*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.28, NO.4, Aug. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.4.941

# 금융회사 내 최적의 정보보호조직 형태에 대한 연구 - 경영진(CISO, CIO, CPO) 관계를 중심으로 -

김 상 호,† 김 인 석‡
고려대학교 정보보호대학원

# A Study on Optimal Information Security Organizational Form in Financial Companies - Based on the Relationship between Management -

Sang-ho Kim,† In-Seok Kim‡
Korea University, Graduate School of Information Security

요 약

금융회사의 정보보호조직 형태는 정보기술최고책임자(CIO)와 정보보호최고책임자(CISO), 개인정보보호책임자(CPO)의 책임과 역할 부여에 따라 다양한 조직 구성의 형태를 갖는다. 하지만 이러한 다양한 형태의 정보보호조직이 최적의 조직 형태인지는 살펴볼 필요가 있다. 본 연구에서는 CISO, CIO, CPO관계 측면에서 다양한 정보보호조직 형태 가운데 일반적으로 금융회사가 갖는 정보보호조직 형태 중 대표적인 6개 조직형태를 후보군으로 선정하고 금융회사만이 갖는 몇 가지 고유한 특성과 공인된 외부의 정보보호 거버넌스 요소를 평가척도로 활용하여 최적의 금융회사 정보보호조직 구성 형태가 어떤 모습인지 연구 및 도출해보고자 한다.

ABSTRACT

The form of information security organization of a financial company has various organizational forms in accordance with the responsibilities and roles of the Chief Information Officer (CIO), the Chief Information Security Officer (CISO) and the Chief Privacy Officer (CPO). However, it is necessary to examine whether these various types of information protection organizations are the optimal organizational forms. In this study, six types of information security organizations among the various types of information security organizations in terms of CISO, CIO, and CPO relationship were selected as candidates. This paper aims to study and elucidate the optimal organizational form of information security for financial companies.

**Keywords:** Organization, Financial Company, Relationship

## I. 서 론

금융회사에서 정보보호조직 형태는 기업의 규모, 연혁, 문화에 따라, 심지어는 개인정보 유출 사고여부에 따라 각기 다양한 조직구성의 형태가 존재하고, 실제 운영되고 있다.

어느 기업에서는 정보보호조직이 IT부문 내 위치하여 정보기술최고책임자(CIO)와 정보보호최고책임자(CISO)를 겸임하는 형태가 있는가 하면, 또 다른 기업에서는 정보보호부문이라는 독립된 조직을 두고 정보보호최고책임자(CISO)와 정보기술최고책임자(CIO)를 대등한 관계로 위치시키기도 한다. 이 밖

Received(05. 28. 2018), Accepted(07. 10. 2018)
† 주저자, preparedman@sgic.co.kr
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

에도 개인정보보호책임자(CPO)와의 관계까지 고려한다면 그 경우의 수 만큼이나 구성할 수 있는 조직의 형태와 구성은 실로 다양하다고 할 수 있다.

본 연구에서는 금융회사의 다양한 정보보호조직 형태 가운데 최적의 정보보호조직 형태 도출을 위해 3가지 평가기준(①공인된 정보보호관리체계, ②금융권 컴플라이언스, ③감독기관의 매뉴얼 및 가이드라인)을 세우고 이 기준에 가장 부합하는 최적의 금융회사 정보보호조직 형태를 모색해 보고자 한다.

## II. 공인된 정보보호관리체계

정보보호관리체계란 조직의 자산에 대한 안전성 및 신뢰성을 향상시키기 위한 절차와 과정을 체계적으로 수립, 문서화하고 지속적으로 관리·운영을 통하여 정보보호목표인 정보의 기밀성, 무결성, 가용성을 실현하기 위한 일련의 과정 및 활동을 의미[1]한다.

이러한 정보보호관리체계의 수준을 측정하고 이를 인증하는 인증제도로서 다양한 정보보호관리체계 인증이 존재한다. 가령 국제 정보보호관리체계 인증으로서 ISO27001, 국내 정보보호관리체계 인증으로서 ISMS, 국내 개인정보보호관리체계 인증으로서 PIMS 등이 있다. 물론 2018년 내 ISMS와 PIMS의 통합이 진행 중이긴 하나 이는 최근 정보보안과 개인정보보호가 밀접해지고 있는 추세를 반영하고 인증 중복운영에 따른 기업부담을 해소하기 위해 논의되는 만큼 본질적인 점검항목에는 큰 영향이 없을 것으로 판단하고 있다.

본 연구에서는 금융회사 내 최적의 정보보호조직 형태 도출의 평가기준으로서 정보보호관리체계에서 요구하는 조직 관련 요구수준을 활용하고자 하며, 위에서 언급한 정보보호관리체계 중 국내 정보보호관리체계(ISMS) 인증과 개인정보보호관리체계(PIMS) 인증을 기준으로 해서 활용해보고자 한다.

### 2.1 정보보호관리체계(ISMS) 인증

2013년에 발생한 3.20 금융전산 사고에 대한 후속조치로 금융권 정보보호 관리체계 인증제도 도입이 논의된 적이 있었다[1]. 그러나 기업의 중복규제 이슈 등으로 인해 최종적으로는 기존의 정보보호관리체계(ISMS) 인증을 활용하되 금융기관에 대한 인증심사를 위해 당시 미래창조과학부(現 과학기술정보통신부)는 정보보호 관리체계 인증 및 인증심사를 일괄적으로 수행하는 전담기구로서 금융보안원을 민간 인증기관으로 최초 지정하여 운영하는 것으로 결정[2]하였고, 이에 따라 2017년 3월 금융보안원은 정보통신(IT) 분야에 초점이 맞춰진 기존 정보보호 관리체계(ISMS) 점검항목에서 1개 항목을 삭제하고 72개 항목을 추가하여 총 324개 점검항목의 금융 분야 정보보호관리체계(ISMS) 인증기준 개발을 완료하여 이를 2017년도 인증 심사 시 선택적으로 적용하고, 2018년 인증 심사부터는 전면 적용할 계획이라고 발표하였다.

본 연구에서는 정보보호관리체계 인증 기준[3] 중 조직과 관련된 부분으로서 한 기업이 조직의 규모, 업무 중요도 등의 특성을 고려하여 정보보호 관리 활동을 지속적으로 수행할 수 있는 정보보호 조직이 구성되어 있는지(관리과정 2), 정보보호최고책임자(CISO)는 지정이 되어있고, 정보보호활동을 체계적으로 이행하기 위한 실무조직을 갖추고 있는지(보호대책 2) 등을 평가기준 항목으로 활용하고자 한다.

### 2.2 개인정보보호관리체계(PIMS) 인증

정보통신망법 47조의3에 기반한 개인정보보호관리체계 인증은 기업이 수립·운영하는 개인정보보호관리체계가 인증심사 기준에 적합한지 여부를 인증기관이 평가하여 인증을 부여하는 제도로서 개인정보보호 관리과정 16개, 생명주기 및 권리보장 20개, 개인정보 보호조치 50개씩, 총3개 분야 86개의 심사항목으로 구성되어 있다[4].

본 연구에서 활용하고자 하는 부분은 조직과 관련한 개인정보 관리체계(PIMS) 인증 기준으로서 개인정보보호책임자(CPO)를 지정하여 운영하고 있는지(관리과정 1.3), 해당 조직에서는 개인정보와 관련한 자산을 식별하고 중요도를 부여하여 관리할 수 있는지(관리과정 2.1), 또한 개인정보보호 영역에 대한 위험을 평가하고 위험수준을 설정하여 관리할 수 있는지(관리과정 2.2)를 활용하고자 한다.

### 2.3 공인된 정보보호관리체계 평가기준

앞서 살펴본 ISMS와 PIMS의 심사항목 중 조직

1) 한경 경제용어사전 '정보보호관리체계' (http://dic.hankyung.com)

과 관련한 항목을 수집하여 마련한 평가기준은 다음 Table 1.과 같다.

Table 1. Criteria for accredited information protection management system standard (ISMS / PIMS)

| No, | Criteria | Related |
|---|---|---|
| 1 | Do you organize an information security organization (CISO, working organization, information security committee, etc.)? | 〔FSI〕 ISMS |
| 2 | Do you designate an executive level Chief Information Security Officer (CISO)? | 〔FSI〕 ISMS |
| 3 | Do you support the role of the Chief Information Security Officer (CISO) and organize a working organization to systematically implement the organization's information security activities? | 〔FSI〕 ISMS |
| 4 | You must designate the Chief Privacy Officer for managing personal information | 〔KISA〕 PIMS |
| 5 | Personal information and personal information related assets should be identified, importance should be determined, security level should be assigned, and the handling procedures should be defined and implemented. In addition, responsibilities for each asset should be clearly defined. | 〔KISA〕 PIMS |
| 6 | The risk management method should be selected and the risk management plan should be established so that risk identification and evaluation can be performed for all areas of personal information protection. Risk identification and evaluation should be performed at least once a year, and as a result, Should be set and managed. | 〔KISA〕 PIMS |

## III. 금융권 정보보호 컴플라이언스 관련

금융관련 법규는 대표적으로 금융위원회에서 소관하는 전자금융거래법과 신용정보 이용 및 보호에 관한 법률을 포함한 40여개 법령〔5〕이 대표적이라 할 수 있으나, 금융회사가 준수해야할 법규는 이뿐 아니라 개인정보보호법과 같은 일반적으로 모든 기업에 광범위하게 적용되는 법도 이에 해당하는가 하면, 고객과 비대면으로 정보통신망을 통해 금융 서비스를 제공하는 경우 정보통신망 이용촉진 및 정보보호에 관한 법률을, 전자서명을 사용한다면 전자서명법을 준수해야 하는 등 금융업무 서비스 유형과 서비스 제공환경에 따라 다양한 관련법규 준수의무가 주어지게 된다.

본 연구에서는 금융회사가 준수해야할 수많은 법규들 가운데 정보보호와 관련하여 대표적인 전자금융거래법과 정보통신망법 그리고 개인정보보호법을 살펴보고 금융회사가 준수해야할 정보보호관련 법규 준수사항은 무엇인지 이를 위해 금융회사의 역할과 조직은 어떻게 구성되어야 하는지를 살펴보고자 한다.

### 3.1 전자금융거래법

전자금융거래법은 비대면적으로 이루어지는 전자금융거래에 대한 안전성과 신뢰성을 확보하기 위해 제정된 법률인 만큼 정보기술과 관련한 각종 규제와 의무조항이 자세히 포함되어 있는 것이 특징이다. 가령 법 제21조의2에서는 일정 규모 이상의 기업은 정보보호최고책임자(CISO)를 임원으로 지정할 것과 다른 정보기술업무를 겸직할 수 없는 겸직금지, 그리고 정보보호최고책임자의 자격요건과 해야 할 역할을 정의해 두고 있다.

### 3.2 개인정보보호법

개인정보보호법에서 직접적으로 정보보호조직 구성을 언급한 조항은 없으나, 개인정보의 안전한 보관 및 관리를 위해서 책임자 지정, 각종 보호조치 준수 등 필요한 활동을 언급한 조항이 존재한다.

법 제31조에서는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보보호책임자를 지정하도록 했으며, 법 제29조에서는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획을 수립하고 접속기록을 보관하는 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하

도록 명시하였다. 이에 대한 구체적이고 세부적인 내용은 「개인정보의 안전성 확보조치 기준」이라는 행정안전부 고시를 통해서 최소한의 기준으로 제시하였다.

고시에서 제시하는 최소한의 기준 내용을 살펴보면 개인정보처리시스템에 대한 접근 권한 관리라든지 접근통제 방법과 개인정보의 암호화 보관 기준, 접속기록 점검, 악성프로그램 방지, 단말기 보호 등 IT 정보보호와 관련된 기술적 보호조치가 상당수를 차지함을 볼 수 있다.

개인정보보호법에서 요구하는 개인정보의 안전한 관리와 보호조치 활동은 관리적인 측면 외에도 기술적인 측면을 상당히 중요하게 고려하고 있으며, 이것은 개인정보보호법이라는 법규준수 활동과 IT부문이 떼레야 뗄 수 없는 밀접한 연관성을 갖게 됨을 의미한다고 볼 수 있다.

### 3.3 정보통신망법

정보통신망법에서 언급하는 정보보호조직 관련 요구사항으로는 첫째로 법률 제45조의3에서 정한 바와 같이 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하도록 하는 것을 들 수 있다.

둘째로 법률 제27조에서 정하는 바와 같이 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보 보호책임자를 지정하도록 하였다. 동 법률 시행령 제15조에서는 개인정보의 안전한 처리를 위하여 개인정보 보호책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항을 다시 한 번 강조하고 있다.

정보통신망법에서 언급하는 정보보호조직 관련 요구사항으로 세 번째는 개인정보보호를 위해 「개인정보의 기술적·관리적 보호조치 기준」이라는 고시를 들 수 있다. 본 고시의 주요내용은 개인정보에 대한 불법적인 접근을 차단, 접속기록의 위조·변조 방지, 비밀번호의 일방향 암호화 저장과 주민등록번호, 계좌정보 및 바이오정보 등 암호화 의무 저장, 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치·주기적 갱신·점검 등에 관한 사항이다. 내용에서 알 수 있듯이 대부분 IT정보보호 조직에서 수행하고 점검해야하는 내용으로 구성되어 있음을 볼 수 있다.

### 3.4 금융권 컴플라이언스 평가기준

위에서 살펴본 금융관련 법규 준수를 위한 금융권 컴플라이언스 평가기준은 다음의 Table 2.와 같다.

Table 2. Criteria for financial information security compliance

| No. | Criteria | Related |
|---|---|---|
| 1 | The person responsible for the personal information protection shall be designated as the person responsible for the handling of the personal information | Personal Information Protection ACT |
| 2 | In order to securely manage personal information, it shall designate a personal information protection officer who has expert knowledge and can carry out protective measures. | |
| 3 | Administrative, and physical measures necessary to ensure safety, such as establishing an internal management plan and keeping records of access, so that personal information is not lost, stolen, leaked, counterfeited, altered or damaged. | |
| 4 | It should designate the person responsible for information security as the general manager of the electronic finance business and the information technology sector security on which it is based. | Electronic Financial Transaction ACT |
| 5 | The chief information security officer of a financial institution or an electronic financial service provider can not be a part of other information technology departments. | |
| 6 | In order to secure the security and information of the information communication system, the chief information security officer of the executive level can be appointed. | Information and Communications Network Act. |
| 7 | In order to protect the personal information of the user and handle the user's complaints related to the personal information, the person in charge of personal information management should be appointed. | |
| 8 | Technical and administrative measures shall be taken to prevent loss, theft, leakage, alteration or damage of personal information. | |

## IV. 감독기관 매뉴얼 및 가이드라인 관련

금융회사는 태생적으로 「금융위원회의 설치 등에 관한 법률」에 의거하여 금융위원회와 금융감독원의 관리·감독 하에 놓여져 있다. 따라서 감독기관이 마련한 매뉴얼 혹은 가이드라인, 그리고 감독기관의 공문 등과 같은 행정지도들은 금융회사의 입장에서는 명시적 법률이 아님에도 불구하고 반드시 지켜야할 간접적인 규제의 형태로 인식되는 것이 사실이다[6].

### 4.1 금융감독원 IT부문 실태평가

1999년도 말 정보기술(IT) 활용능력이 금융기관의 생존과 직결되고 사이버거래 등 전자금융이 급속히 확대되어 정보기술 의존도 및 리스크가 증대됨에 따라 금융감독원은 금융기관의 IT경쟁력 제고 및 금융고객 보호를 위하여 주요금융기관을 대상으로 「IT부문 경영실태평가제도」를 도입하였다[7].

IT부문 경영실태평가는 ①IT감사, ②IT경영, ③시스템 개발·도입 및 유지보수, ④IT서비스 제공 및 지원, ⑤IT보안 및 정보보호, 이렇게 5개 분야로 분류되어 운영되고 있으며[8] 본 연구에서 다루고자 하는 정보보호조직과 관련한 평가항목은 IT보안 및 정보보호분야에 있는 CISO와 CIO의 분리운영 여부를 참고하고자 한다.

### 4.2 정보보호수준 진단 자율평가 가이드라인

금융위원회 및 금융감독원은 민간부문의 자율책임 문화조성이라는 금융개혁 방향에 발맞추어 2018년 내 IT리스크 관리 강화를 위해 금융회사의 정보보호 수준 진단을 위한 자율평가 가이드라인을 시행하겠다고 밝힌바 있다[9].

정보보호 담당자에게 사전 검증용으로 배포된 본 가이드라인을 살펴보면 우선, 금융회사 스스로 고유위험을 측정하여 위험점수와 금융회사의 고유위험 수준을 5단계(높음, 약간높음, 보통, 약간낮음, 낮음)로 산출할 수 있도록 하였고, 고유위험에 따라 목표 보안수준(등급)을 설정하고 현재 보안수준을 진단할 수 있도록 마련하였다.

본 연구에서는 정보보호조직 구조 도출을 위한 평가기준으로서 보안수준 진단항목 중 '보안조직 구성 및 운영' 부분과 '보안전담 조직 구성', 그리고 '전략적 연계' 부분을 평가기준으로 활용하고자 한다.

### 4.3 감독기관의 매뉴얼 및 가이드라인 평가기준

금융회사 최적의 정보보호조직을 모색하기 위한 세 번째 평가기준인 감독기관의 매뉴얼 및 가이드라인 평가기준은 다음의 Table 3.과 같다.

## V. 수행방안

### 5.1 선행연구

정보보호조직과 관련한 선행연구들은 주로 거버넌스의 측면에서 경영진의 책임과 역할 정의 그리고 관리체계 수립으로 이어지는 연구가 진행되었다.

한국정보보호진흥원[10]의 연구에서는 정보보호 거버넌스를 조직화함에 있어 경영진의 역할과 책임이 중요하다고 보고 경영진의 유형별로 역할과 책임을 다르게 부여하였다. 또한 정보보호최고책임자

Table 3. Criteria for Supervisory authority manuals and guidelines

| No. | Criteria | Related |
|---|---|---|
| 1 | Is there a working organization approved by top management to systematically implement information security activities? | Self-Evaluation Guidelines |
| 2 | Does the Chief Information Security Officer (CISO) work in the information technology sector? | |
| 3 | Does the dedicated information security organization consist of dedicated personnel who can perform their work independently from other organizations? | |
| 4 | Is the organization dedicated to information protection equal or superior to other organizations? | |
| 5 | Is the disjointed organizational position a direct organizational form beyond the Chief Information Security Officer (CISO)? | |
| 6 | Does your information security strategy take into account all business departments, not just IT departments, and are they aligned with your company's business strategy objectives? | |
| 7 | Is CISO running separately from the CIO? | Evaluation of IT sector |

(CISO)가 정보시스템에 대한 보호로만 역할이 제한되어 정보기술최고책임자(CIO)직속으로 임명되는 체계를 벗어나 정보시스템뿐만이 아닌 전사적인 관점에서 정보보호가 관리되어 CRO 또는 CEO에게 직접 보고하는 조직구조가 바람직하다고 보았다. 한가지 주목할 사실은 정보보호 거버넌스에서는 개인정보보호책임자(CPO)의 역할과 책임이 별도 기술되지 않았다는 점이다.

개인정보보호책임자(CPO)의 책임과 역할은 정보보호 거버넌스가 아닌 개인정보보호 거버넌스라는 별도의 관리체계의 형태에서 두드러지게 나타난다. 김정덕[11]은 개인정보보호 거버넌스의 핵심성공요인으로 '개인정보보호책임자(CPO)의 이사회 참여'와 '개인정보보호책임자(CPO)가 CEO 또는 이사회에 직접 보고'를 꼽을 정도로 개인정보보호 거버넌스에서 차지하는 개인정보보호책임자(CPO)의 책임과 역할은 매우 막중하다고 보았다. 또한 개인정보관리체계를 수립함에 있어 개인정보보호기능은 정보시스템부와 같은 전산조직이 아닌 별도의 전담조직을 구성하거나 위험관리조직에 위치시키는 것이 바람직하다고 보았다.

선행연구들을 참고해 보면 정보보호최고책임자(CISO)와 정보기술최고책임자(CIO), 그리고 개인정보보호책임자(CPO) 저마다의 역할과 책임이 거버넌스 기반 하에 정의가 되어있음을 분명히 알 수 있다. 그러나 이는 이론적인 정의일 뿐 실제 효과성에 대하여는 여전히 불확실한 부분으로 남아있다. 현실에서는 이들 경영진이 겸직을 할 수도 있고, 수직적 상하관계로 맺어질 수도 있으며, 그와는 반대로 서로 완전히 분리되어 존재할 수도 있다. 그리고 이러한 관계유형에 따라 해당조직의 기능과 수행의 효과성은 다를 수 있다.

## 5.2 연구수행

본 연구에서는 정보보호조직 구성 모델 간 최적의 모델을 도출하기 위해 계층화 분석법(AHP - Analytic Hierarchy Process)을 사용해서 분석하고자 한다. AHP분석은 다양한 정보보호조직 구성 형태 간 상대적인 비교를 통해 상대적인 적합도를 체계적으로 점수화할 수 있는 다기준 의사결정(Multi Creteria decision making)기법이기 때문이다[12].

### 5.2.1 정보보호조직 후보군

일반적으로 정보보호조직의 형태는 수많은 유형과 형태를 보일 것으로 예상되나, 실제 보험업권에 속해있는 생명보험 및 손해보험사 중 18개사를 대상으로 정보보호조직 형태를 조사해 본 결과 크게 5가지 유형으로 구분할 수 있었으며 이를 특징별로 구분하여 본 연구에서는 총 6개의 조직 후보군을 대상으로 비교 연구를 진행하고자 한다.(Table 4. 참조)

Table 4. Examples of information security organization types of 18 companies

| type | case | organization type | count |
|---|---|---|---|
| Horizontal | 1-1 | CIO / CISO / CPO | 3 |
| | 1-2 | CIO / CISO (CPO) | 2 |
| Vertical | 2-1 | CIO / CPO / CISO | 2 |
| | 2-2 | CIO / CISO (CPO) | 0 |
| Integrated | 3-1 | CIO (CISO) / CPO | 7 |
| | 3-2 | CIO CISO (CPO) | 4 |
| TOTAL | | | 18 |

### 5.2.2 대상기업의 가정 및 평가척도 결과값 산출

본 연구를 수행함에 앞서 위의 후보군에 대한 대상기업의 가정을 다음의 Table 5.와 같이 정의하기로 한다. 이러한 가정이 필요한 이유는 예를 들면 정보보호최고책임자를 임원급으로 한다는 평가기준 항목에 대하여 사전에 해당기업의 정보보호최고책임자(CISO) 직위를 정해놓지 않으면 올바른 응답을 내릴 수 없기 때문이다

앞서 살펴본 3가지 평가기준, ①공인된 정보보호 관리체계 기준(ISMS/PIMS)와 ②금융권 정보보호 컴플라이언스 기준, ③감독기관의 매뉴얼 및 가이드

Table 5. The basic assumption of the target company

| |
|---|
| **(Assumption 1)** The target company is a company subject to the Information and Communications Network Act. |
| **(Assumption 2)** Target companies are companies with assets of over 2 trillion won. |
| **(Assumption 3)** The information technology chief information officer (CIO), the information security chief information officer (CISO) and the personal information protection person (CPO) of the target enterprise are executive level. |
| **(Assumption 4)** The organization under the Chief Information Technology Officer (CIO) or the Chief Information Security Officer (CISO) is an organization with IT-related expertise. |
| **(Assumption 5)** If the target company has an independent CPO organization, it is assumed that it is CPO and non-IT person from the business. |
| **(Assumption 6)** The person in charge of personal information protection (CPO) of the target company shall also be the person in charge of personal information management prescribed by the Network Law. |

라인 기준으로 5.2.1절에서 마련된 6개의 조직 후보군에 대하여 평가척도 결과값은 Table 6.과 같다.

평가척도 결과값의 산출은 척도리스트의 평가항목에 대하여 각 후보군에서 만족하거나 수행이 가능한 경우 '1'을 부여하고, 그렇지 못할 경우 '0'의 값을 부여하였다.

### 5.2.3 이원비교 및 결과값의 일관성 검증

산출된 결과값을 토대로 계층화 분석(AHP) 진행을 위해 각 후보간 이원비교를 실시하였다. 이원비교는 6개 후보군이 존재하므로 각 평가기준별 총 15번 ($_6C_2$) 비교를 하게 되며 이원비교 시 사용할 척도값은 앞서 구한 각 후보군의 평가기준별 소계값을 사용하였다. 그에 따른 선호도 결과는 Table 7.과 같다.

이원비교행렬의 결과에서 발견할 수 있는 한 가지 흥미로운 점은 각 평가기준별로 가장 높은 선호도를 가진 조직이 조금씩 다르다는 점이다. 공인된 정보보호 관리체계 기준으로만 보자면 1-2(안), 2-2(안), 3-2(안)이 우위를 보이고, 금융권 컴플라이언스 평가기준으로만 보자면 1-2(안), 2-2(안)이, 그리고 감독기관의 매뉴얼 및 가이드라인 기준으로만 보자면 1-1(안), 1-2(안)이 우위에 있음을 알 수 있었다.

Table 6. Evaluation results of candidate organizations

| criteria | No | Horizontal | | Vertical | | Integrated | |
|---|---|---|---|---|---|---|---|
| | | case 1-1 | case 1-2 | case 2-1 | case 2-2 | case 3-1 | case 3-2 |
| ① ISMS/PIMS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 2 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 3 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 4 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 5 | 0 | 1 | 0 | 1 | 0 | 1 |
| | 6 | 0 | 1 | 0 | 1 | 0 | 1 |
| | Tot | 4 | 6 | 4 | 6 | 4 | 6 |
| ② Financial Compliance | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 2 | 0 | 1 | 0 | 1 | 0 | 1 |
| | 3 | 0 | 1 | 0 | 1 | 0 | 1 |
| | 4 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 5 | 1 | 1 | 1 | 1 | 0 | 0 |
| | 6 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 7 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 8 | 0 | 1 | 0 | 1 | 0 | 1 |
| | Tot | 5 | 8 | 5 | 8 | 4 | 7 |
| ③ Manual & guideline | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 2 | 1 | 1 | 1 | 1 | 0 | 0 |
| | 3 | 1 | 1 | 0 | 0 | 0 | 0 |
| | 4 | 1 | 1 | 0 | 0 | 0 | 0 |
| | 5 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 6 | 1 | 1 | 0 | 0 | 0 | 0 |
| | 7 | 1 | 1 | 1 | 1 | 0 | 0 |
| | Tot | 7 | 7 | 4 | 4 | 2 | 2 |

이제 이러한 이원비교의 결과가 연구 초기에 언급했던 바와 같이 일관성이 있는 비교결과인지 확인할 필요가 있다. 통상적인 개개인 설문 형태의 답변을 사용하는 연구와는 달리 본 연구는 대상기업의 가정에 따라 사실위주의 일관성 있는 결과값을 이원비교에 사용했기 때문에 일관성에 있어서는 절대적인 수

Table 7. Preference result of binary comparison matrix

| result / case | ①ISMS /PIMS | ②Compliance | ③Manual & guideline |
|---|---|---|---|
| 1-1 | 0.13 | 0.14 | 0.27 |
| 1-2 | 0.20 | 0.22 | 0.27 |
| 2-1 | 0.13 | 0.14 | 0.15 |
| 2-2 | 0.20 | 0.22 | 0.15 |
| 3-1 | 0.13 | 0.11 | 0.08 |
| 3-2 | 0.20 | 0.19 | 0.08 |
| Total | 1.00 | 1.00 | 1.00 |

치를 보여야 함이 마땅하기 때문이다.

계층화 분석법(AHP)에서 일관성은 일관성 비율(CR[2])을 산출을 통하여 이루어지며 통상적으로 일관성비율(CR)이 0.1 미만인 경우 일관성이 있다고 판단하며, 일관성비율이 0인 경우, 완벽한 일관성을 갖는다고 본다. 본 연구의 이원비교행렬에 대한 일관성 비율은 모든 평가기준에 대하여 CR=0의 값을 갖는 것으로 계산되었으며 이는 후보군별 사실관계에 기반한 일관성 있는 조사 결과값을 사용하였기 때문인 것으로 충분히 예상할 수 있었다.

#### 5.2.4 상대적 중요도 부여 및 최종 적합도 산출

계층화 분석법(AHP)에서는 평가기준별로 중요도에 따라 가중치를 두어 결과에 반영할 수 있으며 본 연구에서는 두 번째 기준인 '컴플라이언스 준수'에 대하여 법률로써 갖는 강제성과 구속력을 감안하여 나머지 두 가지 기준보다 약간의 중요도를 높이는 방향으로 연구를 진행하였고, 그에 따라 부여한 각 기준별 중요도는 Table 8.과 같다.

이제 이원비교를 통해 산출된 평가기준별 선호도와 평가기준별 상대적 중요도를 사용하여 각 후보군별 최종 적합도를 산출해보기로 한다. 가중합계를 구하는 방법을 1-1(안)의 예를 들어 살펴보면 아래와 같은 산식으로 표현할 수 있다.

i.g. 1-1(안)의 가중합계(최종적합도) =

$= \sum$ (평가기준별 선호도)

$= (0.13\times0.3) + (0.14\times0.4) + (0.27\times0.3)$

$\fallingdotseq 0.17$

위와 같은 방식으로 나머지 후보군에 대하여 구한 가중합계(최종 적합도)와 그에 따른 순위는 Table 9. 그리고 이를 나타낸 그래프는 Table 10.과 같다.

최종 적합도 결과를 통해 알 수 있는 점은 여러 평가기준(공인된 정보보호관리체계 기준, 금융권 컴플라이언스 평가기준, 감독기관의 매뉴얼 및 가이드라인 기준)을 고려할 때 금융권 정보보호조직으로서 가장 바람직한 역할수행을 기대할 수 있는 조직구성은 1-2(안)으로서 정보기술최고책임자(CIO)과 정보보호최고책임자(CISO)가 대등하게 상호 독립적으로 위치하며 정보보호최고책임자(CISO)는 전사 개인정보보호까지 총괄하여 개인정보보호책임자(CPO)역할을 겸하는 조직임을 알 수 있었다.

2) 일관성비율(CR : Consistency ratio)로서 CI / RI로 이루어지며 CI(Consistency Index)는 일관성지수를, RI(Random index)는 무작위지수로서 이원비교를 무작위로 생성했을 때의 일관성지수로서 n이 6일때의 RI는 1.24를 사용한다.

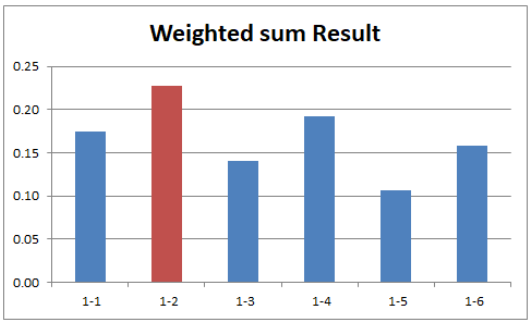
Table 8. Relative Weight by Evaluation Criteria

| Div | ① ISMS /PIMS | ② Compliance | ③ Manual & guideline | Total |
|---|---|---|---|---|
| Relative Weight | 0.3 | 0.4 | 0.3 | 1.0 |

Table 9. Weighted sum Result

| result / case | Weighted sum | Rank |
|---|---|---|
| 1-1 | 0.17 | 3 |
| **1-2** | **0.23** | **1** |
| 2-1 | 0.14 | 5 |
| 2-2 | 0.19 | 2 |
| 3-1 | 0.11 | 6 |
| 3-2 | 0.16 | 4 |
| Total | 1.00 | - |

Table 10. Weighted sum Result Graph




## VI. 결 론

최적의 정보보호조직 구성을 찾기 위한 세 가지 평가 기준들 첫째, 공인된 정보보호 관리체계 기준과 둘째, 금융권 컴플라이언스 준수 기준, 그리고 셋째 감독기관의 매뉴얼 및 가이드라인 기준을 토대로 도출한 최적의 정보보호조직 구성형태는 정보기술최고책임자(CIO)과 정보보호최고책임자(CISO)가 대등하게 상호 독립적으로 위치하며 정보보호최고책임자(CISO)는 전사 개인정보보호까지 총괄하여 개인정

보보호책임자(CPO)역할을 겸하는 조직이었다.

여기서 이야기하는 '상호 독립적으로 위치한다'는 의미는 금융회사에 있어서 정보보호부문과 정보기술부문을 동일 조직에서 수행함으로 얻을 수 있는 운영상의 편익보다 독립적인 위치에서 수행하는 불편함에서 오는 보안상의 유익이 더 중요함을 의미한다고 할 수 있으며, '개인정보보호책임자(CPO)와 정보보호최고책임자(CISO)의 겸직'이 주는 의미는 금융회사에 있어서 정보보호와 개인정보보호는 상호 업무 유사성을 가지고 있어 분리된 조직으로 나뉘어 있는 비효율을 최소화하고 IT전문성을 포함하고 있는 단일 조직에서 책임감있게 업무 수행을 하는 것이 훨씬 효과적이라는 것을 의미한다.

본 연구는 정보보호업무를 여전히 IT보안의 영역으로만 바라보는 대다수의 금융회사들과 개인정보보호조직과 정보보호조직의 역할은 다르다고 생각하는 금융회사들에게 의미있는 결론을 제시한다고 생각한다. 아무쪼록 본 연구를 통해 금융회사의 정보보호조직 구성을 고민하는 이와 기업에게 조금이나마 나은 방향을 제시할 수 있기를, 그래서 해당 기업의 정보보호수준을 향상시키는데 도움이 되기를 기대해본다.

## References


[1] Financial Services Commission "Comprehensive measures to strengthen financial computer security", pp,13, Jul. 2013

[2] Ministry of Science and Technology, No. 2015-0324 "Designation of Information Security Management System Certification Body", Jul. 2015

[3] Korea Internet & Security Agency (KISA), "Information Security Management System (ISMS) Certification Guidebook", pp. 38, April 2017

[4] Korea Internet & Security Agency (KISA), "PIMS Certification Guidebook (Volume 1) - Operating System", pp.18-19, April 2017

[5] Financial Services Commission, Financial Regulatory Complaints Portal, http://better.fsc.go.kr/fsc/subIndex/72.do, 2017-12-18

[6] Financial Services Commission, "Shadow Regulation Improvement by Administrative Guidance", Sep, 2015

[7] Financial Services Commission, "Strengthening Information Technology (IT) Sector Inspection of Financial Institutions", December 1999

[8] Financial Supervisory Service, "IT Inspection Service Guide (January, 17)", Feb, 2017

[9] Financial Supervisory Service, "Holding a Briefing Session on Supervision and Inspection of the IT & FinTech Division in 2018", Mar, 2018

[10] Korea Information Security Agency "Standardization Study on Information Protection Governance for Information and Communication Companies", pp. 80-83, Dec. 2008

[11] Kim, Jeong-Deok, "A Study on the Key Success Factors for Effective Implementation of Personal Information Protection Governance" Jonornal of The Korea Institute of information Security & Cryptology, 21(5), pp. 199-201, Oct. 2011

[12] Thomas L. Saaty, "Analytic Hierarchy Process. In: Gass S.I., Fu M.C. (eds) Encyclopedia of Operations Research and Management Science", Springer, Boston, MA, 2013

## 〈저자소개〉

김 상 호 (Sang-ho Kim) 정회원
2004년 2월: 서강대학교 컴퓨터학과 졸업
2016년 9월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 전자금융보안, 전자금융법규, 개인정보보호

김 인 석 (In-Seok Kim) 정회원
2008년: 고려대학교 정보경영공학과 박사
2011년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 전자금융보안, 전자금융법규, 개인정보보호