금융 IT보안 컴플라이언스 프레임워크 연구

김태희* 김영태* 성재모*
*금융보안연구원
e-mail:{thkim, ytkim, sitcom}@fsa.or.kr

A Study on Financial IT Security Compliance Framework

Tae-Hee Kim* Young-Tae Kim* Jae-Mo Sung*
*Finanacial Security Agency

요 약

기업들은 새롭게 변화하는 법률 및 표준이 포함하고 있는 정보보호 요구사항들을 만족하기 위해 매번 상당한 시간과 비용을 투자하고 있다. 또한, 기업이 자체적으로 개발한 내부 컴플라이언스 정책 및 체계를 활용하고 있어 다양한 법, 표준의 변화가 있을 때 기업 내의 서로 다른 조직들과 협업하여 이를 준수하기란 어려운 상황이다. 이와 같이 관련 법, 표준의 내용들이 변경되는 한, 이에 대한 컴플라이언스를 위해 반복적으로 시간과 자원이 투입되기 때문에 막대한 비용이 소요될 수 밖에 없다. 따라서 본 논문에서는 금융기관들의 컴플라이언스 체계를 개선하며 이를 효율적으로 관리할 수 있는 금융 IT보안 컴플라이언스 프레임워크를 제안한다.

1. 서론

Ernst & Young Advisory의 2007년, 2009년 정보보호에 관한 인식 및 향후 방향에 대해 50여 개국의 기업을 대상으로 조사한 결과에 따르면, 정보보호 분야의 컴플라이언스에 지속적으로 투자할 것이라고 응답하였으며, 실제로 많은 기업들이 변화하는 법률 및 규제 준수를 위해 상당한 자원과 비용을 소비하고 있는 것으로 나타났다[1,2]. 이는 기업들이 컴플라이언스를 기업의 정보보호에 있어 중요한 부분으로 인식하여 새로운 컴플라이언스 요구사항이 발생할 때마다 이를 파악하고 지원하기 위해 반복적으로 시간과 비용을 투자하기 때문이다.

이에 따라 국내·외적으로 기업 비즈니스의 효율성과 이익 측면을 고려하여 지속적인 컴플라이언스 관리 비용을 절감하기 위한 방안들이 연구되고 있다. 일례로 해외에서는 기업의 IT컴플라이언스를 위해 IT UCF(IT Unified Compliance Framework, IT 통합 컴플라이언스 프레임워크)라는 IT영역에서의 법률 및 표준을 보다 효율적으로 준수하고 관리할 수 있는 메커니즘을 구축하여 서비스 중에 있다[3]. 그러나 IT UCF는 해외 IT 컴플라이언스에 중점을 두고 있어 정보보호 통제영역을 중점적으로 다루고 있지 않으며, 국내 환경의 법률 변화들을 적절하게 수용할 수 없다.

따라서 본 논문에서는 국내 금융기관의 IT보안 컴플라이언스를 위해 정보보호 요구사항을 반영한 금융 IT보안 컴플라이언스 프레임워크를 제안한다. 이를 위해 ISO 27001의 통제항목을 기반으로 국내 금융기관에 적용되는 법률 및 표준들의 상관관계를 분석한다. 또한 통제 매트릭스(Control Matrix)를 구축하고, 이를 활용하여 관련 법률 및 표준의 준수 여부를 자체적으로 진단할 수 있도록 도움을 제공하는 동시에 지속적으로 관리할 수 있도록 지원한다.

본 논문의 구성은 다음과 같다. 2장에서는 선행 연구된 IT UCF에 대해 분석하고, 3장에서는 금융 IT보안 컴플라이언스 프레임워크를 제안한다. 끝으로 결론 및 향후 연구 방향을 제시한다.

2. 관련 연구

본 장에서는 IT 통합 컴플라이언스 프레임워크인 IT UCF의 특징들을 간략히 기술하고, 국내 금융기관에 도입 시 발생할 수 있는 이슈사항을 제기한다.

2.1 IT UCF 개요

IT UCF는 기업의 IT영역 컴플라이언스를 위한 프레임워크로서, Network Frontiers LLC와 Latham & Watkins LLP가 공동으로 전 세계 법규, 표준 및 규제 등을 분석하여 IT통제에 대한 단일 매트릭스를 개발하였다, IT UCF의 핵심 서비스는 컴플라이언스 프레임워크(Compliance Framework)와 통제 스프레트시트(Control Spreadsheet)로 구성된다. 기업들은 이를 이용하여, 컴플라이언스 정책 및 절차를 수립하는데 있어 기업에 필요한 컴플라이언스의 요구사항들을 파악하여 이행한 후 자체적으로 법률 및 표준들의 준수 여부를 진단할 수 있다. 현재 Microsoft, CA, Openpages 등 해외의 많은 기업들이 IT UCF에 대한 라이센스 계약을 체결하고 활용하고 있다.

2.2 IT UCF 주요 특징

IT UCF는 금융, 의료, 에너지, 미국 연방 법률 등 미국의 주요 법률과 COSO[4], COBIT[5], ITIL[6], NIST[7] 기준 등 국제적인 표준 및 영국, 캐나다의 주요 IT관련법들을 포함하여 총 500여 개의 IT관련 법률 및 표준과 130여 개의 통제영역으로 구성된다. 이 프레임워크를 기반으로 감사와 위험관리, 인적자원 관리, 기술적 보안 등으로 통제항목들을 분류하여 기업의 컴플라이언스를 지원하는 13개의 통제 스프레드시트를 제공하고 있다.

2.3 IT UCF의 이슈

IT UCF는 국내 금융기관이 준수해야하는 법률의 일부만을 포함하고 있으며, 대부분 미국, 유럽 등 해외의 법률에 대한 요구사항을 제공하고 있다.

이를 국내 금융기관의 IT보안 컴플라이언스를 이행하기 위해 적용한다면, 국내의 금융기관에 요구되는 법률 및 표준 등을 컴플라이언스 프레임워크에 포함하고 이를 IT영역이 아닌 IT보안에 중점을 둔 기준으로 분석하여 요구사항에 대한 준수 여부를 확인할 수 있어야 할 것이다. 따라서 국내 실정에 맞게 관련 법률 및 표준의 범위를 확대하고 정보보호 관리체계에 적합한 국제 표준인 ISO 27001[8]을 활용하여 실효성을 높일 수 있는 금융 IT보안에 특화된 컴플라이언스 프레임워크 개발이 요구된다.

3. 금융 IT보안 컴플라이언스 프레임워크

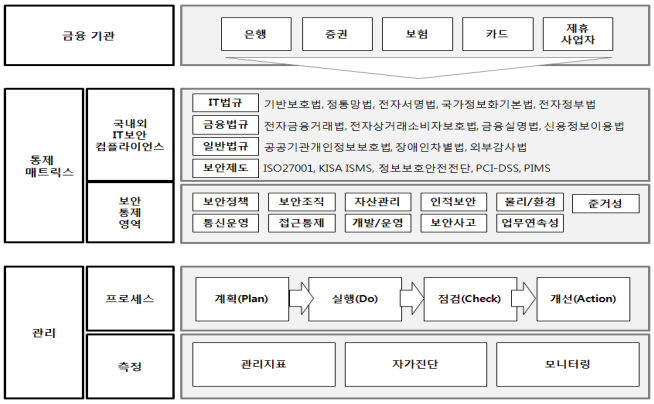
본 장에서는 금융기관에서 컴플라이언스를 이행하는데 도움을 제공할 수 있도록 효과적인 컴플라이언스 프레임워크를 제안한다. 또한, 금융부문에 적용되는 국내외 법률 및 표준 등을 소개하고, 각각의 법률 및 표준 간의 상관관계 분석을 통해, 금융부문의 법률 및 표준을 통합적으로 분류할 수 있는 통제 매트릭스를 구축하여 이를 활용한 컴플라이언스 관리 프로세스를 제시한다.

3.1 금융부문 IT보안 컴플라이언스 프레임워크 개요

다음 (그림1)은 금융 IT보안 컴플라이언스 프레임워크의 구조를 보여준다. 제안한 컴플라이언스 프레임워크는 은행, 증권 등 금융기관을 대상으로 관련 법률 및 표준들에 대해 ISO 27001을 기반으로 상관관계를 분석하고, 구축된 통제 매트릭스를 이용하여 컴플라이언스 이행 여부를 지속적으로 평가하고 관리하는데 도움을 제공한다. 컴플라이언스 프레임워크에는 아래와 같이 실효성, 신뢰성, 확장성 등 3대 기본 원칙이 적용되었다.

- 실효성 : 금융부문에 실질적인 효과가 발생해야 함
- 신뢰성 : 통제항목들이 객관적으로 신뢰할만한 수준이어야 함
- 확장성 : PCI-DSS, K-ISMS, 안전진단 등 다양한 프레임워크로 확장 가능해야 함

(그림 1) 금융 IT보안 컴플라이언스 프레임워크 구조도



또한 컴플라이언스 프레임워크가 추가적으로 갖추어야 할 사항은 다음과 같다. 첫째, 기업의 전략을 반영하고, 둘째, 기업에 필요함 법률 및 표준을 분류하여 요구사항을 파악하는 등 컴플라이언스 이행을 용이하게 하며, 셋째 컴플라이언스 이행 시 이를 판단할 수 있는 성과 측정 및 관리 지표를 통해 지속적으로 모니터링할 수 있어야 한다.

3.2 금융부문 관련 법률 및 표준

현재 금융기관에 해당하는 법률 및 표준은 “정보통신망 이용촉진 및 정보보호 등에 관한 법률”, “신용정보의 이용 및 보호에 관한 법률”, “전자금융거래법”, “금융실명거래 및 비밀보장에 관한 법률”, “정보통신기반보호법”, “KISA ISMS” 등이 있으며, 추가적으로 통제 매트릭스의 확장성을 고려하여 “PCI-DSS”[9], “Basel II”[10], “SAS 70”[11] 등을 포함하였다, 이를 법률 및 표준의 성격에 따라 다음 <표 1>과 같이 총 19개의 금융, 정보보안 관련 법률, 보안 표준으로 분류하였다.

<표 1>금융 IT보안 컴플라이언스 분석 대상

구분	분 석 대 상	
금융 관련 법률 (7개)	①	전자금융거래법(전자금융감독규정, 시행세칙 포함)
	②	금융실명거래 및 비밀보장에 관한 법률
	③	전자서명법
	④	신용정보의 이용 및 보호에 관한 법률
	⑤	주식회사의 외부감사에 관한 법률
	⑥	전자거래기본법
	⑦	자본시장과 금융투자업에 관한 법률
정보 보안 법률 (4개)	⑧	정보통신망 이용촉진 및 정보보호 등에 관한 법률
	⑨	공공기관의 개인정보보호에 관한법률
	⑩	정보통신기반보호법
	⑪	정보보호 안전진단
기타 법률 (4개)	⑫	국가정보화 기본법
	⑬	전자정부법
	⑭	장애인차별금지 및 권리구제 등에 관한 법률
	⑮	전자상거래 등에서의 소비자보호에 관한 법률
보안 표준 (4개)	⑯	PCI-DSS
	⑰	KISA ISMS
	⑱	Basel II
	⑲	SAS70

3.3 상관관계 분석 및 통제 매트릭스 구축

금융부문에 적용되고 있는 총 19개의 법률 및 표준들에 대해 통제 매트릭스를 구축하였다. ISO 27001의 11개 통제영역의 133개 통제항목들을 기준으로 상관관계를 분석하였으며. <표 2>는 ISO 27001의 통제영역에 해당하는 법률 및 표준들의 연관성을 보여준다.

<표 2> 법률 및 표준의 상관관계 분석 결과

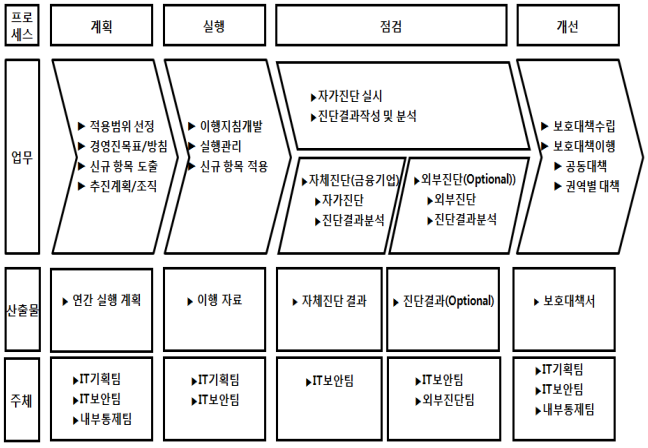
구 분		통제 영역											연관성
		① 보안정책	② 보안조직	③ 자산관리	④ 인적자원보안	⑤ 물리적·환경적보안	⑥ 의사소통·운영관리	⑦ 접근통제	⑧ 정보시스템개발·유지	⑨ 정보보안사건관리	⑩ 업무연속성관리	⑪ 준거성	
금융 관련 법률	①	2	5	-	1	10	14	14	6	3	1	4	45.1%
	②	-	-	-	-	-	-	-	-	-	-	1	0.8%
	③	1	1	-	-	2	-	-	1	1	1	1	6.0%
	④	1	2	-	1	-	-	-	-	-	-	-	3.0%
	⑤	-	-	-	-	-	-	-	-	-	-	-	0.0%
	⑥	-	-	-	1	2	3	-	1	-	-	1	6.0%
	⑦	-	-	-	-	-	-	-	-	-	-	-	0.0%
정보 보안 법률	⑧	1	4	-	-	1	2	3	-	2	1	3	12.8%
	⑨	1	2	-	-	2	2	1	2	-	-	3	9.8%
	⑩	1	2	-	1	1	2	2	1	2	-	3	11.3%
	⑪	2	6	2	3	1	4	10	1	1	-	3	24.8%
기타 법률	⑫	1	-	-	-	-	1	-	-	1	-	1	3.0%
	⑬	1	3	-	1	-	2	6	1	1	-	1	12.0%
	⑭	-	-	-	-	-	-	-	-	-	-	1	0.8%
	⑮	-	-	-	-	-	-	-	-	-	-	1	0.8%
보안 표준	⑯	2	4	-	3	3	15	10	9	1	-	1	36.1%
	⑰	2	7	5	9	13	29	22	15	5	5	9	91.0%
	⑱	1	1	1	-	-	1	-	2	2	4	1	9.8%
	⑲	2	-	-	1	2	6	5	5	1	-	-	16.5%

전반적으로 법률 및 표준들은 각각의 제정 목적에 따라 특정 통제 영역으로 편중되는 경향을 보였으며, 보안 표준 분야의 “KISA ISMS”, 금융관련 법률 분야의 ”전자금융거래법“, 정보보안 법률 분야의 “정보보호 안전진단“이 각 분야에서 ISO 27001의 통제영역과 가장 연관성이 높게 나타났다. 각각의 컴플라이언스의 연관성을 바탕으로 보다 세부적으로 분석 대상들과 ISO 27001의 통제영역 간의 유사 정도를 파악한 결과, 금융 IT보안에 해당하는 법률 및 표준들은 ‘보안정책’, ‘보안조직’, ‘자산관리’, ‘물리적·환경적 보안’, ‘정보시스템 획득 및 개발·유지보수’, ‘준거성’ 등의 영역에서 ISO 27001 통제영역의 목적과 일치하여 대부분의 내용이 중복되는 것으로 나타났다. 이는 해당 통제항목이 컴플라이언스를 위한 가장 기본적인 요구사항임을 나타내며, 비교적 유사한 목적을 지닌 ‘인적 자원 보안’, ‘의사소통 및 운영관리’, ‘접근통제’, ‘정보보안 사건 관리’, ‘업무연속성 관리’ 등의 항목에서는 해당 항목들의 성격으로 미루어 보아 각각의 법률 및 표준들이 기술적인 보안요소에 보다 관리적·물리적 보안요소를 위한 컴플라이언스를 요구하는 것을 알 수 있다.

3.4 컴플라이언스 관리 프로세스

(그림2)는 금융 IT보안 컴플라이언스를 체계적으로 관리 및 운영하기 위한 컴플라이언스 관리 프로세스를 보여준다.

(그림 2) 컴플라이언스 관리 프로세스 개요도



첫째, 계획단계에서는 적용범위 선정, 추진계획 및 조직 등을 통해 연간 실행계획을 도출한다. 둘째, 실행단계에서는 이행지침 개발 등을 통해 이행자료를 산출한다. 셋째, 점검단계에서는 자체진단 또는 외부진단을 통해 자가진단을 실시하고 진단결과를 분석한다. 넷째, 보호대책을 수립·이행한다.

컴플라이언스 관리의 효율성을 높이기 위하여 각 프로세스단계별로 관련 IT기획팀, IT보안팀, 내부통제팀 등이 적극적으로 참여해야 한다.

4. 결론

지금까지 금융기관들은 IT보안의 컴플라이언스 이행을 위해 법률 및 표준의 변화에 따라 반복적으로 시간 및 비용을 투자하였다. 따라서 본 논문에서는 금융부문 정보보호의 컴플라이언스 관리 비용을 절감하기 위한 국내·외 법률 및 표준들의 상관관계를 ISO 27001의 통제항목을 기준으로 분석하고, 통제 매트릭스를 구축하여 금융 IT보안 컴플라이언스 프레임워크를 제안하였다.

향후 연구로는 금융기관들이 법률 및 표준의 준수 여부를 자체적으로 측정할 수 있는 자가진단 체크리스트를 개발하고자 한다. 또한 개인정보보호법 등 새롭게 제정되는 정보보호 관련 법규 및 표준들을 포함할 수 있도록 통제 매트릭스를 확장하고자 한다.

참고문헌

[1] Ernst & Young, “Achieving a Balance of Risk and Performance” (10th annual global information

security survey), December 2007
[2] Ernst & Young, “Outpacing change” (12th annual global information security survey), 2009
[3] http://www.unifiedcompliance.com
[4] The COSO Model: How IT Auditors Can Use It to Evaluate the Effectiveness of Internal Controls, Tommie Singleton, Information systems control journal, Volume 6, 2007
[5] 조희준, IT거버넌스 프레임워크 코빗, 인포더북스, 2010.4
[6] An Introductory Overview of ITIL V3, itSMF, 2007
[7] http://www.nist.gov/index.html
[8] ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems requirements, 2005
[9] Mapping ISO 27001 Controls to PCI-DSS V1.2 Requirements, ISO 27001 Implementer’s Forum, 2009
[10] http://www.bis.org/publ/bcbsca.htm
[11] http://sas70.com