한국산학기술학회논문지
Vol. 11, No. 2, pp. 703-708, 2010

비즈니스 위험관리를 위한 정보보호제도 분석 프레임웍에 관한 연구

김민선[1*]
[1]협성대학교 유통경영학과

A Study on Analysing Framework of Information Security Management Systems for Managing Business Risk

Min Sun Kim[1*]
[1]**Department of Distribution Management, Hyupsung University**

요 약 정보원천의 다양화와 정보시스템 취약성의 증가는 비즈니스 위험을 증가시킨다. 성공적인 비즈니스는 적정한 비즈니스 위험관리를 통해서 가능하다. 그러나 비즈니스 위험관리는 재무적 관점에서 시행되고 있고, 정보보호관리제도는 정보보호의 관점에서만 이루어져 통합적인 비즈니스 위험관리를 수행하기에 부적절하다. 본 연구는 통합적인 비즈니스 위험관리기법을 개발하기 위하여 정보보호관리제도인 ISMS, EA, ISO27001, COBIT, SPICE, 정보시스템감리, SSE-CMM 등을 비즈니스 위험관리관점에서 분석하였다. 본 연구에서 분석된 정보보호관리제도는 비즈니스 위험관리를 위한 원천으로 활용가능하다.

Abstract Various information sources and the increasing vulnerabilities of information systems could increase the risks of a business. The successful management of business risks depends on appropriate level of risks in business. Business risk management would be conducted in terms of financial risk management and information security management. The financial management and the information security management could not achieve an integrated business risk management. For developing the integrated business risk management, this study analyzes the various information security management systems such as ISMS, EA, ISO27001, COBIT, SPICE, Auditing. This study analyzes information security systems, which could be utilized in developing business risk management.

Key Words : Business Risk Management, Information Security, Framework

1. 서론

정보원천의 다양화와 정보시스템 취약성의 증가는 비즈니스 위험을 증가시킨다. 성공적인 비즈니스는 적정한 비즈니스 위험관리를 통해서 가능하다. 그러나 현재의 비즈니스 위험관리는 재무적 관점과 정보보호관리 측면에서 이루어지고 있기 때문에 비즈니스 위험관리를 위해서는 통합적인 비즈니스 위험관리 기법이 필요하게 된다. 정보시스템은 비즈니스 관리에 있어서 토대를 제공한다. 따라서 정보시스템의 위험관리와 비즈니스 위험관리는 밀접한 관련을 이루고 있다.

본 연구는 비즈니스 위험관리를 위하여 정보보호관리제도를 분석함을 통하여 통합적인 비즈니스 관리에 활용하고자 한다.

본 연구는 정보보호를 위하여 활용되는 7가지의 제도를 정보보호 관리, 프로세스 관리, 프로세스 측정의 3가지 관점에서 비교하였으며, 정보보호 제도와 정보보호 견고화와의 연관성을 비교분석하였다. 이러한 비교를 통하여 정보보호강화 제도를 보완하고, 각 제도에 상호보완적인 연계점을 찾는 것이 가능하다[8].

국내외 정보보호관리기법 방법론은 정보보호관리체계

*교신저자 : 김민선(sunnyminkim@hanmail.net)
접수일 10년 01월 18일 수정일 10년 02월 23일 게재확정일 10년 02월 24일

(ISMS), ISO 27001, EA(Enterprise Architecture), COBIT, 정보시스템감리, CMMI, SPICE 등이 있다.

2. 정보보호관리기법

정보보호관리기법을 분석하면 다음과 같다.

2.1 정보보호관리체계(ISMS)

ISMS는 각 기관이 정보보호를 위해 필요한 관리적·기술적·물리적 기준에 적합한 정보보호관리체계를 갖추었는지 심사하여 인증기준에 따라 적절히 운영되고 있는 경우 인증서를 부여하고 지속적으로 사후관리를 수행하는 제도이다[2,3].

2.2 ISO 27001

ISO 27001 인증제도는 물리적(출입통제, 인적보호), 기술적(정보시스템보호), 관리적(정보보호정책, 정보자산 식별, 위험분석평가 등) 보호 조치 수준에 대한 객관적인 평가를 통해 인증서가 발급되는 것으로서, 적합한 정보보호관리 수준을 평가하는 제도이다. 국내 ISMS와 유사한 제도이다[9].

2.3 EA(Enterprise Architecture)

EA(Enterprise Architecture, 전사적 아키텍처)는 조직의 주요 비즈니스, 정보, 응용시스템, 기술 기반구조를 정의하고, 요소간 상호 연계되는 모습을 총괄적으로 표현하며, 조직이 나아가야 할 방향에 대한 지침을 포함하는 실체로서, 효과적인 IT 관리를 수행하기 위한 도구이다.

2.4 COBIT

COBIT는 IT 보호 및 통제 부문에서의 모범적인 업무수행 방법에 대한 일반적으로 적용가능하고 인정되는 기준으로 개발되었다. COBIT 구조는 34가지 상위통제목표, 아래에 세부통제목표, 관리지침, 그리고 성숙도모델로 이루어져 있으며, 계획 및 조직(plan and organize), 도입 및 구현(acquire and implement), 납품 및 지원(delivery and support), 모니터 및 평가(monitor and evaluate)의 네 가지 업무영역(domain)으로 그룹화 되어 있다[7].

2.5 정보시스템 감리

정보시스템 감리는 감리발주자 및 피감리인의 이해관계로부터 독립된 자가 정보시스템의 효율성을 향상시키고 안전성을 확보하기 위하여 제 3자적 관점에서 정보시스템의 구축에 관한 사항을 종합적으로 점검하고 문제점을 개선하도록 하는 제도이다. 기존의 제도를 점검하는 성격이 강한 제도이다[1].

2.6 CMMI

CMMI는 소프트웨어와 시스템공학의 역량성숙도를 평가하는 모델로서, 프로젝트계획(project planning), 공급자계약관리(supplier agreement management), 기술솔루션(technical solution), 검증(verification), 확인(validation) 등 22개 영역으로 구성된다[6].

2.7 SPICE

SPICE는 소프트웨어 프로세스 전반을 망라하여 심사를 하고 그 결과에 따른 조직의 프로세스를 개선하는 활동에 대한 표준화 방법으로, CMMI와 방법론에서 유사하다. 적용대상 범위는 프로세스계획, 관리, 실행, 통제 및 개선에 두고 있으며, CUS(고객-공급자프로세스 범주), ENG(공학프로세스 범주), SUP(지원프로세스 범주), MAN(관리프로세스 범주), ORG(조직프로세스 범주) 등 5가지 큰 프로세스 범주로 구성되며, 소프트웨어획득프로세스, 품질관리프로세스, 개발프로세스 등 24개 영역으로 되어있다[10].

3. 정보보호관리 및 사례

정보보호관리는 정보보호관리에 초점을 맞춘 제도, 전체적인 프로세스관리에 초점을 맞춘 제도, 전체 프로세스나 각 프로세스의 수준(보호, 업무기준만족, 품질 등) 측정에 초점을 맞춘 제도의 3가지로 분류가 가능하다[4,5].

[표 1] 국내외 정보 보호강화를 위한 제도들

분류	유사제도
정보보호 관리에 초점	정보보호관리체계, ISO 27000 시리즈
프로세스 관리에 초점	정보시스템감리, EA, COBIT
프로세스 측정에 초점	CMMI, SPICE

표 1에서 정의한 국내외 정보보호강화를 위한 제도들의 초점에 대한 구조, 대상범위에 대한 비교는 표 2와 같다. 여기서 G-ISMS는 행정기관을 위한 국내 ISMS이다.

[표 2] 국내 ISMS와 ISO27000, G-ISMS의 비교

구분	ISMS	ISO 27000	G-ISMS
관점	정보보호관리를 위한 종합적인 시스템	정보보호관리를 위한 종합적인 시스템	행정기관에 적합한 정보보호관리를 위한 종합적인 시스템
구조	- 정보보호관리관정(5단계, 14개 통제사항) - 문서화(3개통제사항) - 정보보호대책 (15개 분야,120개 통제사항)	- 11개의 통제영역와 38개 통제목표, 133개의 통제항목 - 관리적보호, 물리적보호, 기술적보호의 3요소	- 정보보호관리관정(4단계, 15개 통제사항) - 문서화(3개통제사항) - 정보보호대책 (11개 분야)
평가대상	- 정보통신서비스 제공자 - 정보통신서비스를 위한 물리적 시설을 제공하는 자 - 그 밖에 정보통신망을 운영하는 자	- 정보보호관리가 필요한 조직(인터넷기업, 금융기업, 일반기업에 걸친 전분야)	- 행정기관
인증범위	- 조직의 규모와 특성에 따라 정보보호관리체계의 범위를 조직의 일부로 정의함	- 조직의 정보자산을 관리, 운영하는 시스템 및 프로세스	- 행정기관이 정하는 자율적으로 정하는 범위 - 그 범위가 얼마나 타당하고 적절한지를 평가하는 것이 원칙임

3.1 정보보호관리에 초점

정보보호관리란 정보보호관리에 중점을 두는 제도를 의미한다. 조직의 효율성, 프로세스 개선 보다 정보보호관리에 초점을 집중하는 제도로서 대표적인 제도로는 국내의 정보보호관리체계, G-ISMS, 국외의 ISO27000 시리즈 등이 있다.

3.2 프로세스관리에 초점

프로세스관리란 프로세스관리에 중점을 두는 제도를 의미한다. 조직의 정보보호뿐만 아니라, 효율성, 프로세스 개선 등 정보보호 관리가 하나의 요소가 되는 제도로서 대표적인 제도로는 국내의 감리, 국외의 EA, COBIT 등이 있다.

[표 3] 감리와 EA, COBIT의 비교

구분	감리	EA	COBIT
관점	프로세스, 산출물, 성과의 관점에서 정보시스템의 구축에 관한 사항을 종합적으로 점검하고 문제점을 개선하도록 하는 것	조직의 주요 비즈니스,정보, 응용시스템,기술 기반구조를 정의하고, 요소간 상호연계되는 모습을 총괄적으로 표현하며, 조직이 나아가야 할 방향에 대한 지침을 포함하는 실체	조직이 전사적으로 IT 거버넌스 구조를 구현할 수 있도록 하는 국제적이고 일반적으로 인정된 IT 통제 프레임워크
구조	3가지 감리관점(절차,산출물,성과) 절차_계획 적정성,절차 적정성,준수성 산출물 _ 기능성,무결성, 편의성,안정성,보호성, 효율성,준거성,일관성 성과 _ 실현성,충족성	- 아키텍처 활동(추진체계정립, 개발,활용, 관리) - 아키텍처 산출물(4가지 도메인,Buleprint, 원칙) - 참조 및 기준(참조모델, standards/profile)	- 경영자를 위한 개요 - 프레임워크(COBIT의 4가지 업무 영역과 관련된 34개의 IT프로세스) -34가지 상위통제목표(high-level control objective) 아래에 세부통제목표(detailed control objective), 관리지침(management guidelines), 성숙도모델(maturity model)로 이루어져 있으며 4가지 업무영역(domain)으로 그룹화됨
평가대상	감리의 대상이 되는 정보화사업	기업의 비즈니스와 정보, 그리고 이를 지원하기 위한 애플리케이션, 인프라등 기술 구성요소	경영자,사용자,정보시스템 감시인의 세부류의 이해관계자들을 대상으로 개발됨
인증범위	대상이 되는 프로세스 전체	- 비즈니스 아키텍처에서 시작하여 관련된 데이터,응용, 인프라아키텍처까지 수립 - 인프라 기술 표준에서 시작하여 비즈니스 아키텍처까지 수립	IT 보호 및 통제 부문

3.3 프로세스 측정에 초점

프로세스측정이란 정보보호관리, 프로세스관리뿐만 아니라 이들을 수준별로 평가하는 제도를 의미한다. 조직의 프로세스를 몇 단계의 수준으로 보고 각 수준별 단계마다 수행하는 프로세스가 다르다. 대표적인 제도로는 SPICE와 CMMI 등이 있다.

[표 4] SPICE와 CMMI의 비교

구분	SPICE	CMMI	
관점	개별 프로세스	SPICE와 CMM 통합	
구조	2차원	Staged	Continuous
평가대상	프로세스별 능력수준	조직	프로세스
레벨	6레벨(0~5)	5단계(1~5)	6단계(0~5)

4. 정보보호강화 제도의 현황

각 제도의 수행기관 및 정의, 관리영역, 관리 방법, 국내외 현황은 다음과 같다.

[표 5] 정보보호 관리에 초점을 둔 제도의 소개

방법론 및 제도	수행기관 및 인증기관	정의	관리영역 및 관리방법	국내외현황
정보보호관리체계(ISMS)	한국정보보호진흥원(KISA)	기술,관리,물리적 정보보호 대책을 구현하여 지속적으로 관리·운영하는 종합적 시스템	정보보호관리과정 요구사항이 5단계로 있고, 문서화 요구사항이 3가지 있으며, 정보보호 관리통제 점검항목으로 15개 통제분야가 있음	2008년 12월까지 총 58건 인증서 발급. 2005년 이후 포털, 의료, 교육 분야로 확대, 2008년에는 원격교육설비기준에 권고사항으로 반영
ISO 27000 시리즈	국제표준화기구(ISO)	정보보호 관리체계 국제규격 인증으로 보호정책, 자산분,위험 관리 등	11개의 통제영역와 38개 통제목표, 133개의 통제항목으로 이루어져 있음	BS7799에서 국제규격으로 승격됨에 따라 최근 정보보호 컨설팅 업계인 증획득을 향한 움직임을 보이고 있음

[표 6] 프로세스 관리에 초점을 둔 제도의 소개

방법론 및 제도	수행기관 및 인증기관	정의	관리영역 및 관리방법	국내외 현황
정보시스템 감리	한국정보사회진흥원(NIA)	정보시스템의 구축에 관한 사항을 종합적으로 점검하고 문제점을 개선하도록 하는 것	6개의 사업유형으로 분류하고, 감리 관점(절차, 산출물, 성과)과 감리영역을 정의하여 점검함	2008년 본격적으로 확대되어, 정보기술아키텍처(ITA/EA)를 새로 도입하는 공공기관이 40여 곳에 달해 이를 점검하는 감리활동 활성화를 기대함
EA	한국전산원	조직의 주요 비즈니스, 정보, 응용시스템, 기술기반구조를 정의하고, 요소간 상호연계되는 모습을 총괄적으로 표현하며, 조직이 나아가야 할 방향에 대한 지침을 포함하는 실체	단계별 정보보호 관리절차(계획/구현/운영단계)와 시스템, 네트워크, 응용시스템, 사용자, 데이터 등 정보기술자원 전반을 포함함	EA에 대한 정부 및 기업의 관심은 매우 고조되어 있는 상황이며, ITA/EA 구축 노력이 활발히 진행되고 있음
COBIT	정보기술관리협회(ITGI)	조직이 전사적으로 IT 거버넌스 구조를 구현할 수 있도록 하는 국제적이고 일반적으로 인정된 IT 통제 프레임워크	4가지 업무영역 및 상위 34개 IT 통제 목적과 그에 따른 302개의 세부적/구체적인 통제 목적을 제시함	향후 계속해서 진화해 나갈 것이며, COBIT를 바탕으로 추가연구가 진행되고 있음

[표 7] 프로세스 측정에 초점을 둔 제도의 소개

방법론 및 제도	수행기관 및 인증기관	정의	관리영역 및 관리방법	국내외 현황
CMMI	소프트웨어 공학 연구소 (SEI :Software Engineering Institute)	소프트웨어와 시스템 공학의 역량성숙도를 평가하는 모델로써, 조직 프로세스를 보다 적절히 관리하기 위해 준수해야 할 지침을 체계화한 것	4가지 영역(프로세스 관리, 프로젝트 관리, 공학 지원)에 따라 정의된 5레벨의 역량성숙도로 시스템 평가	몇 개의 나라들의 정부기관에서는 소프트웨어 개발계약에 있어 지원업체에게 레벨 3 기준을 기본으로 요구하고 있는 실정임
SPICE	국제 표준화 기구 (ISO)	소프트웨어 품질 표준화 심사 평가 모형으로 소프트웨어 프로세스 전반을 망라하여 심사를 하고 그 결과에 따른 조직의 프로세스를 개선하여 나가는 활동에 대한 표준화방법	프로세스 차원은 5개의 카테고리로 구분하고, 세부 프로세스는 40개로 정의함. 각 수준별 측정 관점에 따라 0에서부터 5까지의 범위를 가지는 6개의 수준으로 시스템 평가함	CMMI보다 성공하지 못하고 있고, 한국형 SPICE모델인 KSPICE에 대한 지속적인 연구가 이루어지고 있는 실정임 인증서 취득 위주의 형식적인 인증획득의 경향이 있음

5. 결론

정보보호관리기법을 분석은 개별 정보보호관리기법이 보다 보완될 수 있고, 각 제도가 서로 연계하는데 도움을 준다. 그러나 위의 분석만으로는 완벽한 연계와 보완이 어려우며, 서로 연관된 부분이 존재하지만 현 상황에서 각 방법론들을 연계하기 위해서는 쉽지 않을 것으로 판단된다. 본 연구는 국내외에 존재하는 정보보호관리기법을 이해하고, 각 제도의 차이점과 공통점의 분석은 비즈니스 위험관리 기법으로 활용할 수 있는 토대가 된다.

정보보호관리기법은 정보보호에만 초점을 두지 않고, 조직의 업무 처리 프로세스, 인사, 업무, 프로세스 등에 광범위하게 초점을 두고 있다. 따라서 정보보호관리기법은 비즈니스 위험관리에 사용될 수 있는 적절한 대안이다.

본 연구는 정보보호관리기법을 프로세스 측정, 프로세스 관리, 정보보호관리 등의 관점에서 분석한다. 비즈니스 위험관리는 비즈니스 프로세스, 비즈니스 프로세스의 성숙도, 정보보호관리의 관점에서 정의될 수 있다. 따라서 본 연구가 채용한 분석 프레임웍은 비즈니스 위험관리 프레임웍 개발에 유용하게 사용될 수 있다.

참고문헌

[1] 한국정보사회진흥원, 정보시스템감리점검해설서(안) V3.0, 2004.

[2] 한국정보보호진흥원, 정보보호관리체계 관리과정 가이드, 2003.

[3] 한국정보보호진흥원, 정보보호관리체계 위험관리 가이드, 2004.

[4] 한국정보보호진흥원, 정보보호관리체계 인증준비 가이드, 2005.

[5] 한국정보보호진흥원, 정보보호관리체계인증, http://www.kisa.or.kr/index.jsp

[6] Carnegie Mellon Software Engineering Institute, Capability Maturity Model Integration(CMMI), Version1.1, 2002.

[7] IT Governance Institute, COBIT 4.0.

[8] Information technology – Security techniques – Information security management systems – Overview and vocabulary, ISO/IEC 2009.

[9] ISO/IEC 12207 Amendment 1, Information Technology - Software Life Cycle Processes, May 1, 2002.

[10] http://www.dnv.co.kr/binaries/BS7799 description, tcm34-89786.pdf. pp. 1~4 (BS7799 정보보호경영시스템).

김 민 선(Min Sun Kim) **[정회원]**

- 1990년 2월 : 이화여자대학교 대학원 경영학과 (경영학석사)
- 2006년 2월 : 이화여자대학교 대학원 경영학과 (경영학박사)
- 1995년 9월 ~ 2006년 2월 : 이화여자대학교 지식정보화전략연구센터 책임연구원
- 2009년 9월 ~ 현재 : 협성대학교 유통경영학과 교수

<관심분야>
E-business, IT 서비스관리, IT 거버넌스, EA/ITA 등