding readability and tracibility ◦ Adequacy of inter/intra interface of application system and implementation of functions concerned ◦ Adequacy of integration test, plan for user test, and results ◦ Adequacy of system optimization activity
Database	4	◦ Adequacy of implementation of database table ◦ Adequacy of access authority and control to data ◦ Adequacy of preparing of the initial data ◦ Adequacy of user manual
System Architecture and security	5	◦ Specification and design for system architecture and security ◦ Adequacy of phasing and installation of system and set up a ◦ security environment ◦ Adequacy of examination on system element ◦ Adequacy of plan for system test and its results ◦ Adequacy of operation manual

sumed to evaluate the target system. Almost all of the proposed check items were applicable to the information system in the final case, and 10 risk factors from 14 risk factors were related to the RFID/USN specific and defected problems. The total number of recommendation items are 19 including 9 items and 10 items related to proposed RFID/USN specific risks. The all findings about risks (recommendation items) and its impact were submitted to the acquirer (municipal organization) and the implementer.

In addition, there was extra finding except for the above depicted RFID/USN specific check item in <Table 7>, which is related to a network topology and also related to a critical risk to successful IT implementation as follows : Network topology can be critical, since without careful definition of ad hoc network (e.g. Zigbee), safety and availability are hard to be obtained. In the 6th case, sensor node was revealed to operate as relay that was the evidence sensor was implemented as FFD (Full Function Device). However, an edge node is expected to be RFD (Reduced Function Device) and coordination node is desirable to be FFD. The impact of newly finding risk was set to be 'weak negative' through careful examination by the researchers and the certified auditors.

Above newly founding could be added to the RFID/USN specific knowledge or common NIAF knowledge after the examination on the importance or repeatability of the items. The applica-

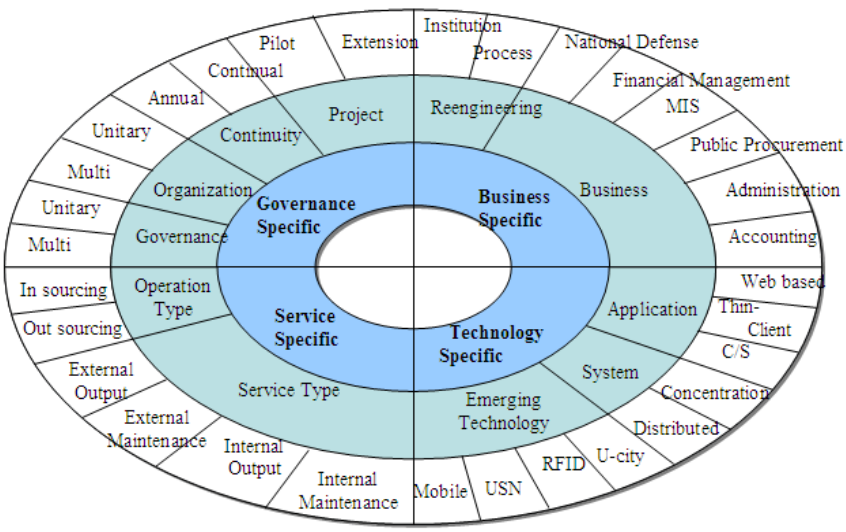
〈Table 6〉 Items Related to Defected Findings

Auditing Dimension	Proposed check list		Recommendation list		
	Basic check items	RFID/USN specific items	Basic check items	RFID/USN specific items	Total
Project Management and Quality assurance	7	3	3	2	5
Application	5	4	1	3	4
Database	4	3	1	2	3
System architecture and security	5	4	4	3	7
Total	21	14	9	10	19

tion and validation of the proposed risk items showed that the RFID/USN specific knowledge is applicable to the IS concerning same technology issues, consequentially, that the RFID/USN specific knowledge based on NIAF can be developed through the e-Gov IS implementation.

Transform of the NIA IS Framework : NIA IS Audit framework can be used as evolving and transformational knowledge base. The current NIAF (ver 2.0), which is organized based on software development lifecycle and project type, can be extended to the multi-faucet model including the technology dimension as depicted in [Figure 3].

The feasibility study of technology specific knowledge also showed other specified knowledge can be re-used and extended through NIAF efficiently. Beyond the technology or business specific knowledge, if the extended information was acquired and managed under the NIAF perspective, a variety of information can



[Figure 3] Extension of NIA IS Audit Framework

be combined and applied to practitioner's IS of the convergent domain, and consequently, can contribute to the high quality of various IS implementation demands. The proposed multi-faucet NIAF model, which is based on [14]'s work, is the one of the considerations to adapt the convergence of IT implementation and it has major advantage of its flexibility and wide range of available auditing. The extension of framework also makes it possible to gather information of the emerging technology with agility, because the proposed framework is flexible to brand new information technology.

5. Discussion

Turning to the research questions, it is possible to grasp technology specific knowledge based on the heuristic cases concerning same technology issues. Even though 5 cases were conducted by different practitioners in difference periods, there were the overlapped and repeated risk factors founded by the certified experts with the reasonable recommendations, which are known as best practices, and consequently, 14 risk factors were explored. After the extraction process from the repository of NIA, this study proposed RFID/USN specific risk items, which were used for the last case (articulation of knowledge).

The research question is about the feasibility whether the proposed items can be apply to the IS implementation with same technology and business regards. Through the pragmatic approach to the final case, this research showed that the proposed items were applicable as well the common body of NIAF (combination of knowledge). Interestingly, network topology issue which hasn't been dealt in the previous auditing was found from the final case, so that is in need of being added to the proposed items. The knowledge of best practice for enhancing of high quality and reliability of e-Gov implementation, of course, should be dispersed but specialized so as to achieve efficiency and flexibility at the same time.

6. Conclusion

The principal finding of this study is important for several reasons. First, under the perspective of researcher of audit methodology, it demonstrates the useful scenario in which the researchers develop the guidelines through extracting from previous experience knowledge and apply those guidelines to the following site. More specifically, the findings from e-Gov RFID/USN IT implementation confirm the conclusion of applicability of the proposed audit guideline-risk items. Second, it suggests the multi-faucet model to manage extensible knowledge. Beyond the software life cycle concern, business specific or technology specific issues could be addressed in this extensible framework. This study yield general insight into extendible knowledge management through practical audit scheme.It is hoped that this paper will serve as a platform from which NIAF studies of greater depth and specify may be undertaken.

Limitation : This study dealt with the limited factual data of audit experience, which some might characterizes as insufficiently reliable. There could be the loss of information about the previous auditing time, so the study was limited in extracting knowledge from previous audit

experience. Cleary, this extracting of knowledge might be speculative, and considerable work needs to be done. The final case, so as to valid the proposed risk items, was a single case. Since the multi-case has higher external validity than single-case [30], research on the multiple sites may increase the external validity. The conclusions of this case study await further refinement and correction in the light of further research.

References

[1] Anon, "Research on Korean IT market", available at http://www.krgweb.com/, (accessed 2010).

[2] Bacon, C. J., "The Use of Decision Criteria in Selecting Information Systems/Technology Investments", *MIS Quarterly*, (1992), pp.335-353.

[3] Benbast, I., Godstein. D. K, Mead, M., "The case research strategy in studies of information systems", *MIS Quarterly*, Vol.11, No.1(1987) pp.365-386.

[4] Bedard, J. et al., "Information Systems Risk and Audit Planning", *International Journal of Auditing*, Vol.9, No.2(2005), pp.147-163.

[5] Blackburn et al., C. C. Blackburn, C. L. Augustine, R. Li, R. P. Harvey, M.A. Malin, R. L. Boyd, J. F. Miller, and G. Morahan, "The nu gene acts cell-autonomously and is required for differentiation of thymic epithelial progenitors", 1996.

[6] Cho, I., "Information Systems Audit Legislation Passed in Korea. Information Systems Control Journal Online", (2008), pp.1-6.

[7] Debreceny, R. S. and G. L. Gray, "IT Governance and Process Maturity : A Multinational Field Study", *Journal of Information Systems*, Vol.27, No.1(2013), pp.157-188, doi : 10.2308/isys-50418.

[8] Ellis, D., R. Barker, S. Potter, and C. Pridgeon, "Information audits, communication audits and information mapping", *International Journal of Information Management* Vol.13(1993), pp.134-151.

[9] Faraj and Sproull, "Coordination expertise in software development team", *Management Science*, Vol.46, No.12(2000), pp.1554-1568.

[10] Gilhooley, I. A., "Auditing Computerized Systems", *EDPACS : The EDP Audit, Control and Security Newsletter*, Vol.9 No.8(1982), pp.1-8.

[11] Grabski, S., J. H. Reveau, and S.A. West, "Comparison of Judgment, Skills, and Prompting Effects between Auditors and Systems Analysts", *MIS Quarterly*, Vol.11, No.2 (1987), pp.151-161.

[12] Harter, D., M. Krishnan, and S. Slaughter, "Effects of process maturity on quality, cycle-time, and effort in software product development", *Management Science*, Vol.46, No.4(2000), pp.451-466.

[13] Kim, C., "*Research on actual status of IS Audit in the public sector*, NIA, National Information society Agency", 2000.

[14] Kim, C., "The IS Auditor Basic Education and Professional Education Textbook", NIA, National Information Society Agency, 2007.

[15] Lainhart, J. W., "Cobit : A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities", *Journal of Information Systems*, Vol.14(2000), pp.21-25.

[16] Lee, C., "*The Study on the effects of IT au-*

dit in the national administration network project", NIA, National Computerization Agency, 1992.

[17] Nidumolu, S., "The Effect of Coordination and Uncertainty on Software Project Performance : Residual Performance Risk as an Intervening Variable", *Information Systems Research*, Vol.6, No.3(1995), pp.191-219.

[18] Nidumolu, S. R., "A Comparison of the Structural Contingency and Risk-Based Perspectives on Coordination in Software-Development Projects", *Journal of Management Information Systems*, Vol.13, No.2 (1996), pp. 77-113.

[19] Park, S., "*The Study of the measure of IT audit efficacy"*, NIA, National Computerization Agency, 1998.

[20] Ridley, G., J. Young and P. Carroll, "COBIT and its Utilization : A Framework from the Literature, *Proceedings of the 37th Hawaii International Conference on System Sciences",* 2004.

[21] Rittenberg and G. B. Davis, "The Roles of Internal and External Auditors in Auditing EDP Systems", *Journal of Accountancy*, (1977), pp.51-58.

[22] Rittenberg, L. and P. Charles, "The Internal Auditor's Role in MIS Developments", *MIS Quarterly*, Vol.2, No.4(1978), pp.47-57.

[23] Seo, S., "*The ISA PR Material"*, NIA, National Computerization Agency, 2001.

[24] Seo, S., "A study on the Effectiveness of Information Systems Audit", NIA, National Computerization Agency, 2002.

[25] Seo, S., "A Study on the Enhancement of the IS Audit Framework", NIA, National Computerization Agency, 2003.

[26] Sun, L., R. P. Srivastava, and T. J. Mock, "An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions", *Journal of Management Information Systems*, Vol.22, No.4 (2006), pp.109-142.

[27] Weber, R., "Information systems control and audit", New York : Prentice Hall, 1998

[28] Weiss, I. R., "Auditability of Software : A Survey of Techniques and Costs", *MIS Quarterly*, (1980), pp.39-50.

[29] Wu, R. C., "The information systems auditor's review of the systems development process and its impact on software maintenance efforts", *Journal of Information Systems Spring*, (1992), pp.1-13.

[30] Yin, R. K., "*Case Study Research : Design and Methods. 2nd Edition"*, CA : Sage Publication, 1994.

◈ 저 자 소 개 ◈

김 소 정 (bizkims@nus.edu.sg)

현재 싱가포르국립대(National University of Singapore) Centre for Governance, Institution, and Organisation(CGIO)에 재직하고 있다. 전 국가정보화전략위원회 전문위원 및 한국정보화진흥원 책임연구원으로 재직하였으며. 성신여자대학교에서 전산학, 서강대학교에서 컴퓨터공학 석사, 경영학 박사 학위를 취득하였다. 주요 관심분야는 소프트웨어 개발 에코시스템, 거버넌스, IT기업의 지속가능성 등이며, 연구 결과는 MIS Quarterly Executive 등의 저널에 출판 되었다.

구 철 모 (helmetgu@khu.ac.kr)

현재 경희대학교 호텔관광대학 조교수로 재직 중이다. 서강대학교에서 경영정보시스템 전공으로 박사학위를 취득하였다. 주요 연구관심분야는 스마트 관광(Smart Tourism)이다. International Journal of Electronic Commerce, International Journal of Information Management 등에 논문을 게재하고 있다.

고 창 은 (Chang.Koh@unt.edu)

죠지아 대학(University of Georgia)에서 경영정보학으로 박사학위를 취득하고 현재 북텍사스대학 (University of North Texas) 에 재직하고 있다. 주요 연구분야는 IT의 가치와 경영효과, IT의 국제적 문화적 비교연구 등이며 연구 결과는 MIS Quarterly, Information and Management, International Journal of Electronic Commerce 등의 주요 저널에 출판되었다.