정보보호 거버넌스 프레임워크 개발에 관한 연구

이 성 일* · 황 경 태**

A Research on the Development of Information Security Governance Framework

Seong il Lee* · Kyung Tae Hwang**

Abstract

Enormous losses of shareholders and consumers caused by the risks threatening today's business (e.g., accounting fraud and inside trading) have ignited the necessity of international regulations on corporate ethics and internal control, such as Basel II and SOX. Responding to these regulations, companies are establishing governance system, applying it consistently to the core competency of the company, and increasing the scope of the governance system. Recently occurred security related incidents require companies to take more strict accountability over information security. One of the results includes strengthening of legislation and regulations. For these reasons, introduction of information security governance is needed. Information security governance governs the general information security activities of the company (establishment of information security management system, implementation of information security solutions) in the corporate level.

Recognizing that the information security is not restricted to IT domain, but is the issue of overall business, this study develops information security governance framework based on the existing frameworks and systems of IT governance. The information security governance framework proposed in the study include concept, objective, and principle schemes which will help clearly understand the concepts of the information security governance, and execution scheme which will help implement proper organization, process and tools needed for the execution of information security governance.

Keywords : Information Security, Information Security Governance, Corporate Risk

논문접수일 : 2011년 05월 11일 논문게재확정일 : 2011년 06월 07일

* Ernst&Young Advisory ITRA Manager, e-mail : seong-il.lee@kr.ey.com
** 교신저자 : 동국대학교 경영대학 경영정보학과 교수, e-mail : kthwang@dongguk.edu

1. 연구의 배경 및 목적

기업의 리스크 관리에 대한 최근 동향을 보면, 전통적인 운영 리스크뿐만 아니라 기업 핵심 기술의 경쟁사 유출로 인한 비즈니스 경쟁력 상실 및 지식에 대한 손실 또한 심각한 문제로 인식되고 있다[OECD, 2004].

이러한 인식으로 인해 IT 관련 정보보호 뿐만 아니라 핵심 정보 유출 같은 비즈니스 차원의 정보보호에 초점을 둔 정보보호 관리의 중요성이 강조되고 있지만, 대부분의 국내 기업들은 정보보호를 단순히 기술적 이슈로 인식하고 있으며, IT 부서 내에 정보보호 담당 조직을 운영하고 있다. 이러한 환경에서 정보보호 이슈를 경영의 이슈와 연계하여 최고 경영진의 관심과 지지를 확보하고 전사 차원의 노력을 집중하는 것은 현실적으로 어려운 상황이다[한국정보사회진흥원, 2008a].

하지만, 최근 발생한 고객 개인정보 유출 사고와 내부 기밀정보 유출 사고 등 기업의 경영과 직접적으로 연관된 보안 사고는 정보보호가 단순히 IT 인프라에 국한된 이슈가 아닌 기업의 경영과 관련된 중요 이슈임이 증명되었다[한국정보사회진흥원, 2008b].

이러한 최근의 현안은 기업의 비즈니스 운영을 위협하는 리스크가 회계 부정, 횡령 같은 전통적인 운영 리스크 뿐만 아니라 보다 다양하고 광범위하게 존재함을 의미하며, 이로 인해 IT 담당 임원과 IT 부서에 한정적인 기존 대응 방식의 전반적인 개선을 요구하고 있다. 따라서 중요 정보 유출 등 최근 정보보호 이슈를 효과적으로 해결하기 위해서는 IT 담당 임원만이 아니라 모든 경영층의 관심과 지지를 기반으로 전사적 리스크 관리 노력, 보고 체계 수립, 책임성 확보 등을 강조하는 거버넌스 체계가 정보보호 분야에 도입되어야 함을 의미한다.

IT 분야의 경우, 국제 표준화 기구에서는 "ISO/IEC 38500 : Corporate Governance of IT(정보기술에 대한 기업 거버넌스)"를 제정하여 IT 거버넌스의 개념 및 프레임워크를 정의하고 있다. 동 표준에서는 IT 운영 위험의 일부로서 정보보호를 언급하고 있지만 비즈니스 레벨에서의 정보 유출에 대한 언급은 하지 않고 있다.

따라서 본 논문에서는 정보보호를 IT와 Non-IT 영역을 총망라한 기업의 전사적 거버넌스 대상으로 관리할 수 있는 정보보호 거버넌스 프레임워크를 제시하고자 한다.

본 논문의 구성은 다음과 같다.

첫째, 정보보호 거버넌스 프레임워크 개발을 위한 이론적 배경을 고찰하고, 정보보호 거버넌스 프레임워크의 필요성에 대해 살펴본다. 둘째, 정보보호 거버넌스 프레임워크의 개발 과정 및 방법을 서술하고, 본 연구에서 수립한 정보보호 거버넌스 프레임워크에 대해 설명한다. 셋째, 정보보호 분야 전문가들과의 포커스 면담을 통해 본 연구에서 제시한 정보보호 거버넌스 프레임워크의 필요성과 실현 가능성을 검증한다. 마지막으로 연구 결과를 종합하여 결론과 연구의 한계, 향후 연구 방향을 제시한다.

2. 이론적 배경

본 장에서는 기업 거버넌스, IT 거버넌스, 정보보호 거버넌스를 포함한 거버넌스의 개념, IT 거버넌스 프레임워크 등에 대한 이론적인 배경을 살펴보고, 정보보호 거버넌스 프레임워크의 필요성에 대해 알아본다.

2.1 거버넌스의 개념과 정의

2.1.1 거버넌스의 개념

어의학적으로 거버넌스는 그리스어인 Kuberman에서 중세라틴어인 gubernare로 이어졌는데, 이것은 조종(piloting), 규칙제정(rule making), 키잡이(steering)와 동일한 의미를 지니고 있다.

Hodges은 거버넌스를 의사결정, 성과, 조직 통제와 관련된 절차로서, 조직에 전반적인 방향을 부여하기 위한 구조를 제공하고 외부의 이해관계자들이 갖고 있는 합리적인 책임감(accountability)에 대한 기대를 만족시키는 개념으로 제시하고 있다[Hodges et al., 1996].

Daft는 거버넌스를 조직을 지시, 통제 및 관리 과정으로 보고 있다[Daft, 1989].

Ljungqvist는 조직의 생존과 복지(well-being)를 위한 이사회의 책임을 거버넌스의 개념으로 제시하고 있으며, 거버넌스 활동은 관리(management), 감독(supervision)의 개념과는 구분되는 것이라고 주장하였다[Ljungqvist, 1999].

Baker는 거버넌스의 개념이 거버넌스 책임과 거버넌스 구조가 혼동되어 사용되고 있음을 지적하고 있다[Baker, 1992].

선행 연구들을 요약해 보면, 거버넌스를 설명하기 위해 <표 1>과 같이 의사결정권한, 책임성, 조직 통제, 지시, 성과 모니터링, 관리와의 구분 등 6가지 핵심 개념을 정의하고 있는데, 본 연구에서는 이를 '개념 요건'과 '실행 요건'으로 구분하였다.

개념 요건이란 정보보호 거버넌스의 개념 체계를 구현하기 위한 요건으로, 실행 요건이란 정보보호 거버넌스의 실행 체계를 구성하기 위한 요건으로 정의하였다.

〈표 1〉 거버넌스 개념의 핵심 요소

구 분	거버넌스의 개념	연구자
개념 요건	책임성	Hodges, Baker
	관리와의 구분	Alexander, Baker
	조직통제	Hodges, Daft, Alexander
실행 요건	의사결정권한	Hodges, Daft, Alexander, Baker
	지시	Hodges, Daft, Baker
	성과모니터링	Hodges, Alexander

2.1.2 기업 거버넌스의 정의

OECD(Organization for Economic Cooperation and Development) 원칙에 따르면 기업 거버넌스는 "경영층, 이사회, 주주, 기타 이해관계자들 간의 관계를 포함하며, 또한 기업 전략 목표의 설정, 목표 달성 방법, 성과 모니터링을 위한 체계를 제공한다."로 정의되어 있다[OECD, 2004].

ITGI(Information Technology Governance Institute)에서는 "기업 거버넌스란 전략적 방향 제시를 목적으로 이사진과 최고 경영층이 기업의 목표 달성과 적절한 위험 관리가 이루어지도록 하고, 책임성 있는 자원 관리를 검증하기 위한 일련의 수행 방법 및 책임을 의미한다."로 기업 거버넌스를 정의하였다.

기업 거버넌스의 개념을 정의한 선행연구에서는 이해관계자, 전략목표 연계, 책임성, 목표 달성 방법, 성과 모니터링, 위험 관리 및 자원 관리 등의 7가지 세부 항목이 활용되었는데, 본 연구에서는 이를 개념 요건, 목표 요건 및 실행 요건의 3가지로 구분하여 <표 2>와 같이 정리하였다.

'개념 요건'과 '실행 요건'은 앞서 정의한 바와 같고, '목표 요건'은 정보보호 거버넌스의 목표 체계를 구현하기 위한 요건을 말한다.

〈표 2〉 기업 거버넌스 개념의 핵심요소

구 분	기업 거버넌스 개념	연구자
개념 요건	이해 관계자 관계	Hodges, OECD
목표 요건	전략 목표 연계	OECD, ITGI
	책임성	Hodges, OECD, ITGI
실행 요건	목표달성 방법	OECD, ITGI
	성과 모니터링	Hodges, OECD
	위험관리	Hodges, ITGI
	자원관리	ITGI

<표 2>의 핵심 요소 중 “책임성”은 <표 1>의 거버넌스 개념에 관한 선행 연구 정리에서는 개념 요건에 포함되었으나, 기업 거버넌스 관련 선행 연구에서는 책임성의 개념이 보다 구체화되어 기업 거버넌스 활동을 위한 목표로서 제시되어 있으므로 목표 요건으로 구분하였다.

위험 관리와 자원 관리의 경우, 정보보호 영역에서는 정보보호관리 체계 활동을 통해 수행되며, 정보보호관리 체계 국제표준인 ISO/IEC 27001을 통해 정보보호를 위한 위험 관리와 자원 관리 활동의 세부 요건이 정의되었다[ISO/IEC, 2005].

따라서 정보보호 영역에서는 정보보호관리 체계를 대상으로 한 거버넌스 활동이 필요한 것으로 판단된다.

2.1.3 IT 거버넌스의 정의

정보기술에 대한 의존도가 높아짐에 따라 IT의 효율적인 관리에 보다 많은 관심이 집중되었고, 1990년대 이후 기업 거버넌스의 구현을 위한 관련 법규, 프레임워크 및 표준이 제정되는 과정에서 IT를 거버넌스 대상으로 포함하게 되었다. 2008년 제정된 국제 표준인 ISO/IEC 38500(IT 거버넌스 표준)에서는 IT 거버넌스를 조직의 이사회 및 최고 경영층이 IT가 효율적이고, 효과적이며, 책임성 있게 활용될 수 있도록 평가, 지시, 감독하는 체계로 정의하였다[ISO/IEC, 2008].

Weill and Ross는 IT 거버넌스를 ‘IT의 사용에 있어 바람직한 행위를 촉진하기 위해 의사결정권한과 책임소재의 틀을 규정하는 것’으로 정의하고 있다[Weill et al., 2004].

가트너는 “IT 거버넌스의 핵심 성과는 비즈니스 가치로 대변되는 효율성과 효과성을 측정하는 것으로 의사결정 권한과 책임성을 나타내는 프레임워크를 구체화함으로써 바람직한 IT 활용을 유도하기 위한 프로세스”라고 설명하고 있다[Gartner, 2006].

IT 거버넌스는 기업 거버넌스의 틀 안에서 작동하기 때문에 IT 거버넌스의 개념을 정의한 선행 연구는 개념 자체를 설명하는 것보다 IT 거버넌스의 목표와 활동을 중심으로 개념을 정의하고 있다[이정훈 등, 2007; Lee et al., 2008].

IT 거버넌스의 개념을 정의한 선행 연구들의 핵심 요소는 <표 3>과 같다. 본 연구에서는 IT 거버넌스 개념에 대한 선행 연구에서 제시한 6가지 핵심 요소를 ‘목표 요건’과 ‘실행 요건’으로 재 구분하였다.

〈표 3〉 IT 거버넌스 개념의 핵심 요소

구 분	IT 거버넌스의 정의	연구자
목표 요건	책임성	ISO, Weill and Ross, 가트너
	비즈니스 기여	Weill and Ross, 가트너
실행 요건	의사결정 권한	Weill and Ross, 가트너
	평가	ISO, 가트너
	지시	ISO
	감독 (성과 모니터링)	ISO, Weill and Ross, 가트너

2.1.4 정보보호 거버넌스의 정의

정보보호 거버넌스에 대한 선행 연구에서는 정보보호 거버넌스의 개념을 설명하기 위해 IT 자산 보호에 초점을 둔 거버넌스 보다는 비즈니스 전략과 연계한 전사 차원의 접근 방법을 주장하고 있다.

NIST(National Institute of Standards and Technology) SP 800-100에 의하면, 정보보호 거버넌스는 “위험관리 노력의 일환으로, 정보보호 전략이 비즈니스 목표와 연계되고 이의 달성을 지원하

며, 정책과 내부통제를 통해 관련 법규와 규정을 준수하도록 하고, 책임을 할당하기 위한 프레임워크와 이를 위한 경영 구조 및 프로세스를 수립하는 과정"으로 정의되었다[NIST, 2007].

ITGI에서는 정보보호 거버넌스를 "전략적 방향을 제시하고, 목표가 달성되도록 하며, 적정하게 위험을 관리하고, 책임감 있게 조직의 자원을 사용하며, 전사적 보안 프로그램의 성공 정도를 모니터링 하는 기업 거버넌스의 일부"라고 정의하고 있다[ITGI, 2002].

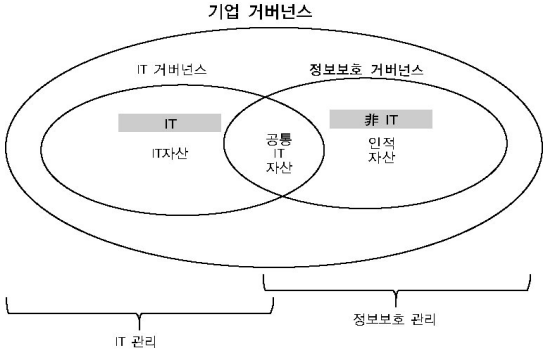
또한 CMU(Carnegie Mellon University)에서는 정보보호 거버넌스를 "조직의 일상적 활동(신뢰, 행위, 능력, 행동)내에 보안 문화(사용자 인식 및 참여와 연계)를 수립하고 지속시키기 위한 지시 및 통제 행위"라고 정의하고 있다[Westby et al., 2007].

선행 연구에서는 정보보호 거버넌스의 개념을 정의하는데 9개의 핵심 요소를 활용하고 있고, 본 연구에서는 이를 '개념 요건', '목표 요건' 및 '실행 요건'으로 재 구분하였다(<표 4> 참조).

〈표 4〉 ISG 개념의 핵심 요소

구 분	정보보호 거버넌스의 정의	연구자
개념 요건	전사 위험관리와 연계	NIST, ITGI,
목표 요건	책임성	NIST, ITGI, CMU
	비즈니스 목표와 연계	NIST, CMU
	컴플라이언스	NIST, ITGI
실행 요건	목표 달성 방법	NIST, ITGI, CMU
	경영층의 참여	NIST, ITGI, CMU
	지시	CMU
	성과 모니터링	ITGI
	내부통제 활용	NIST

정보보호 거버넌스의 개념을 정의한 선행 연구는 정보보호 거버넌스가 수행해야 할 최소한의 요건만을 정의하고 있으나, 기업 및 IT 거버넌스와의 관계를 고려한 전체적인 관점의 연구는 미흡하다. 따라서, 본 연구는 다음의 <그림 1>과 같이 정보보호 거버넌스의 위상을 고려한 프레임워크를 제시하고자 한다.



〈그림 1〉 기업, IT, 정보보호 거버넌스의 관계

정보보호는 IT 보안이 다루지 않는 Non-IT 자산(종이 문서, 이미지 등)에 대한 보호까지 포함하고 있으므로 IT 거버넌스와 공통된 영역 외에 별도의 부문이 존재한다. 따라서 정보보호 거버넌스는 <그림 1>과 같이 기업 거버넌스의 핵심적인 일부분으로서 IT 거버넌스와의 연계성은 인정하지만 별도 영역으로 간주해야 한다[김정덕, 2009].

정보보호 거버넌스 개념을 재정립하기 위해서는 <그림 1>에 나타난 관계를 고려해야 하므로 기업 거버넌스의 전체적인 틀에서 정보보호 거버넌스의 위상과 IT 거버넌스와의 차별화를 위해 다음과 같은 사항을 고려해야 한다.

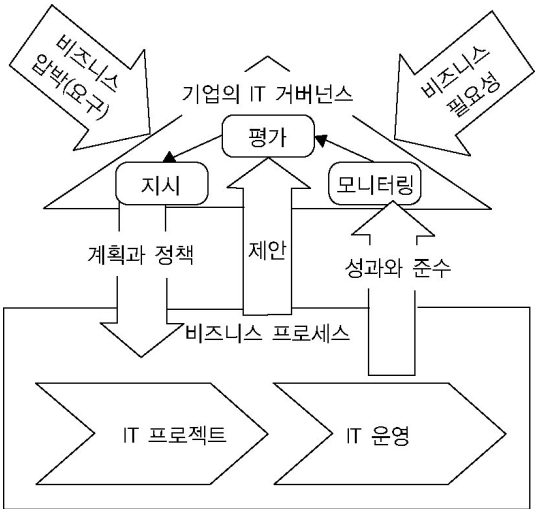
첫째, 기업 거버넌스의 틀 안에서 정보보호 거버넌스가 작동되어야 한다는 점을 명시해야 한다.

둘째, 정보보호 거버넌스의 목표를 명시해야 한다. 선행 연구에서 제시하고 있는 정보보호 거버넌스의 개념은 정보보호 거버넌스의 개념, 목표, 활동이 혼재되어 있고 거버넌스 대상을 IT와 Non-IT로 구분하지 않으므로 IT 거버넌스와의 중복 이슈 등이 발생하고 있다. 이러한 이슈를 해결하기 위해서는 정보보호 거버넌스의 목표를 달성하기 위한 정보보호 활동과 활동 대상을 명확하게 개념 정의에 표현해야 한다.

2.2 IT 거버넌스 프레임워크

본 연구에서는 IT 거버넌스 프레임워크에 대한 선행 연구를 고찰하여 정보보호 거버넌스 프레임워크의 구조를 수립하는데 참조하였다.

ISO/IEC 38500에서 제시하고 있는 IT 거버넌스 프레임워크는 개념, 목표, 원칙, 활동 등으로 거버넌스의 체계를 정형화하고 있다. 동 표준에서는 IT 거버넌스 활동을 '평가'(Evaluate), '지시'(Direct), '모니터링'(Monitor)의 세 가지 유형으로 제시하고 있다(<그림 2> 참조).



〈그림 2〉 ISO/IEC 38500의 ITG 프레임워크

<그림 2>에 나타난 세 가지 활동 중, '평가'는 비즈니스의 IT 활용에 대한 제안과 대안을 평가하는 활동이고, '지시'는 구체적 IT 계획과 정책의 수립과 집행을 지시하고 통솔하는 활동이며, 모니터링은 IT 활동의 '성과'와 '준수'를 감독하는 활동이다[ISO/IEC, 2008].

Simonsson and Johnson은 IT 거버넌스를 주로 정보자산에 대한 의사결정과 관련된 것으로 정의하고, 도메인, 의사결정 프로세스, 범위의 세 차원으로 분류한 프레임워크를 제시하였다[Simonsson et al., 2006].

Webb and Pollard 등은 IT 거버넌스란 효과적인 IT 통제, 책임 및 권한의 적절한 배분, 성과 관리, 위험 관리의 지속적인 개발과 유지를 통해 기업의 목표와 IT를 전략적으로 연계시키는 것이라는 점을 강조하며, 거버넌스 프레임워크의 구성요소를 '구조', '통제 프레임워크', '프로세스'로 분류하여 제시하였다[Webb et al., 2006].

이정훈, 전성현, 황경태는 기존 관점을 통합한 진화된 IT 거버넌스 프레임워크를 제시하였다. IT 거버넌스는 기준을 제공하는 개념 체계, 목적 체계, 원칙 체계와 IT 거버넌스의 대상 및 실행 방법인 실행 체계로 구성된다[이정훈 등, 2007].

이정훈 등(2007)의 IT 거버넌스 프레임워크는 다른 선행 연구를 종합한 보다 진화된 프레임워크를 제시하여, IT 거버넌스의 선행 연구를 일원화된 관점에서 참조할 수 있다.

이정훈 등(2007)의 IT 거버넌스 프레임워크 구조를 정보보호 거버넌스에 적용하기 위한 방안은 다음의 <표 5>와 같다.

〈표 5〉 IT 거버넌스 프레임워크 구조 및 정보보호 거버넌스 적용방안

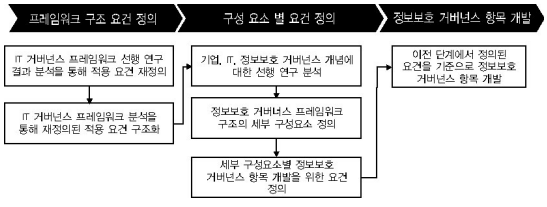
구조	적용방안		연구자
개념 체계	정보보호 거버넌스의 구조 및 통제 프레임워크에 대한 설명 필요		Webb and Pollard ISO38500
목적 체계	정보보호 거버넌스 구현 목표 정의		Simmonson and Jonhnson ISO38500 Webb and Pollard
원칙 체계	거버넌스 구현 목표 달성을 위한 원칙 정의		ISO38500
실행 체계	프로세스	거버넌스 실행을 위한 세부 절차	Simmonson and Jonhnson Webb and Pollard ISO38500
	조직	거버넌스 실행의 주체 정의	Simmonson and Jonhnson ISO38500
	도구	거버넌스 실행지원 수단	Simmonson and Jonhnson

2.3 정보보호 거버넌스 프레임워크의 필요성

정보보호 거버넌스를 조직에 구현하기 위한 구조와 적용 요건, 적용 항목을 프레임워크 형태로 제시한 연구는 활발히 이루어지고 있지 않다. <그림 1>에 나타난 정보보호 거버넌스의 위상을 고려하면 정보보호 거버넌스가 조직에 효과적으로 적용되기 위해서는 기업 거버넌스 프레임워크의 틀 내에서 IT 거버넌스와 구조를 공유할 수 있는 정보보호 거버넌스 프레임워크가 개발되어야 한다[김정덕, 2009]. <그림 1>에 나타난 정보보호 거버넌스의 위상을 기준으로 IT 거버넌스와 정보보호 거버넌스가 IT 보안이슈를 효과적으로 공유하고, 정보보호 거버넌스에서 Non-IT 보안 이슈를 IT 보안 이슈와 동등한 수준으로 다루도록 하기 위해서는 정보보호 거버넌스 프레임워크를 개발할 때 IT 거버넌스 프레임워크 구조를 적용하여 조직 거버넌스 활동과의 일관성을 확보할 필요가 있다.

3. 정보보호 거버넌스 프레임워크의 개발 방법

정보보호 거버넌스 프레임워크의 개발은 (1) 프레임워크의 구조 요건 개발, (2) 구성 요소별 요건 정의, (3) 정보보호 거버넌스 항목 개발의 단계로 진행된다(<그림 3> 참조).



〈그림 3〉 정보보호 거버넌스 프레임워크의 개발 단계

3.1 정보보호 거버넌스 프레임워크의 구조 요건 정의

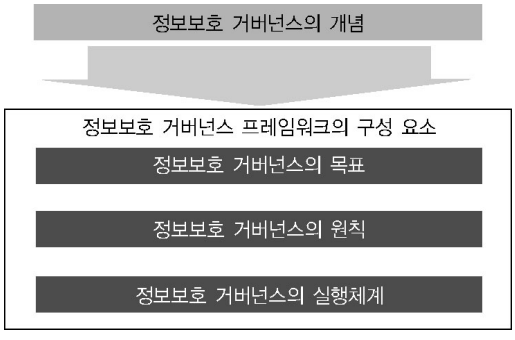
본 연구에서는 정보보호 거버넌스 프레임워크의 구조에 대한 요건을 다음과 같이 정의한다(<표 6> 참조).

〈표 6〉 정보보호 거버넌스 프레임워크의 구조 요건

ITG		ISG 적용요건	연구자
개념 체계		정보보호 거버넌스 개념 정의	Webb and Pollard ISO38500
목적 체계		정보보호 거버넌스의 목표 정의	Simmonson and Jonhnson ISO38500 Webb and Pollard
		법, 규제에 대한 준수 필요성	정보보호 영역의 특성에 따라 추가
원칙 체계		목표 달성을 위한 원칙 정의	ISO38500
실행 체계	조직	실행 주체의 정의	Simmonson and Jonhnson Webb and Pollard ISO38500
	프로세스	실행 프로세스 정의	Simmonson and Jonhnson ISO38500
	도구	실행을 위한 수단 정의	Simmonson and Jonhnson ISO38500

<표 6>에 나타난 바와 같이 정보보호 거버넌스 프레임워크는 IT 거버넌스 프레임워크의 구조를 원용하고 있지만, 목적 체계의 구성 요소인 '법, 규제에 대한 준수 필요성'은 현재 정보보호 규제 추세와 선행 연구(NIST, ITGI)의 목적 요건을 정보보호 거버넌스의 주요 목적으로 반영하기 위해 새로운 구성 요소로 추가하였다.

<표 6>의 구조화 요건에 따라 정보보호 거버넌스 프레임워크의 구조는 다음과 같이 정의하였다(<그림 4> 참조).



〈그림 4〉 ISG 프레임워크의 구조

<그림 4>에서 첫 번째 영역은 정보보호 거버넌스의 개념을 정립하는 영역이다. 정보보호 거버넌스는 무엇을 대상으로 하며 어떤 활동으로 이루어지는가를 명시하고, 이를 기존의 정보보호 활동들과 구별한다[한국정보사회진흥원, 2008a; 이정훈 등, 2007].

두 번째 영역은 정보보호 거버넌스의 목표를 명시하는 영역이다. 정보보호 거버넌스를 통해 얻고자 하는 효과가 무엇인지를 도출하고, 세부 목표들 간의 관계를 명시한다[한국정보사회진흥원, 2008a; 이정훈 등, 2007].

세 번째 영역은 정보보호 거버넌스의 원칙을 수립하는 영역이다. 앞서 명시된 정보보호 거버넌스 목표는 구체적인 정보보호 거버넌스 원칙의 형태로 정리되며, 이 원칙은 정보보호 거버넌스의 목표와 구현 수단을 연결하는 고리가 된다[한국정보사회진흥원, 2008a; ISO/IEC, 2005; 이정훈 등, 2007].

네 번째 영역은 정보보호 거버넌스의 실행체계를 설계하는 영역이다. 위에서 제시된 정보보호 거버넌스 원칙을 구현하는 제반 활동을 식별하고, 이를 수행하는 조직 구조 및 수단을 설계하는 영역이다[한국정보사회진흥원, 2008a; 김정덕, 2009].

3.2 정보보호 거버넌스의 개념 및 목표 정의 요건

정보보호 거버넌스의 개념을 활동의 내용에 따라 판단하는 것은 정보보호 분야의 실제 상황을 적용해 보면 상당한 혼란을 야기하게 된다[이정훈 등, 2007].

따라서 본 논문에서는 <표 7>과 같이 정보보호 거버넌스의 개념 요건과 목표 요건을 기반으로 하여 정보보호 거버넌스의 목표를 우선 정의하고, 이로부터 정보보호 거버넌스의 개념을 정의한다.

〈표 7〉 정보보호 거버넌스의 개념 및 목표 요건

구 분	요건정의	연구자
개념 요건	이해 관계자 관계	Hodges, OECD
	책임성	**Hodges, Baker**
	관리와 구분	Alexander, Baker
	조직 통제	Hodges, Daft, Alexander
	전사 위험관리와 연계	NIST, ITGI,
목표 요건	전략 목표 연계	**OECD, ITGI**
	책임성	Hodges, OECD, ITGI
	비즈니스 목표와 연계	**NIST, CMU**
	컴플라이언스	NIST, ITGI

<표 7>에서 볼 수 있는 바와 같이, 선행 연구의 개념 및 목표 요건을 통합한 결과 중복된 요

건 1건과 유사 요건 1건이 발견되었다. “책임성” 요건은 “정보보호 활동 결과에 대한 책임 소재를 분명히 해야 한다”는 취지이므로 정보보호 거버넌스 구현을 위한 개념이라기보다는 정보보호 거버넌스 구현 시 달성해야 할 목표로서 내용을 보정하였다. “전략 목표 연계”와 “비즈니스 목표와 연계” 요건은 공통적으로 정보보호와 비즈니스의 연계성 확보를 요구하는 요건이므로 “비즈니스 연계성” 요건으로 통합하였다.

<표 8>은 정보보호 거버넌스의 개념 및 목표 정의를 위해 <표 7>의 중복 및 유사 요건을 정리한 내용이다.

〈표 8〉 개선된 정보보호 거버넌스의 개념 및 목표 요건

구 분	요건정의		연구자
개념 요건	이해 관계자 관계	거버넌스의 주체가 되는 이해관계자 식별, 관계정의	Hodges, OECD
	관리와의 구분	정보보호 관리 활동과 거버넌스 활동의 명확한 구분	Alexander, Baker
	조직 통제	거버넌스 활동은 조직 통제를 위해 전사적인 영향력을 가져야 함	Hodges, Daft, Alexander
	전사 위험관리와 연계	정보보호 거버넌스는 기업 거버넌스의 틀 내에서 IT 거버넌스의 위험관리와 연계해야 함	NIST, ITGI,
목표 요건	책임성	거버넌스 주체의 정보보호 활동 실행과 결과에 따른 책임확보 필요	Hodges, OECD, ITGI
	비즈니스 연계성	비즈니스 목표에 따라 정보보호 전략수립 및 연계	NIST, CMU
	컴플라이언스	정보보호 관련 법, 제도를 준수해야 함	NIST, ITGI

3.3 정보보호 거버넌스의 원칙 요건

선행 연구를 분석한 결과, 정보보호 거버넌스에 적용 가능한 원칙 요건을 별도로 구분할 수 있는 수준으로 상세히 제시한 연구 결과는 미흡하였다. 그러나 이정훈, 전성현, 황경태의 연구는 ISO/IEC 38500에서 제시하고 있는 7개의 일반 원칙을 포함하여 원칙의 구조, 거버넌스 목표와 실행 체계를 연계하는 원칙의 역할 등을 상세히 기술하였다[이정훈 등, 2007].

정보보호 거버넌스 프레임워크 구조요건(<표 6> 참조)에 따르면 원칙은 정보보호 거버넌스의 개념 및 목표에 따라 거버넌스 활동을 실행하기 위한 매개체의 역할을 수행하는 중요한 요건이므로 ISO/IEC 38500의 원칙까지 포괄하고 있는 이정훈 등[2007]의 IT 거버넌스 원칙 구조를 참조하였다.

이정훈 등[2007]의 IT 거버넌스 원칙 요소를 정보보호 거버넌스 영역에 적용하기 위한 요건은 다음의 <표 9>와 같다.

〈표 9〉 정보보호 거버넌스 원칙 요건

구 분	적용 요건
공동원칙	IT 거버넌스에서는 ISO38500의 원칙을 원용하고 있으나 정보보호 거버넌스는 ISO에서 표준화가 진행 중이므로 향후 연구를 통해 원칙을 보완해야 함
전제조건 원칙	정보보호 거버넌스 목표 별 전제되어야 하는 사항을 원칙으로 정의
활동 원칙	정보보호 부문에 적합한 형태로 변형 필요 리스크 분석 및 관리는 정보보호 부문에서는 기본 활동이므로 정보보호 분야에서는 활동 원칙과 통합하여 일반 원칙으로 구성
리스크 관련 원칙	

3.4 정보보호 거버넌스 실행체계 요건

정보보호 거버넌스의 실행 체계란 정보보호 거버넌스 목표와 원칙을 놓고, 이들을 구현하기 위해 기업이 수행하는 제반 활동 및 이를 위한 각종 수단들 간의 관계를 체계적으로 명시하는 틀이다[한국정보사회진흥원, 2008a; 김정덕, 2009].

기업, IT, 정보보호 거버넌스에 대한 선행 연구 분석을 통해 실행체계의 항목을 정의하기 위한 요건을 정리하여 <표 6>의 정보보호 거버넌스 구조 요건에 반영한 결과는 다음의 <표 10>과 같다.

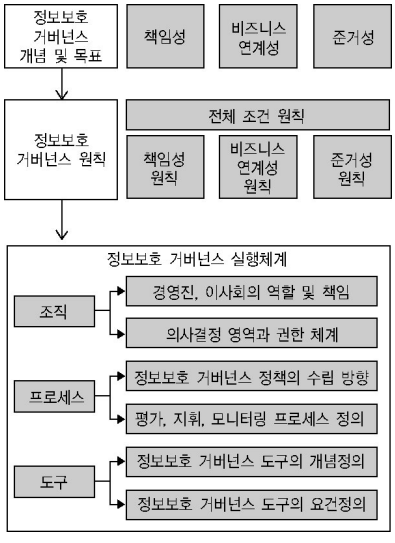
〈표 10〉 정보보호 거버넌스 구조 요건에 따른 실행체계 요건 정의

요건 정의			연구자
조직	의사결정 권한	거버넌스 활동의 수행을 위한 거버넌스 주체의 권한	Hodges, Daft, Alexander, Baker
	경영층의 참여	경영층이 정보보호 거버넌스의 주체가 되어야 함	NIST, ITGI, CMU
프로세스	평가	정보보호 활동의 효율성과 효과성 평가	ISO, 가트너
	지시	거버넌스 목표 달성을 위해 거버넌스 활동을 지시	Hodges, Daft, Baker, ISO
	성과 모니터링	거버넌스 주체는 정보보호 활동의 성과를 지속적으로 모니터링	Hodges, Alexander, ISO
도구	목표달성 방법	정보보호 거버넌스 목표 달성을 위한 수단 및 도구의 정의 필요	OECD, ITGI
	내부통제 활용	거버넌스 수단으로서 내부통제 활용	NIST

<표 10>을 정리하는 과정에서 선행 연구에서 실행체계 항목으로서 정의된 위험 관리와 자원 관리는 <표 8>의 개념 요건에서 관리와 거버넌스의 구분이 요구되는 관계로 삭제되었다. 정보보호관리체계 국제 표준인 ISO/IEC 27001의 도메인에 포함된 위험 관리와 자원 관리는 거버넌스 활동이 아니라 대상이며 평가, 지시, 성과 모니터링의 거버넌스 활동을 통해 해당 관리체계의 운영 적정성을 파악할 수 있다.

4. 정보보호 거버넌스 프레임워크 항목 개발

정보보호 거버넌스 프레임워크 항목 개발은 정보보호 거버넌스 프레임워크 구조 요건의 틀 내에서 프레임워크의 세부 항목을 정의하는 과정이다(<그림 5> 참조).



〈그림 5〉 ISG 프레임워크와 세부 구성 항목

4.1 정보보호 거버넌스의 목표와 개념 정의

정보보호 거버넌스 목표 정의 요건에 따라 정보보호 거버넌스의 목표를 아래의 세 가지 사항으로 정의하였다(<표 8> 참조).

- 책임성(Accountability) : '정보보호 활동의 성과에 대해 누가 책임을 지는가?'
- 비즈니스 연계성(Business Alignment) : '정보보호 활동이 기업의 비즈니스 목표 달성에 기여하는가?'
- 준거성(Compliance) : '정보보호 활동이 원칙과 기준(법, 제도, 기업 내부의 규정 등)'에 따라 수행되는가?'

기업 거버넌스 측면에서 주장하는 책임성의 목표는 기업 경영 활동에 대해 궁극적으로 누가 어떻게 책임을 지느냐의 문제이다. 이러한 틀을 고려할 때 정보보호 거버넌스에서의 책임성 목표는 기업 내에서 정보를 보호해야 하는 역할과 책임을 명확히 결정하는 것이다. 이러한 역할과 책임의 명확한 정의는 기업 IT의 기획에서 운영까지 역할 및 책임을 요구하는 IT 거버넌스에서의 책임성 목표와도 연계될 수 있다.

기업 및 IT 거버넌스에서 효과성을 목표로 하고 있다면 정보보호 거버넌스에서는 내재된 원천적 제약사항을 극복하기 위해 비즈니스 연계성을 목표로 해야 한다. 기업 거버넌스 측면에서 효과성은 기업 경영 활동이 기업 목표 달성에 얼마나 효과적으로 기여하는가를 고려하는 문제이다. IT 거버넌스에서 효과성은 기업의 IT가 기업의 경영 활동을 얼마나 효과적으로 지원하느냐를 고려하는 문제이다. 반면, 효과적인 정보보호는 철저한 통제를 의미하지만 철저한 통제는 오히려 기업의 경영활동을 저해하는 요인이 될 수도 있다. 따라서 정보보호 거버넌스에서 효과성의 목표는 비즈니스와 연계될 수 있는 정보보호 통제를 구현해야 하는 목표를 지향하며 이것은 효과성이 아닌 비즈니스 연계성으로 표현될 수 있다.

기업 및 IT 거버넌스에서 투명성은 활동이 공정한 절차와 규칙을 준수하면서 투명하게 수행되고 있는가의 문제이다. 하지만 정보보호에서 투명성의 위배는 법, 제도 및 규정의 위반을 의미하며 보안 사고로 발전하게 된다. 이러한 근거에서 정보보호 거버넌스의 투명성은 준거성이라는 보다 엄격한 표현으로 목표를 수립하여야 한다.

위의 3가지 정보보호 거버넌스 목표와 정보보호 거버넌스 개념 정의 요건을 구성하고 있는 이해관계자 관계, 관리와의 구분, 조직 통제, 전사적인 위험 관리와의 관계를 종합하여 정보보호 거버넌스의 개념을 정의하면, 정보보호 거버넌스는 “기업 거버넌스의 일환으로서 비즈니스와의 전략적 연계, 관련 법과 규정의 준수, 의사결정 권한과 책임의 할당을 위한 프로세스 및 실행체계”로 정의될 수 있다.

4.2 정보보호 거버넌스의 원칙 항목 정의

정보보호 거버넌스 원칙 항목을 정의하기 위한 요건은 전제 조건 원칙과 일반 원칙으로 구성되어 있다(<표 9> 참조).

정보보호 거버넌스의 전제조건 원칙은 거버넌스의 목표와 수단에서 도출되는 원칙, 다시 말해 정보보호 거버넌스의 목표를 책임성, 비즈니스 연계성, 준거성으로 설정했을 때, 각 목표 달성을 위해 전제되는 원칙이며, 이를 위해 동원하는 실행 도구(수단)에 전제되는 원칙들이다. 이러한 전제가 충족되지 않고서는 정보보호 거버넌스에 대한 논의 자체를 시작할 수 없다.

이들 거버넌스 목표와 실행 도구의 전제요건들을 원칙의 형태로 정리한 것은 다음과 같다.

정보보호 거버넌스의 ‘책임성’ 목표의 전제에는 ‘권한과 책임’ 및 ‘보상과 처벌’이 저변에 자리잡고 있다. 이러한 권한과 책임, 보상과 처벌이 전제되지 않은 책임성은 아무런 의미가 없다[이정훈 등, 2007].

정보보호 활동이 비즈니스와 연계될 때 효과성을 확인하기 위해서는 두 가지가 전제되어야 한다. 하나는 활동의 ‘추적 가능성’이고 다른 하나는 ‘측정 가능성’이다. 전자는 기업 활동이 궁극적으로 기업 목표와 연결되는지 인과관계를 ‘추적’ 할 수 있어야 한다는 것이고, 후자는 그러한 활동에 소요된 투입과 산출의 정도를 ‘측정’ 할 수 있어야 한다는 것이다[이정훈 등, 2007].

정보보호 거버넌스는 ‘준거’의 개념에 바탕을 두고 있고, 따라서 ‘규정’과 ‘표준’의 존재 및 이

들에 대한 준거를 요구하는 '이해관계자'들의 정당성 및 합의를 그 핵심 전제 조건으로 인식해야 한다. 이러한 준거성의 원칙은 기업의 주주 및 경영진들이 기업을 전반적으로 거버넌스 하기 위한 중요 수단으로서 활용될 수 있다[한국정보사회진흥원, 2008a; 김정덕, 2009].

선행 연구에서는 거버넌스 원칙을 거버넌스 목표와 실행 체계를 연결하는 매개체로 정의하고 있다[ISO/IEC, 2008; 이정훈 등, 2007]. 이러한 매개체 역할을 정보보호 거버넌스에 적용하기 위해 본 연구는 다음과 같이 정보보호 거버넌스의 3개 목표를 기준으로 일반 원칙을 정의하였다[한국정보사회진흥원, 2008a].

(책임성 관련 원칙)
- 리더의 준수 책임
- 역할, 책임 및 권한의 정의
- 적절한 자원의 할당
- 구성원의 인식과 훈련

(비즈니스 연계성 관련 원칙)
- 비즈니스 요구사항과의 연계
- 리스크 기반의 거버넌스
- 업무활동 기반

(준거성 관련 원칙)
- 정책에 근거한 활동
- 조직 외부 법규 및 규정 준수
- 검토와 평가

4.3 정보보호 거버넌스 실행체계

정보보호 거버넌스 구조화 요건(<표 6> 참조)에 따르면 정보보호 거버넌스의 실행체계는 정보보호 거버넌스 목표와 원칙을 실행하기 위한 제반 활동 및 이를 위해 동원되는 각종 도구와 그들 간의 관계를 체계적으로 명시하여야 한다.

정보보호 거버넌스 실행 체계는 요건을 기반으로 1) 거버넌스 조직, 2) 거버넌스 프로세스, 3) 거버넌스 도구의 3가지 범주로 구분하였고 각 항목은 선행연구의 결과를 적용하여 정의되었다.

4.3.1 정보보호 거버넌스 조직 항목 정의

정보보호 거버넌스 조직 항목 정의를 위한 요건에는 의사결정 권한을 갖춘 경영층의 거버넌스 조직 참여와 활동 실행이 포함되어 있다. 따라서, 정보보호 거버넌스 조직 항목은 정보보호 거버넌스 활동을 위한 경영층, 이사회 등 주요 의사결정자 그룹의 역할을 정보보호 거버넌스 목표에 따라 기술함으로써 정의된다.

국내 기업의 현황은 경영진과 이사회의 구분이 모호하고 대부분의 이사진이 위원회의 위원을 겸직하는 형태를 나타내고 있다. 이러한 제약사항을 고려하여 조직 내 위상에 따른 정보보호 거버넌스 목표 별 역할 및 책임을 제시하면 다음의 <표 11>와 같다[한국정보사회진흥원, 2008a].

〈표 11〉 정보보호 거버넌스 목표에 따른 주요 의사결정자의 역할 및 책임

정보보호 거버넌스의 "책임성"	
이사회	• 정보보호에 대한 전사적 원칙과 방향을 설정
경영진	• 정보보호에 대한 전사적 통합 프로세스 결정
위원회	• 업무 부문과 보안영역의 통합전략 수립 지원, 검토
정보보호 거버넌스의 "비즈니스 연계성"	
이사회	• 보안활동의 비용과 업무적 가치에 대한 평가 및 보고 기준 마련
경영진	• 비즈니스 영역의 가치 측정과 정보보호 영향에 대한 기준 마련
위원회	• 업무, 정보보호 목표 달성을 위한 범위 및 적절성에 대한 검토
정보보호 거버넌스의 "준거성"	
이사회	• 전사적 위험관리 규제 준수를 위한 정보보호 정책 설정
경영진	• 위험관리 역할과 책임 할당 • 규제준수 모니터링
위원회	• 긴급 위험 확인, 업무별 보안활동 권장, 규제 준거 이슈 확인

현재 국내 기업의 경영 여건이 선진화 되는 과정이며 다양한 외부적 조건에 의해 많은 영향을 받고 있는 상황이므로 <표 11>에 정의된 역할 및 책임을 충족하지 못할 수 있으나, 향후 바람직한 정보보호 거버넌스 본연의 목적을 달성하기 위해서는 이사회와 경영진의 명확한 분리를 통해 정보보호의 실천과 이에 대한 감독 및 상벌이라는 역할과 책임을 체계화하는 것이 필요하다.

4.3.2 정보보호 거버넌스 프로세스 항목 정의

정보보호 거버넌스 프로세스 항목 정의를 위한 요건에는 평가, 지시, 성과 모니터링의 거버넌스 생명주기가 반영되었다.

이러한 거버넌스 생명주기는 ISO/IEC 38500을 통해 거버넌스 프로세스로서 국제표준화 되었으며, 선행 연구를 종합한 항목 정의 요건에도 부합되므로 정보보호 거버넌스 프로세스는 평가, 지시, 성과 모니터링의 생명주기를 중심으로 구성되었다(<표 12> 참조).

〈표 2〉 정보보호 거버넌스의 평가, 지시, 모니터링 프로세스

정보보호 거버넌스의 “평가”	
대상	정보보호 활동 및 수행 내역
구성활동	• 현재와 미래의 정보보호 전략 • 수행 내역에 대한 진단과 평가 • 비즈니스 연계에 대한 분석과 평가
정보보호 거버넌스의 “지시”	
대상	정보보호 계획과 정책
구성활동	• 정보보호 권한과 책임 할당 • 정보보호 전략 계획의 수립과 실행 • 정보보호 투자 방향 설정 • 정보보호 운영규정 • 정보보호 활동 규범 설정
정보보호 거버넌스의 “모니터링”	
대상	정보보호 성과와 준수
구성활동	• 정보보호 활동 성과 측정 및 분석 • 정보보호 정책 등 원칙 준수 확인 • 정보보호 관련 내・외부 규칙과 규범 준수 확인

정보보호 거버넌스의 평가, 지시, 모니터링 활동은 일정한 순서에 의해 수행되지 않으며 지속적으로 상호 작용하는 활동이기 때문에 정보보호 거버넌스 프로세스의 완결성을 위해 다음과 같은 추가 단계를 정의하였다.

- 조직의 이해 : 조직의 비즈니스 현황과 존재하는 정보보호 취약점 파악
- 정보보호 거버넌스 정책 수립 : 거버넌스 목표와 원칙을 고려한 정책 수립
- 평가
- 지시
- 모니터링
- 개선과 검토 : 평가 결과 검토 및 개선 사항을 정리하고 정보보호 거버넌스 활동 전반에 반영

4.3.3 정보보호 거버넌스 도구 항목 정의

정보보호 거버넌스 실행 체계 내에서 도구 항목은 정보보호 거버넌스 목표 달성을 위한 모든 도구와 수단이 포함될 수 있다(<표 10> 참조).

정보보호 거버넌스의 도구로 다양한 도구와 수단들이 활용되고 있는 것이 현실이지만, 본 연구에서 제시하는 정보보호 거버넌스 프레임워크는 전사적 시각에서의 관리와 정보보호관리 활동의 운영 성과를 주기적으로 평가하는 것이 핵심이다. 이에 따라 본 연구에서는 ‘전사 정보보호 아키텍처’와 ‘성과지표 모델’을 정보보호 거버넌스 도구로 선정하였다.

(1) 전사적 정보보호 아키텍처

정보보호 활동에 대한 지시와 통제 행위를 포함하는 정보보호 거버넌스를 실행하기 위해서는 정보보호 체계를 단일화된 관점에서 확인할 수 있는 청사진이 필요하다[김정덕, 2009].

전사적 정보보호 아키텍처는 기업의 정보보호에 대한 청사진을 제공하여, 비즈니스와의 연계

성, 정보보호 기능 및 조직들 간의 관계, 정보보호 기술 간의 연계성 등을 보장하므로 거버넌스 도구로서 활용 가능하다. 또한 EA(Enterprise Architecture)와의 관계를 제시하여 IT 영역과의 거버넌스 활동 간 교류에도 활용 가능하다.

⑵ 성과지표 모델

정보보호 거버넌스 성과 지표는 정보보호 관리 활동의 성과 지표를 기반으로 도출되어야 한다. 정보보호 거버넌스 지표는 정보보호 관리 지표를 대상으로 책임성, 비즈니스 연계성, 준거성을 확인하는 기능을 수행해야 하므로 두 가지 지표는 밀접한 연관관계를 갖는다.

5. 정보보호 거버넌스 프레임워크의 검증

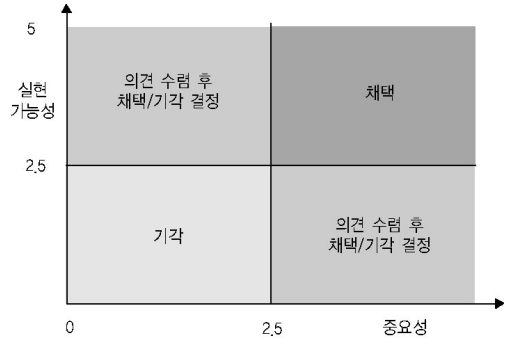
5.1 검증 방법

현재 국내에는 정보보호 거버넌스를 구현한 사례가 전무한 실정이므로 본 논문에서는 정보보호 거버넌스 프레임워크의 적정성 평가를 위해 정보보호 거버넌스를 조직에 구현하는데 필요한 구성요소들 중에서 우선순위가 높은 요소가 본 논문에서 제시한 프레임워크에 포함되어 있는지를 정보보호 분야의 전문가들로 구성된 포커스 그룹을 대상으로 확인하였다.

Cabrera et al.[2008]은 조직적 해결과제의 우선순위를 결정하기 위한 중요도와 실현 가능성을 5점 척도를 이용해 결정하였다. 한편, 도출된 문제의 중요도가 높지만 실현 가능성이 낮은 경우 또는 중요도는 낮지만 실현 가능성이 높은 경우에는 전문가의 의견을 수렴해 우선순위를 부여하였다. Sork[1982]은 우선순위 결정을 위해 5가지의 중요도 평가 기준과 3가지의 실행 가능성 평가기준에 따른 개별 선호도를 평가하고, 각각의 평가 점수들을 합산하는 집합적 의사결정(Aggregated Decision) 방법을 제시하였다.

Ozdemir et al.[2009]은 기업 거버넌스 도입을 위해 제시된 바젤 Ⅱ의 구현에 대해 연구하였는데, 바젤 Ⅱ를 성공적으로 구현하기 위해 필요한 사항들을 중요성과 실행 가능성 기준으로 평가하여 우선순위를 결정하였다.

본 연구에서는 이 중에서 본 연구와 연구의 내용이 가장 유사한 Ozdemir and Miu[2009]의 중요성과 실현 가능성을 검증 항목으로 사용하여 <그림 6>과 같이 프레임워크의 적정성을 판단하였다.



〈그림 6〉 ISG 프레임워크 검증 매트릭스

중요성은 높지만 실현 가능성이 낮은 경우와 중요성은 낮지만 실현 가능성이 높은 경우에는 포커스 그룹의 의견을 수렴하여, 채택 및 기각 여부를 판단하였고, 중요성 및 실현 가능성이 2.5이하인 구성 요소는 정보보호 거버넌스 프레임워크의 구성요소로서 부적합한 것으로 판단하였다.

5.2 자료 수집 및 분석 방법

본 논문에서는 주제와 관련하여 공통된 특성을 가지고 있는 구성원들의 상호작용을 통하여 연구자가 정한 주제에 대한 자료를 수집하는 포커스 그룹 인터뷰(Focus Group Interview)를 사용하였다[김성재 등, 2007].

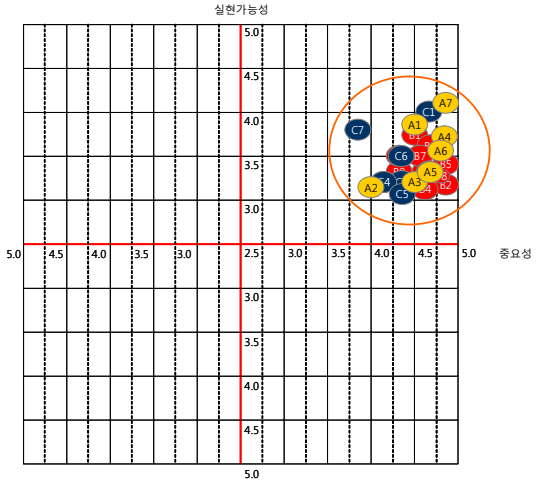
Krueger et al.[2000]에 따르면 포커스 그룹 인

터뷰는 아이디어, 소재, 계획 또는 정책을 미리 시험해 보고자 할 때 유용하므로 프레임워크 검증을 위해 적합한 방법이라고 판단하였다.

포커스 그룹 인터뷰를 수행하기 위해 연구소 및 정보보호 분야의 전문가 25명이 참여한 포커스 그룹을 구성하여 설문과 심층 면접을 수행하였다. 설문은 도출된 정보보호 프레임워크 구성 요소의 중요성과 실현 가능성을 측정하기 위해 리커드 5점 척도를 사용하였고, 설문 종류 후 30분에 걸쳐 참여자들 간에 의견을 교환하고, 도출된 정보보호 프레임워크 구성 요소가 중요한 이유를 연구자의 주도하에 대화형식으로 토론하였다.

5.3 검증 결과

포커스 그룹 인터뷰 결과, 본 연구에서 제시하고 있는 정보보호 거버넌스 프레임워크의 구성요소들은 “<그림 6> 검증 매트릭스”의 채택 영역에 모두 포함되었다(<그림 7> 참조).



〈그림 7〉 ISG 프레임워크 구성요소의 분포
(〈표 13〉의 "번호" 항목 참조)

포커스 그룹에 포함된 전문가들은 정보보호 거버넌스 프레임워크의 구성 요소들이 중요성은 매우 높지만, 실현 가능성은 다소 높은 수준으로 평가하였다. 이러한 평가 결과는 전문가들이 정보보호 거버넌스의 중요성은 인정하지만, 실제 구현 가능성에 대해서는 중요성 만큼 높은 점수를 주지 못하고 있다는 것을 보여준다.

다음의 <표 13>에는 포커스 그룹 인터뷰를 통해 파악된 정보보호 거버넌스 프레임워크 구성요소의 중요성 및 실현 가능성 점수가 자세하게 정리되어 있다.

〈표 13〉 포커스 그룹 인터뷰 결과

정보보호 거버넌스 프레임워크 구성요소			번호	중요성	실현 가능성
개념 및 목적		이해관계자 관계	A1	4.5	3.9
		관리와의 구분	A2	4.0	3.1
		조직통제	A3	4.5	3.2
		전사위험관리와 연계	A4	4.8	3.8
		책임성	A5	4.3	3.3
		비즈니스 연계성	A6	4.7	3.7
		컴플라이언스	A7	4.7	4.1
원칙	전제조건 원칙	정보보호 거버넌스 목표 실행을 위한 전제 조건	B1	4.5	3.7
	일반 원칙	리더의 책임 의식과 의지	B2	4.8	3.3
		역할, 책임 및 권한의 정의	B3	4.3	3.7
		적절한 자원의 할당	B4	4.2	3.1
		구성원의 인식과 훈련	B5	4.8	3.4
		비즈니스 요구사항과 연계	B6	4.2	3.3
		리스크 기반 거버넌스	B7	4.2	3.4
		업무 기반 거버넌스	B8	4.8	3.4
		정책에 근거한 활동	B9	4.3	3.4
		조직 외부 법규 및 규정 준수	B10	4.3	3.5
		검토와 평가	B11	4.2	3.3
실행 체계	조직	의사결정 권한	C1	4.6	4.0
		경영층의 참여	C2	4.6	3.3
	프로세스	평가	C3	4.3	3.2
		지시	C4	4.1	3.3
		모니터링	C5	4.4	3.2
	도구	목표달성 방법	C6	4.3	3.3
		내부통제 활용	C7	3.9	3.8
			평균	4.4	333.5

5.4 포커스 그룹 인터뷰 결과 시사점 및 향후 연구

포커스 그룹 인터뷰 결과에서 나타난 중요성과 실현 가능성의 편차는 실현 가능성 제고에 기여할 수 있는 추가적인 연구가 필요하다는 점을 시사한다(<표 13> 참조). 예를 들어, 비즈니스 연계성을 확보하기 위한 목표와 원칙들은 개념적으로는 중요하지만, 정보보호가 비즈니스에 어떠한 가치를 제공하는지 정량적으로 측정 가능한 지표 없이는 정보보호와 비즈니스를 연계하기 힘들다는 것이 포커스 그룹의 의견이었다. 또한, 컴플라이언스에 대한 지속적인 평가를 실행할 수 있는 지표 없이는 중요도에 비해 실행을 보장하기 어렵다는 것이 전문가의 견해였다. 따라서 정보보호 거버넌스의 실행 측면을 보완할 수 있도록 본 연구에서 제시한 핵심성과지표 부문에 대해 정보보호 가치의 측정을 위한 지표 개발, 정보보호 관련 법/규정의 준수 여부를 측정하기 위한 지표 개발 등의 연구가 추가적으로 필요하다고 판단된다.

6. 결 론

현재 정보보호 거버넌스 개념 자체에 대해 많은 혼란이 있으며, 이론적 기반이 매우 취약하고, 그 추진 방법이나 수단에 대한 실무적 연구 결과가 전무한 실정이다.

본 연구는 기업 및 IT 거버넌스 영역과 연계할 수 있는 정보보호 거버넌스 프레임워크를 제시함으로써 거버넌스 개념을 둘러싼 오류와 혼란을 최소화할 수 있도록 거버넌스의 분명한 개념을 정립하고, 거버넌스의 영역과 경계를 설정하였다. 또한 이를 토대로 거버넌스 추진의 원칙과 실행의 방향을 제시하였다.

본 연구가 제시한 정보보호 거버넌스 프레임워크는 특정 거버넌스 방법론이나 기법에 고착되지 않는 포괄적 방안으로서, 조직은 이러한 프레임워크를 토대로 자신들의 거버넌스 노력을 점검, 조명, 설계, 추진할 수 있을 것으로 기대된다.

본 연구의 한계로는 정성적 분석방법에 의한 프레임워크의 검증을 들 수 있다. 이러한 검증 결과는 객관성 확보 및 일반화가 어렵다는 한계점을 가지고 있다. 따라서, 향후의 연구에서는 본 논문의 프레임워크를 실제 기업에 적용한 사례 연구를 수행하여 본 프레임워크를 진화시키고 정보보호 우수기업의 경영층을 대상으로 한 포커스 그룹 인터뷰를 실시함으로서 연구 결과의 검증 부문 강화가 필요할 것으로 판단된다.

참 고 문 헌

[1] 김성재, 오상은, 은영, 손행미, 이명선 역 (Morgan, D. L. 저, 2007), “질적 연구로서의 포커스 그룹”, 군자출판사, 2007.

[2] 김정덕, 정보보호 거버넌스 국제 표준화 동향, http://www.tta.or.kr/data/weekly_view.jsp?news_id=2605, 2009.

[3] 이정훈, 전성현, 황경태, IT 거버넌스 프레임워크 개발, 한국정보사회진흥원, 2007.

[4] 한국 정보보호진흥원, 정보통신 기업을 위한 정보보호 거버넌스 표준화 연구, *2008*a.

[5] 한국 정보보호진흥원, 국내 개인정보보 법규 현황 및 방향, 2008b.

[6] Ljungqvist, Alexander, “The Role of Hostile Stakes in German Corporate Governance”, 1999.

[7] Baker, W. E., The Network Organization in Theory and Practice.-Networks and Organizations Structure, Form, and Action, (Ed.) Nohria, N. and R. G. Eccles, *Harvard Business School Press,* 1992, pp. 397-411.

[8] Birman K. P., The next-generation internet : unsafe at any speed. *IEEE Computer 2000,* Vol. 33, No. 8, pp. 54-60.

[9] Cabrera, D., J. T. Mandel, J. P. Andras, and M. L. Nydam, What is the crisis? Defining and prioritizing the world's most pressing problems, *Front Ecol Environ*, 2008, pp. 469-475.

[10] Cordite, J., Best Practices in Information Technology, Prentice Hall, Upper Saddle River, NJ, 1998.

[11] Daft, R. L., Organization Theory and Design, West Publishing, St. Paul, MN., 1989.

[12] Gartner, IT Governance in Government Agencies Frequently Asked Questions, Gartner Research, 2006.

[13] Hodges, R. M., Wright and K. Keasey, Corporate Governance in the Public Services : Concepts and Issues, *Harvard Business School Press*, 1996.

[14] ISO/IEC 27001, Information Security Management Sytems, 2005.

[15] ISO/IEC 38500, Corporate Governance of Information Technology, 2008.

[16] ITGI, "Information Security Governance : Guidance for Boards of Directors and Executive Management", 2002.

[17] ITGI, Board Briefing on IT Governance Report, Second Edition, Rolling Meadows, Vol. 1, 2003.

[18] Krueger, R. and Casey, M. Focus Groups : A Practical Guide for Applied Research. Thousand Oak, CA : Sage Publications, Inc, 2000.

[19] Lee, J.-H., Juhn, S.-H., and Hwang, K. T., New Development of Advanced ITG Framework, HICCS, 2008.

[20] Monnoyer, E. and Willmott, P., Paul, What IT Leaders Do, The Mckinsey Quarterly, August, 2005.

[21] NIST SP 800-100, "Information Security Handbook for Managers", 2007.

[22] OCC, Basel Ⅱ, 2003.

[23] OECD, "OECD Principles of Corporate Governance", 2004.

[24] Ozdemir, B. and P. Miu. Basel Ⅱ Implementation : A Guide to Developing and Validating a Compliant, Internal Risk Rating System. McGRAW-HILL. 2009.

[25] Posthumus, S. A., Framework for the Governance of Information Security, Computer and Security, 2004.

[26] Simonsson, M. and Johnson, P., "Defining ITG-A Consolidation of Literature", *the 18th Conference on Advanced Information Systems Engineering*, 2006.

[27] Sork, T. J., Determining Priorities, Vancouver, Canada, University of British Columbia, 1982.

[28] Webb, P., Pollard, C., and Ridley, G., Attempting to Define IT Governance : Wisdom or Folly?, Proceedings of the 39th Hawaii International Conference on System Sciences, 2006.

[29] Weill, P. and Ross, J. W., IT Governance-How Top Performers Manage IT Decision Rights for Superior Results, *Harvard Business School Press*, 2004.

[30] Westby, J. R., and Allen, J. H., "Governing for Enterprise Security(GES) Implementation Guide", Carnegie Mellon University, Soft ware Engineering Institute, CERT®, 2007.

저자소개

이 성 일

중앙대학교 산업정보학과에서 석사를 취득하였고, 동국대학교 경영정보학과 박사과정을 수료하였다. 시큐아이닷컴 컨설팅사업부를 거쳐 현재 Ernst and Young Advisory ITRA 부서에 근무하고 있다. 관심분야는 정보보호 거버넌스, 정보보호관리체계, IT 위험관리 등이다.

황 경 태

현재 동국대학교 경영대학 경영정보학과 교수로 재직 중이다. 연세대학교 상경대학을 졸업하고, George Washington University에서 경영학 석사, State University of New York at Buffalo에서 경영정보학 박사학위를 취득하였다. 주요 관심분야는 정보전략, IT 서비스 관리, IT 거버넌스 등이다.

◈ 이 논문은 2011년 05월 11일 접수하여 2011년 06월 07일 게재확정되었습니다.