J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

정보보호 관리체계를 위한 주요 통제영역 연구: 금융 관련 조직을 중심으로☆

A study on primary control area for information security management system (ISMS): focusing on the finance-related organizations

강 윤 철[1] 안 종 창[2*]
Youn-chul Kang Jong-chang Ahn

요 약

금융서비스산업 전반에 고객의 금융정보 및 금융서비스를 적절하게 보호하고 유지하기 위해, 조직은 정보보호 관리체계(ISMS), 개인정보보호 관리체계, 비즈니스연속성 관리체계와 같은 경영시스템을 도입하여 운영하기 시작하였다. 본 연구는 금융권이 ISMS를 고려하는 것이 바람직하며 정보보안 문화, 실무 및 가이드라인을 고려하는 다양한 조직 안에 각기 다른 형태를 가질 수 있다는데서 출발하였다. 금융서비스산업 내에서도 분야에 상관없이 적용 가능하고 보편적으로 널리 알려진 국제 정보보호 관리체계 ISO27001을 도입한 금융 관련 조직을 대상으로 인증 심사에 따른 부적합 추이 및 통제 요인의 분석을 통해 해당 ISMS의 주요 통제 영역을 도출하게 된다. 이에 따라 ISMS를 도입하여 운용하고 있는 금융 관련 5개 조직의 사례분석을 통해 정보보호 수준의 개선 효과를 분석해 보고자 했다. 금융 섹터에서 인증을 유지하고 있는 곳이 적어 실증 연구를 위한 자료 확보가 어려웠지만, 초기 연구 대상으로서의 의미가 있는 것으로 분석되었다. 분석을 통해, 대상 업체들에서 최초심사로부터 3년 주기가 지나는 동안 부적합 건수가 매년 감소하고 있음을 확인할 수 있었다. 부적합 빈도수가 가장 높았던 물리적 환경적 보안, 의사소통 및 운영관리, 접근통제 영역이 각 23%, 19%, 17%를 나타내 전체 부적합의 59% 정도를 차지하는 주요 통제영역으로 도출되었다. 이를 통해 금융권에서 중요하게 다루어지지 않았던 기술적, 관리적, 물리적 보안 이슈를 ISMS가 충족시키고, ISMS가 금융서비스산업에 적용 가능한 효과적인 관리체계가 될 수 있음을 발견하였다.

☞ 주제어 : 개인정보보호 관리체계, 부적합 추이, 비즈니스연속성 관리체계, 인증 심사, 정보보호 관리체계, 통제 영역

ABSTRACT

Financial service industry has introduced and operated management systems such as information security management system (ISMS), personal information security management system, business continuity management system to protect and maintain suitably customer's financial information and financial service. This study started that it's desirable financial industry takes consideration of ISMS and it can be different types among various organizations taking consideration of culture, practical work, and guideline of information security. The study derives primary control areas of ISMS through analyzing non-conformity trends and control factors according to certification audit for finance-related organizations introduced international ISMS of ISO27001 which is well known and commonly applicable irrespective of areas in financial service industry. Through case analyses for five finance-related organizations operating ISMS, this study analyzed improvement effects of ISMS. It has a meaning as an initial research though it was difficulty in acquiring data for empirical study because of rare organizations maintaining certification in financial sector. As a result, number of non-confirmity from the first audit to three years' elapse was decreased every year. Physical and environmental security, communication and operations management, and access control having the highest frequency of non-conformity each presented 23%, 19%, and 17%, which reached 59% in total and they are derived into primary control areas. ISMS can fulfill technical, managerial, physical security issues, which have

1 Department of Digital Management, Korea University, Seoul, 30019, Korea.
2 Department of Information Systems, Hanyang University, Seoul, 04763, Korea.
* Corresponding author (ajchang@hanyang.ac.kr)
[Received 7 August 2018, Reviewed 21 August 2018, Accepted 14 September 2018]

☆ 이 논문은 2018년도 한국인터넷정보학회 춘계학술대회 우수논문 추천에 따라 확장 및 수정된 논문임
☆ 이 논문은 한양대학교 교내연구지원사업으로 연구되었음 (HY-2017년도)

not been treated importantly in financial industry. In addition, this study presented that ISMS can be an effective management system applicable for financial service industry.

☞ keyword : Personal information security management system; Non-conformity trends; Business continuity management system; Certification audit; Information security management system; Control area

1. 서 론

정보보호 관리체계(ISMS; Information Security Management System)는 정보보호가 기업의 비즈니스 경영 방침과 연계될 수 있도록 정보보호 최고책임자를 지정하고 위험분석을 통한 정보보호정책을 수립하여 그에 대한 정보보호 활동을 전개할 수 있도록 하는 체계이다. 또한 정보보호 관리체계(이하 ISMS로 약칭함)는 정보보호 정책에 따라 수행된 정보보호 활동을 모니터링 및 검토하여 지속적으로 개선할 것을 요구한다. 이러한 일련의 과정을 통해 ISMS를 구축한 조직은 정보보호 정책과 활동의 일관성을 확보하여 보다 효과적인 정보보호 체계를 구축할 수 있도록 한다[1].

금융권 역시 2014년 말부터 ISMS인증이 의무 시행되어오다 2016년 5월 대통령소속 규제개혁위원회에서 격론 끝에 금융기관은 ISMS 인증 의무화 대상에서 제외되고 금융권의 자체적인 자율규제로 전환하기로 결정하였다[2]. 그 후 의무대상은 아니지만 상당수 금융사가 자율보안체계 확립차원에서 ISMS 인증을 획득하고 있다. 또한 금융보안원은 금융보안 관련 규정 및 표준을 참고해 2017년 상반기 정보보호 정책과 접근통제, 운용보안, 시스템 개발보안, 물리적 보안 등을 강화하고 정보보호 관련 국제 표준인 ISO27001, PCI-DSS 등도 일부 준용하여 금융권에 적합한 ISMS 인증기준 점검항목(총 324개)을 공개하였고 2018년 전면 적용 중이다. 참고로 2017년 7월 기준 금융보안원에서 ISMS 인증서를 발급한 곳은 시중은행 8개를 비롯해 46개사이다[3].

이처럼 금융권의 정보보안 조직도 ISMS를 고려하는 것이 바람직하며, 정보보안 문화, 실무 및 가이드라인을 고려하는 다양한 조직 안에서 ISMS는 각기 다른 형태를 가질 수 있다[4]. 이에 따라 본 연구에서는 ISMS를 도입하여 운용하고 있는 금융 관련조직의 사례 분석을 통해 정보보호 수준의 개선 효과를 분석해 보고자 한다. ISO27001 인증 비교 대상 사례 기업들을 분석한 결과, 이 인증을 받은 모든 업체에서 최초심사로부터 3년 주기가 지나는 동안 부적합 건수가 매년 감소하고 있음을 확인할 수 있었다. 최초심사 기준으로 적게는 27%, 많게는 100%의 개선이 이루어졌다.

다음 장에서는 먼저 ISMS 관련 선행연구와 국내외 참조 모델을 살펴본다. 이어서 선행 연구 방법론을 고려하여 국내 5개 금융관련 조직의 사례를 분석한다. 마지막으로, 분석 결과를 바탕으로 연구의 의의, 한계점, 추가 연구 방향을 논의하게 된다.

2. 선행연구와 참조모델

2.1 ISMS 선행연구에 대한 검토

국제 표준인 ISO27001인증과 KISA-ISMS인증을 통해 정보보호 수준이 개선되거나 정보보호 통제항목 도출에 활용할 수 있다는 것을 검증한 국내외 선행연구를 보면 다음과 같다.

ISMS 기반의 초기 연구로는 BS7799에 기반한 ISMS를 공공기관에 적용하고자 한 전용준 외의 연구[5]가 있다. 본격적인 ISMS 관련 주요 연구로는 Kim 외(2017)[6]와 Jo 외(2011)[7]의 연구가 있다. 각각 ISMS를 설명하고 비교연구를 수행 하였다. Jo 외의 연구는 다양한 ISMS들을 비교하고 조직이 정보보안 수준을 참조하고 향상시킬 수 있는 새로운 정보보호관리 평가모델을 제공하고 있다[7]. Kim 외의 연구는 국내의 ISMS 보안통제에서 발생한 보안흠결의 상호 관계를 분석하고 각 보안 통제의 상대적 중요도를 측정하였다. 두 집단으로 설계된 사례통제 연구(case-control study)를 통해 전문가 인터뷰나 비교연구의 단점인 주관적인 편견(bias)을 제거하고자 했다[6].

김지숙 외의 연구[8]에서는 민간영역과 공공영역 정보보호관리 통제항목을 매핑하고 각 영역별 결함사항을 분석하였다. 연구 방법으로는 정보보안 인증 유효기간 3년에 걸쳐 수행한 각 업체들의 결함 수 및 결함 개선 추이를 확인함으로써 세부 통제항목별 결함 건수 및 발생빈도를 도출 하였다. 이를 통해 민간영역과 공공영역의 특성에 따라 정보보호 통제항목을 보강하고 관리 프로세스가 제대로 가동되는지를 점검하는 방향으로 나아가야 함을 제시하였다[8].

김환국 외의 연구[9]에서는 ISMS 인증제도 도입 및 임원급 정보보호 최고책임자(CISO) 지정 등 정보통신망법

개정에 따른 기업 정보보호 관련 제도현황 및 ISMS 인증 제도 유형을 소개하였다. 경영진 참여 및 책임 강화, 정보보호 조직 구성 강화, 모바일 기기 보안 강화, 주요 직무자 인터넷 접속 제한을 강조 하였다. 또한 이제는 기업의 정보보호를 지출해야하는 비용의 개념이 아니라, 비즈니스 기회를 예측하고 현재와 미래의 위험에 적절히 대응할 수 있는 핵심 경쟁력인 동시에, 예상하지 못한 위기상황에서 기업전반의 비즈니스 안정성을 유지하고 정보자산을 적절하게 보호하기 위한 경영활동의 일부로 보아야 한다고 주장하였다[9].

장상수와 이호섭의 연구[10]에서는 고객의 지불, 결제 정보를 취급하는 금융 및 전자결제 서비스 기업을 포함한 ISMS 인증심사 수행결과를 토대로 주요 결함을 도출하고 주요 결함에 대한 보안조치 방안을 제시 하였다. 특히 아래 그림 1처럼 국내 ISMS와 국제 ISMS 간의 국내외 인증표준을 구성하고 있는 통제항목별 세부 보안 통제항목간의 매칭이 가능함을 보여주었다[10]. 이는 ISO27001 통제항목을 활용한 분석이 국내 ISMS에 충분히 연계될 수 있음을 나타낸다.

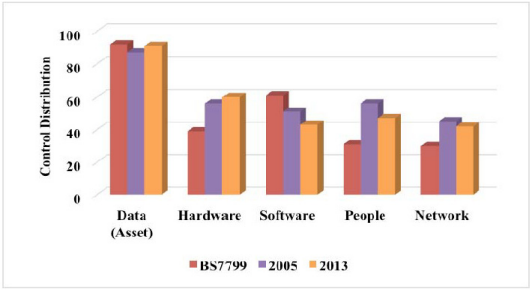
1	정보보호 정책	5	5	보안정책	2
2	정보보호 조직	4	6	정보보안 조직	11
3	외부자 보안	4	7	자산 관리	5
4	정보자산 분류	4	8	인원 보안	9
5	정보보호 교육 및 훈련	4	9	물리적/환경적 보안	13
6	인적보안	5	10	통신 및 운영 관리	32
7	물리적 보안	12	11	접근 통제	25
8	시스템개발 보안	13	12	정보 시스템 취득, 개발, 유지보수	16
9	암호통제	3	13	보안 사고 관리	5
10	접근통제	14	14	사업 연속성 관리	5
11	운영관리	22	15	준거성	10
12	전자거래 보안	5		합계	133
13	보안사고 관리	7			
14	검토, 모니터링 및 감사	11			
15	업무연속성 관리	7			
	합계	120			

(그림1) 국내 ISMS와 ISO27001 통제항목별 연관도
(Figure 1) Degree of relationship among control items of domestic ISMS and ISO27001

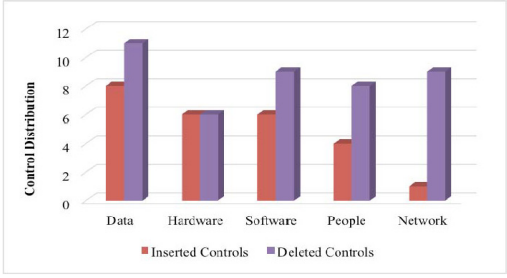
Boehmer는 2008년 ISO27001을 기반으로 ISMS의 부적합추이를 포함하여 효과성 및 효율성을 평가하고자 관련 핵심성과지표(Key performance indicator; KPI)를 분석하여 성과측정 메트릭스를 제시하였다[11].

Sharma와 Dash 연구[12]에서는 인도에서 ISO27001에 대한 이행이 정보보안 사고에 대해 효과적인 보호체계이고, 금융 분야 조직 운영에 도움이 된다는 가설을 바탕으로 ISO27001 도입의 긍정적인 측면을 제시하였다. 이 과정에서 ISO27001인증 조직 545개 중 정량적 데이터 수집을 위해 15개 조직을 최종 선정하여 연구를 진행 하였다[12].

Shojaie 외[13]의 연구에서는 그림 2와 그림 3처럼 ISO27001의 2005년 버전과 2013년 버전을 비교 분석하여 주요 통제 영역을 데이터, 하드웨어, 소프트웨어, 사람 및 네트워크로 분류하였다. 또한 버전별 차이점을 기술하고 주의 깊게 다루어야 할 영역을 제시하였다[13].



(그림 2) 5개 범주에 기반 한 BS7799, ISO 27001:20005, ISO 27001:2013의 비교
(Figure 2) Comparison among BS7799, ISO 27001:20005 and ISO 27001:2013 based on five categories



(그림 3) 5가지 범주에 기반 한 ISO 27001:2005에서 삭제된 통제와 ISO 27001:2013에 추가된 통제의 비교
(Figure 3) Comparison between deleted controls from ISO 27001:2005 and inserted controls into ISO 27001:2013 based on five categories

본 연구에서는 이러한 선행 연구들의 연구 방법론에 입각하여 국내 ISMS의 바탕이 되는 국제 ISMS ISO27001 인증심사를 수행한 금융 관련 조직을 대상으로 정보보호

를 위한 주요 통제 영역을 분석해 보고자 한다.

2.2 국내/외 연구참조 모델

2.2.1 국내 ISMS : KISA-ISMS

정보보호 분야의 국제인증인 ISO27001을 바탕으로 국내 실정에 좀 더 적합하게 제정 및 법제화한 국내 ISMS 인증제도는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조에 따라, 기업 또는 조직의 ISMS가 인증기준에 적합한지를 독립적이고 객관적인 입장에 있는 제3의 인증기관이 평가하여 인증을 부여하며, 이를 위해 ISMS에 대한 표준적 모델 및 기준을 제시한다. 인증제도의 공정성과 객관성을 확보하기 위해 한국인터넷진흥원 외에도 한국정보통신진흥협회(2014.5), 한국정보통신기술협회(2015.2), 금융보안원(2015.7)이 인증기관으로 추가 지정되어, 인증제도의 효율성을 높이는 노력이 계속되고 있다[1].

ISMS 인증심사 기준은 2002년 제도도입 이후 2013년 방송통신위원회고시(제2013-4호)로 개정기준을 공표하였으며, 아래 표 1과 같이 정보보호 관리과정(5단계, 12개 통제항목)과 정보보호대책(13개 분야, 92개 통제항목)의 두 가지로 구성되어 있다.

이는 2011년 12월 개정된 '정보통신망법'에 따라 기존의 실효성이 낮은 점검항목을 통합하고 최신 보안관리 기준을 반영하는 등 인증 심사 기준의 통제항목을 137개에서 104개로 변경한 내용이다. 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 연간 매출액 또는 세입 등이 1,500억 원 이상 이거나 정보통신서비스 부문 전년도 매출액이 100억 원 이상 또는 3개월간의 일일평균 이용자수 100만 명 이상으로, 대통령령으로 정하는 기준에 해당하는 자 등 '정보통신망법'에 따른 의무대상자*외 자율신청기업**이 인증 취득을 희망할 경우에도 자율적인 신청을 통한 인증 심사가 가능하다. 국내 ISMS 인증서는 2002년 최초 인증서를 발급한 이후, 아래 표 2처럼 2015년 12월까지 527건(누적)의 인증서가 발급되었으며[1], 2017년 4월 기준으로 총 659건 발급, 455건***이 유지되고 있다.

(표 1) ISMS 인증 기준
(Table 1) ISMS certification criteria

Class	Control group	No. of controls	No. of detailed controls
Security Mangagement Process (SMP)	1. Establishment of Security Policies & Setting ISMS Scope	2	5
	2. Responsibilites and Security Organization	2	5
	3. Risk Management	3	11
	4. Implementation of Security Coutermeasures	2	3
	5. Post Management	3	8
Sum		12	32
Security Counterm easure Process (SCM)	1. Security Policies	6	12
	2. Security Organization	4	9
	3. Security of External Parties	3	6
	4. Information Asset Classification	3	9
	5. Education and Training on Information Security	4	10
	6. Personal Security	5	14
	7. Physical Security	9	20
	8. System Development Security	10	32
	9. Cryptography Security	2	5
	10. Access Conrtrol	14	19
	11. Operations Security	22	67
	12. Intrusion Incident Handling	7	19
	13. IT Disaster Recovery Planning	3	7
Sum		92	229
Total sum		104	261

(표 2) 국내 ISMS 인증서 누적 발급 건수 (단위: 건)
(Table 2) Cumulative issuing number of domestic ISMS certification (unit: item)

Year	2010	2011	2012	2013	2014	2015
Issuing no.	99	126	151	278	482	527

2.2.2 국제 ISMS : ISO/IEC 27001

현재 ISO/IEC 27001:2013으로 표기****되고 ISMS라고도 불리는 국제 ISMS는 정보보안 경영체계라 불리기도 하며 조직의 정보 자산이 적절히 보호되고 있는지를 인증

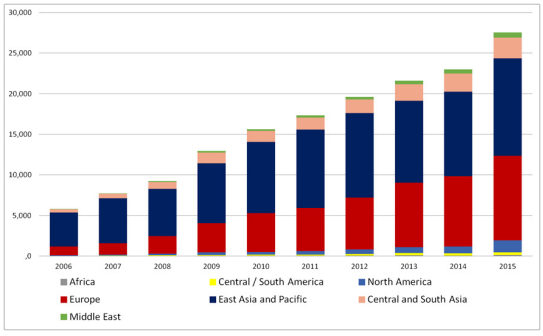
* '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제47조 제2항 의무대상자
** 의무대상자 외 기업
*** 한국인터넷진흥원 2017년 4월 인증서 발급현황 참조

**** 인증 규격은 관련 기관명, 해당 인증명, 발행년도 순으로 표기하며 여기서, ISO는 International Organization for Standardization(국제표준화기구)를 IEC는 International Electrotechnical Commission(국제전기표준회의)을 의미함

하는 것으로, 조직이 위험평가를 실시하고 적절한 통제를 구현하여 국제적으로 인지되는 ISMS 규격에 적합한 정보보호를 이행하여 왔음을 입증하는 것이다. 이는 PDCA (plan-do-check-action) 사이클에 따라 지속적인 개선을 추구하며 조직의 규모에 상관없이 모든 산업분야에 적용 가능하다[14, 15].

ISO27001 요구사항의 구성을 살펴보면 최신 버전인 ISO27001:2013 규격의 경우 7개 조항(4조~10조) 및 부속서의 14개 통제분야, 114개 통제항목으로 구성되어 있으나* 본 연구의 사례에서 다룰 ISO/IEC 27001:2005 규격은 5개 조항(4조~8조)과 부속서의 11개 통제분야, 133개 통제항목으로 구성되어 있다[15].

국제 ISMS 즉, ISO27001 인증서는 그림 4처럼 2015년 기준으로 전 세계 약 27,536개, 한국에서는 2015년 기준 305개의 ISO27001 인증서가 유지되고 있다. 산업별 섹터는 표 3과 같이 39개로 구분되며 세계 상위 5개 산업별 섹터는 정보기술 분야(33번 코드)를 비롯하여 다른(other) 서비스(35번), 교통/저장장치/통신(31번), 전기와 광 장비(19번), 건강과 사회사업(38번) 이다[15].



(그림 4) 전 세계 ISO27001 인증 추이 (단위: 건)
(Figure 4) Trends of world ISO27001 certification (unit: item)

(표 3) 산업별 인증
(Table 3) Certification by jndustrial sector

EA* Code No.	ISO/IEC 27001 by Industrial Sector
1	Agriculture, fishing
2	Mining and quarrying
3	Food products, beverages and tobacco
4	Textiles and textile products
5	Leather and leather products
6	Wood and wood products
7	Pulp, paper and paper products
8	Publishing companies
9	Printing companies
10	Manufacture of coke & refined petroleum products
11	Nuclear fuel
12	Chemicals, chemical products & fibres
13	Pharmaceuticals
14	Rubber and plastic products
15	Non-metallic mineral products
16	Concrete, cement, lime, plaster, etc.
17	Basic metal & fabricated metal products
18	Machinery and equipment
19	Electrical and optical equipment
20	Shipbuilding
21	Aerospace
22	Other transport equipment
23	Manufacturing not elsewhere classified
24	Recycling
25	Electricity supply
26	Gas supply
27	Water supply
28	Construction
29	Wholesale & retail trade; repairs of motor vehicles, motorcycles & personal & household goods
30	Hotels and restaurants
31	Transport, storage and communication
32	Financial intermediation, real estate, rental
33	Information technology
34	Engineering Services
35	Other Services
36	Public administration
37	Education
38	Health and social work
39	Other social services

* EA= European Accreditation

2.2.3 국제금융서비스 정보보호가이드 ISO/IEC TR 27015

ISO/IEC TR 27015는 금융 서비스에 대한 정보보호체계 가이드라인(Information technology - Security techniques - Information security management guidelines for financial services)이다(ISO/IEC TR 27015:2012). 이는 금융서비스를 제공하는 조직 내 정보보호에 대한 착수, 구현, 유지관리

* ISO27001:2013 Requirement, ISO 2013년 9월 25일 발행 기준

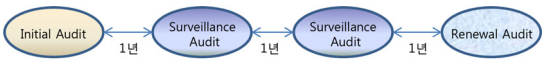
및 개선을 위하여 ISO/IEC27002에 기술된 통제영역에 대한 구현 지침 이외의 추가적 또는 보완적인 내용을 제공한다.* 앞서 설명한 ISO/IEC 27001:2005의 부속서 ISO/IEC27002가 11개 도메인 133개 통제항목에 대한 일반적인 구현 지침을 기술하고 있다면, 이 가이드라인은 ISO/IEC27002:2005를 기반으로 금융서비스 분야에 적용되는 30개 통제항목에 대한 보완적인 구현 지침을 기술하고 있다. 현재 금융거래를 이용하는 고객 정보 및 금융거래 정보를 포함하여 관련 정보에 접근하는 인력, 금융정보 처리, 결제 장비 및 금융업에 관련된 법률 등의 사항들을 반영하고 있으며 ISO/IEC27001과 ISO/IEC27002가 지난 2013년 9월 25일 개정됨에 따라 ISO27015도 일부 개정 가능성이 있다. 본 연구에서는 ISO27001의 금융서비스 영역을 지원하는 ISO27015와의 연계 설명을 위해 ISO27001:2005년 규격을 대상으로 한다. 또한 ISMS 도입을 통한 금융 관련 조직의 정보보호 주요 통제영역 분석을 통해 해당 통제영역에 매핑 되는 가이드의 추가 통제영역도 제시해 보고자 한다.

3. 사례 분석

3.1 ISO27001 적용 주요사항

국내에서도 분야 구분 없이 ISMS를 구축하고 해당 국제인증인 ISO27001 인증을 받은 기업들이 증가하고 있으며, 그 중 국내 금융서비스산업 내 ISMS를 구축 및 운영하고 있는 기업들을 대상으로 연구를 진행하였다.

기본적으로 ISO 인증심사는 그림 5처럼 크게 최초심사, 사후심사 그리고 갱신 심사로 구성된다. 이는 KISA-ISMS의 인증프로세스와 동일하다.



Type	Contents
Initial Audit	It is conducted in the first applying for certification or according to an important change in certification scope
Surveillance Audit	It is conducted in order to execute post-management each year after certification including certification update
Renewal Audit	It is conducted in applying for certification again due to the expiration of certification duration

* 인증심사 종류는 https://isms.kisa.or.kr/ 참조

(그림 5) 인증심사종류

(Figure 5) Type of certification audit

* 2013.09.26, 금융보안연구원, ISO/IEC TR 27015:2012 요약보고서

최초심사와 갱신 심사는 문서심사와 현장심사로 구성되며, 사후심사에서는 현장심사만 진행한다. 최초심사 후 매년 1회 이상의 사후 심사를 수행해야하며 인증 유효기간인 3년이 경과하면 갱신 심사를 통해 최초심사와 마찬가지로 새롭게 인증심사를 진행한다. 이는 주위 환경이 급격히 변함에 따라 관련 이슈에 대한 사항이 많이 달라졌음을 인정하는 것이며, 달라진 규격 요건이나 법적 요소들을 반영하여 정보보안 수준을 지속적으로 개선시켜 나갈 수 있다. 인증 심사에서 발생한 부적합(Nonconformity)은 중부적합과 경부적합으로 나뉘며, '중부적합(Major Nonconformity)'은 정보보안경영시스템에 중대한 영향을 미치는 발견사항을 의미하고, '경부적합(Minor Nonconformity)'은 정보보안경영시스템(ISMS)에 중대한 영향을 미치지 않는 발견사항을 의미한다. 부적합 사항 외 객관적인 증거부족으로 부적합 판정이 어려운 경우 또는 관리부재로 인해 부적합/손실로 악화될 수 있는 경우에는 '관찰사항(Observation)'으로 분류하는데 심사원의 판단 및 경험으로 개선이 권고되는 경우 '개선권고사항(Opportunity or improvement)'으로 분류할 수 있다.

최종 결과에서 중부적합이 없는 경우 인증 추천이 이루어지며, 경부적합만 발견되는 경우, 인증 유지/추천이 가능하나 시정조치계획의 제출 및 시정조치의 유효성을 검증해야 한다. 끝으로 모든 인증제도는 인증 신청기관의 심사범위(Audit scope)에 대해 인증심사 시점에서 인증기준의 적합성 여부를 심사하는 것이다. 따라서 조직이 인증을 받는다는 의미가 정보보안과 관련된 어떠한 침해나 유출사고가 발생하지 않는다는 것을 담보하는 것이 아니므로, 조직은 보안 수준의 지속적인 유지 및 향상을 위해 끊임없이 노력을 기울여야 한다.

본 연구에서는 다음의 이유로 ISO27001:2005 규격 기준으로 분석이 진행되었다.

1) ISO27001:2013 규격에 대한 국내 인증심사는 2014년 하반기부터 이루어져 현 시점에서 최초심사 및 전환심사 후 3년 주기의 인증 사이클을 충족한 조직의 자료가 충분하지 않다.
2) ISO27015:2012의 통제항목은 ISO27001:2013규격에 맞춰 개정되지 않아 아직 ISO27001:2005규격 기준이다.

3.2 ISMS 구축 전과 후 비교

3.2.1 대상 기업 선정 및 측정 지표

앞서 살펴본 표 3의 EA 코드에 따라 분류된 Financial

intermediation, real estate, renting 섹터(코드번호 32)의 국내 ISO27001인증은 2015년 기준 3건에 불과하며 Information technology(정보기술)의 경우 58건으로 확인 된다. 이는 일부 응답자가 자료를 제공하지 않은 부분도 있겠지만 국내 금융사의 경우 IT주관 부서 또는 IT전담 자회사 등에서 IT 섹터 인증을 획득한 경우도 있기 때문인 것으로 보인다. 따라서 분석 대상 기업 선정 방법은 ISO27001 인증을 받은 국내 전체 기업 중 조직의 규모에 관계없이 정량적 데이터 수집이 가능한 금융사, 카드사, 금융 회계 및 IT지원 서비스 사 38곳을 우선 선정하고 3년 인증 주기 동안의 데이터를 제공받을 수 있는 금융 관련 조직 다섯 곳을 최종 선정 하였다.

해당 조직은 표 4와 같이 시중은행 한 곳과 해당 금융기관에 IT솔루션 서비스를 제공하는 업체 한 곳, 시가총액 약 18조에 해당하는 시중은행 및 카드사에 IT운영 서비스를 제공하는 업체 한 곳과 해당 금융기관의 제휴 카드사 한 곳, 회계법인 한 곳까지 금융권 대기업을 중심으로 선정하였다. 상세 자료는 실무자 협의를 거쳐 연구 목적에 필요한 최소한의 정보만을 활용하기로 하였다. 분석 대상 업체는 2009년 또는 2010년 이후에 최초심사가 진행되어 3년 주기의 인증 사이클에 따라 2013년까지 사후심사가 완료되었다.

(표 4) ISO27001 도입에 따른 정보보호 수준 개선효과 분석 대상 업체

(Table 4) Analysis target organizations for improvement effect of information security level according to ISO27001 introduction

Organization	Revenue (million won)	Number of employees	Number of staffs working for information security under certification range
A	over 3,000,000	over 780	about 100
B	over 170,000	over 2,000	about 2
C	over 57,000	over 620	about 6
D	over 300,000	over 840	about 4
E	over 20,000,000	over 15,000	about 4

국내에서 ISO27001 인증을 받은 업체가 2015년 기준 305개지만 금융섹터로 분류되어 인증을 유지하고 있는 곳은 매우 적은 편이며, Sharma와 Dash의 연구[12](전체 545곳 중 최종 15곳 선정)처럼 실증적인 연구를 위한 자료 확보가 어려운 점을 감안하면 적은 조직 숫자라도 초기 연구 대상으로서의 의미가 있을 것으로 예상하였다.

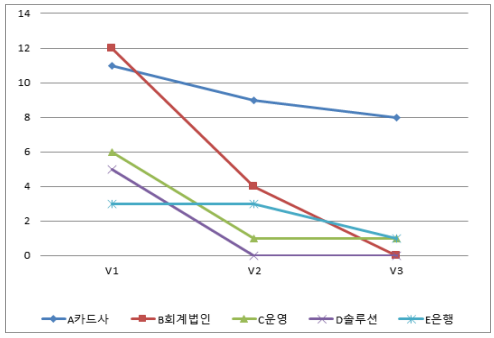
측정 지표로는 Boehmer 연구[11]에서도 사용된 ISO27001:2005 인증심사 보고서의 '부적합 수'를 바탕으로 각 업체의 ISMS 구축 후 최초심사에서 발견된 부적합 건수가 매년 사후심사가 진행됨에 따라 얼마나 감소하는지에 대한 통계치를 분석해 보기로 하였다. 즉, 3년의 인증주기 동안 통제영역에 대한 '부적합 추이'의 측정을 통해 각 금융기업의 정보보호 수준이 개선되고 있음을 검증하는 것이다. 또한, '보고된 부적합사항'의 발생 비율을 분석함으로써, ISMS에 영향을 끼치는 주요 통제영역들을 도출하고 국제금융서비스 정보보호 가이드인 ISO27015의 통제항목을 통해 추가적인 보안 조치를 제시하였다.

조사결과 얻어진 데이터는 수치적인 계산과 용이한 해석을 위해 Microsoft Excel VBA(Visual basic application) 코드인 Chart, Add매서드, Chart 관련 속성, Shapes, AddShape 메서드 등을 활용하였다.

3.2.2 정보보호 수준 개선 효과 분석

ISO27001 인증 비교 대상 업체들을 분석한 결과, ISO27001 인증을 받은 모든 업체에서 최초심사로부터 3년 주기가 지나는 동안 부적합 건수가 아래의 그림 6과 같이 매년 감소하고 있음을 확인할 수 있었다.

그림 6에서 X축은 최초심사(V1), 사후심사(V2, V3)를 나타내며, Y축은 발견된 경부적합(Minor Nonconformity) 건수를 의미한다. 해당 자료를 분석해 보면 최초심사 기준으로 적게는 27%, 많게는 100%의 개선이 이루어졌으며, 부적합 외에 심사원의 판단 및 경험으로 개선이 권고되는 개선권고 사항이나 단순한 관찰사항 정도만 발견



(그림 6) ISMS 구축 후 부적합 추이

(Figure 6) Non-conformity trends after introducing ISMS

되었다. 물론 샘플링을 통해 증적 자료(Auditing trail)를 확인하고 프로세스 접근법으로 심사를 진행하는 만큼 요구사항의 100% 준수라는 것이 완벽한 보안이라는 의미는 아니다. 그렇지만 위의 통계 자료는 금융권에서 ISMS가 보안의 완전성을 보장하지는 못해도 상대적으로 통제에 필요한 기준을 제시하고 이에 따라 기업이 가진 리스크를 감소 시켰다는 것을 의미한다.

3.2.3 ISMS 도입에 따른 주요 통제영역

앞서 살펴본 ISMS 도입에 따른 효과성 측정과 관련하여, 금융권 비교 대상 업체의 인증 주기 전반에 걸쳐 부적합사항으로 지적된 통제영역 및 각 항목의 빈도를 측정해 보면 아래 표 5와 같다.

(표 5) ISO27001:2005 통제영역 별 빈도
(Table 5) Frequency of each ISO27001:2005 control area

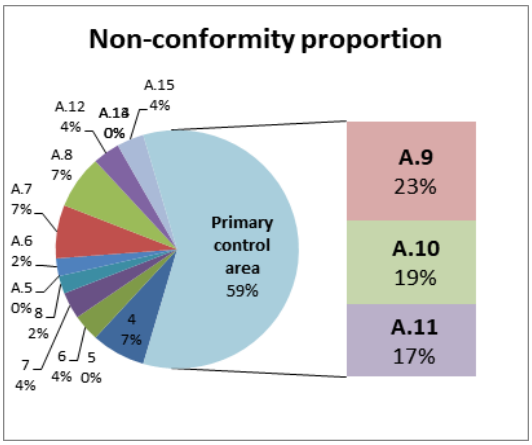
Requirements	Freq.	Specific control area
4 Information Security Management System	6	4.2.1 Istablish the ISMS 4.2.3 Monitor and review the ISMS 4.3.2 Control of documents
6 Internal ISMS audits	3	6 Internal ISMS audits
7 Management review the ISMS	3	7.2 Review input
8 ISMS improvement	2	8.2 Corrective action
A.6 Organization of information security	2	A.6.1.4 Authorization process for information processing facilities A.6.1.8 Independent review of information security
A.7 Asset management	6	A.7.2.2 Information labelling and handling
A.8 Human resources security	6	A.8.2.2 Information security awareness, education and training A.8.3.1 Termination responsibilities A.8.3.2 Return of assets A.8.3.3 Removal of access rights
A.9 Physical and environmental security	19	A.9.1.2 Physical entry conrtrols A.9.1.3 Securing offices, rooms and facilities A.9.1.4 Protecting against external and environmental threats A.9.1.5 Working in secure areas A.9.1.6 Public access, delivery and loading areas A.9.2.1 Equipment siting and protection A.9.2.2 Supporting utilities A.9.2.3 Cabling security A.9.2.6 Secure disposal or re-use of equipment A.9.2.7 Removal of property
A.10 Communications and operations management	16	A.10.1.1 Documented operating procedures A.10.1.2 Change management A.10.2.1 Service delivery A.10.2.3 Managing changes to third party services A.10.3.2 System acceptance A.10.4.1 Controls against malicious code A.10.6.1 Network controls A.10.7.1 Management of removal media A.10.10.6 Clock synchronization
A.11 Access control	14	A.11.2.2 Privilege management A.11.2.4 Review of user access rights A.11.3.1 Password use A.11.3.3 Clear desk and clear screen policy A.11.4.6 Network connection control A.11.5.1 Secure log-on procedures A.11.5.2 User identification and authentication A.11.5.6 Limitation of connection time
A.12 Information systems acquisition, development and maintenance	3	A.12.5.5 Outsourced software development A.12.6.1 Control of technical vulnerabilities
A.15 Compliance	3	A.15.1.4 Data protection and privacy of personal inforamtion

통제 요인 별 빈도를 측정해 본 결과, ‘A.9 물리적 환경적 보안’, ‘A.10 의사소통 및 운영관리’ 그리고 ‘A.11 접근통제’ 영역이 가장 높은 빈도를 나타내고 있었다. 이를 ‘원형 대 가로막대 형’ 차트로 정리해 보면 아래 그림 7과 같다.

이처럼 금융권 비교 대상 업체로 선정된 다섯 곳을 기준으로 부적합 빈도수가 가장 높았던 ‘A.9 물리적 환경적 보안’, ‘A.10 의사소통 및 운영관리’ 그리고 ‘A.11 접근통제’ 영역이 각 23%, 19%, 17%를 나타내 전체 부적합의 59% 정도를 차지하는 주요 통제영역으로 도출되었다.

이는 금융서비스를 제공하기 위해 사용되는 서버, 네트워크, PC 등 IT와 관련된 자산들의 보호가 중요하고,

정보자산을 활용함에 있어 제3자 보안을 포함하여 각 부서 간 의사소통 및 운영통제의 중요성 그리고 내/외부 시스템에 접속함에 있어 더욱 세심한 주의가 필요함을 의미한다.



(그림 7) 금융 관련 조직의 정보보호 주요 통제영역
(Figure 7) Primary information security control areas of finance-related organizations

추가적으로, 부적합으로 보고되지 않은 통제영역들 중 금융 서비스의 중단과 같은 금융권 사고는 비용적인 측면부터 대외 이미지 등 조직에 끼치는 영향이 매우 크므로 'A.14 비즈니스 연속성 관리'와 같은 통제영역은 금융권에서 보다 비중 있게 관리되어지는 것으로 보인다. 기타 5개 조항 및 부속서의 11개 도메인 133개 통제항목에 대한 통제가 제대로 이루어지기 위한 정책, 절차, 지침의 수립 단계가 4조항, 이를 바탕으로 조직 전반에 구축된 ISMS를 검토하고 개선해 나가기 위한 내부감사, 경영검토, 시정조치 및 예방조치의 6, 7, 8조항은 어떠한 배제도 허용되지 않는 주요 통제영역임에도 일부 경부적합이 발생하는 것을 확인할 수 있었다. PDCA 사이클에 따라 ISMS를 수립, 운영, 점검 및 조치를 하려면 기본적으로 관련 정책, 지침, 절차 및 프로세스들의 문서화가 우선되고 조직에 전파되어야 한다. 이를 보완하기 위해 금융서비스를 제공하는 조직 내 정보보호에 대한 착수, 구현, 유지관리 및 개선을 위한 금융서비스 분야 가이드라인 ISO27015의 통제 항목을 앞서 도출된 통제영역에 적용하면 표 6과 같이 매칭 할 수 있다.

위와 같이 도출된 통제영역 외에 다른 영역에도 ISO27015 금융보안 가이드를 적용할 수 있으며, 향후 연

(표 6) ISO/IEC TR 27015:2012에 따른 보안 조치 방안*
(Table 6) Method for security execution according to ISO/IEC TR 27015:2012

Reqire-ments	ISO/IEC 27001	ISO/IEC 27015
A.8 Human resources security	A.8.2.2 Information security awareness, education and training	
	Presentation of items including in awareness improvement and continuous training	Consideration of legislations and regulations including regulatory agency's announcements
A.9 Physical and environmental security	A.9.1.5 Working in secure areas	
	Presentation of guideline in secure areas prohibiting usage of unapproved mobile equipments	Prohibiting usage of mobile devices in important work processing area such as processing of credit card or customer information
	A.9.2.1 Equipment siting and protection	
	Presentation of guideline to protect equipments like deploying equipment to minimize unnecessary access	Protection of installed payment equipment outside organization such as ATM, SST, POS, etc.
	A.9.2.6 Secure disposal or re-use of equipment	
	Presentation of secure removal guideline like physically destroying equipments stored sensitive information	Secure removal of information related to customer and finance such as ATM, SST, HDD, POS, internal memory, etc.
A.10 Communications and operations management	A.10.4.1 Controls against malicious code	
	Presentation of guideline protecting from malicious codes such as policy setting against use of unapproved software	Detection and recovery of malicious code including payment equipment such as ATM, SST, POS, etc.

구에서는 이러한 ISMS 도입에 따른 개선 및 보안 성숙도에 따라 나머지 통제영역들에 끼치는 영향도 연구해 볼 수 있을 것이다. 이와 관련, 다음 장에서는 위의 배경을 바탕으로 금융권 ISMS를 활용한 연구 및 관련 ISO27001:2013의 연구 필요성을 제시하고자 한다.

* 금융서비스에 제공되는 추가적인 가이드가 없는 경우 제외, 구현지침 내용은 금융보안연구원, 전자금융보안동향&연구 2013년 9월 제9호를 참조함

4. 결 론

4.1 연구의 의의

본 연구에서는 ISMS를 구축하는데 있어 고려해야하는 요소들을 살펴보고 실제 금융서비스산업에 ISMS를 구축함으로써 조직전반에 정보보호 수준이 개선된 사례를 살펴보았다. 금융권의 ISMS 적용 결과는 국제 인증에 따른 물리적, 기술적, 관리적 보안통제 그리고 법규 및 컴플라이언스를 통해 금융권의 정보보안 리스크 통제가 가능함을 보여주는 사례라 할 수 있다. ISMS가 금융권의 보안업무를 수행하는데 있어 얼마나 효과적인지에 대한 부분은 관련 담당자마다 상대적일 수 있으나 준수사항이 많아지더라도 이에 대한 체계적인 관리가 이루어지면 기업의 정보보호 수준은 개선될 수 있다는 것을 해당 사례 분석을 통해 확인할 수 있었다.

ISMS는 해당 시스템이 '법적, 제도적 정보보호 요구사항에 맞춰 기업 업무 프로세스 전반에 대한 보안 조건을 충족하고 지속적으로 유지되고 있음을 보증(assurance)하는 것'이다. 물론 ISMS를 갖춘다고 하여 정보보호에 대해 완전하다고 말할 수는 없다. 이는 기업이 ISMS를 갖추고 해당 인증을 획득한다고 하더라도 해킹, 정보유출 등의 보안 사고를 모두 막을 수 있는 것도 아닐뿐더러, 각 기업들의 ISMS를 합격, 불합격으로 재단하기에는 무리가 따르기 때문이다. 즉, ISMS를 갖춤으로써 조직의 정보보호 수준이 해당 기준에 부합함(conformity)을 합리적인 수준으로 보증할 수 있다는 의미이지 절대적으로 보장(guarantee)한다는 의미는 아니다. 하지만 정보보안을 위한 최소한의 기준이나 가이드가 없다면 수많은 리스크로부터 조직의 어느 부분을 어떻게 보호해야 할지에 대한 방향조차 잡을 수가 없을 것이다. 정보보호는 더 이상 일부의 업무 분야가 아니라 조직 전반의 모든 구성원들이 훈련 및 인식교육을 통해 내재화되어야 하는 필수 사항이다. 그러므로 습관화를 통한 체질 개선이 이루어져야 보다 효과적이고 효율적인 ISMS의 운영이 가능할 것이다.

4.2 연구의 한계와 추가 연구

연구의 한계점으로, 비교 대상 기업들이 동일 인증을 획득하여 공통 통제영역을 기준으로 분석이 가능하였으나, 선정 업체들이 금융 관련 산업 전체를 대표한다고 볼 수는 없어서 금융 관련 조직에 끼치는 객관적인 효과성에 대해서는 추정만 가능한 상태이다. 향후 연구에서는 금융서비스 업무 전반의 성과측정이 가능하도록 연구모델을 보완할 필요가 있다.

ISO 국제인증체계는 특성상 제조업, 서비스업 등 관련 산업 특성에 상관없이 모든 산업 분야에 적용할 수 있어 동종 업계는 물론 타 업종과의 효과성 정도 차이에 대해서도 지속적인 검증이 가능하리라 본다. 이에 따라 본 연구와 관련한 향후 연구 방향으로 크게 세 가지를 제시하고자 한다.

첫째, 최신 규격을 적용한 기업의 분석이다. 국제 ISMS(ISO27001) 인증이 ISO27001:2013규격으로 2013년 10월 1일 개정 발행되었지만, 인증심사를 수행하는 인증기관의 전환 절차에 따라 2014년 하반기부터 공식적인 인증심사가 시행되기 시작했다. ISO27001:2013 기준으로는 아직 전환 후 3년의 인증 주기가 도래하지 않았거나 자료 확보가 어려워 금융권은 물론 다른 산업분야의 ISMS 도입에 따른 정보보호 수준 개선효과를 확인하기가 어려운 시점이다. 또한 국제금융서비스 정보보호 가이드라인인 ISO 27015:2012가 아직 ISO27001:2013 규격에 맞춰 개정되지 않았다. 이러한 이유로 현 시점에서는 ISO27001:2005규격을 기준으로 한 본 연구가 의미가 있으나, 향후 ISO27001:2013규격에 따른 인증심사 결과에 대한 유효성 검증도 필요할 것이다.

둘째, 정보보안을 지원하는 타 규격과의 연계 분석이다. 개인정보보호 관리체계(PIMS) 인증인 BS10012나 IT 서비스관리체계(ITSM) 인증인 ISO20000과의 연계성을 분석하여 관련 조직의 ISMS의 효과에 영향을 끼치는지에 대한 상관 분석을 수행하고, 이에 따른 비용 및 인력 절감 등의 부가적인 제반사항들이 깊이 있게 다루어질 수 있다. 이를 통해 금융권 ISMS 구축을 통한 보안업무의 효율성 또한 심도 있게 측정해 볼 수 있을 것이다.

끝으로, 해당 관리체계의 적용에 있어 업종별로 주요하게 다루는 통제영역의 차이가 있을 수 있으므로, 또 다른 산업분야에 적용된 사례를 분석하여 향후 ISMS 정책 적용 방안을 제시할 수 있을 것이다.

참고문헌(Reference)

[1] White Paper for National Information Security, Korea Internet and Security Agency (KISA), 2016, pp.183-185. https://isis.kisa.or.kr/ebook/download_pdf/2016.pdf

[2] "Finance-related area, mandatory ISMS certification is abolished", Boannnews, 2016.05.31.

https://www.boannews.com/media/view.asp?idx=50772&kind=2&search=title&find=

[3] ISMS Certification-related Documentation, Financial Security Institute, 2017.03.02. http://www.fsec.or.kr/user/bbs/fsec/148/319/bbsDataView/740.do?page=1&column=&search=&searchSDate=&searchEDate=&bbsDataCategory=

[4] R. Alavi, "Information Security Management Systems: Modelling Human Factors", The State of Security, Tripwire, 3 Nov. 2013. https://www.tripwire.com/state-of-security/security-data-protection/3

[5] Y.J. Jun, G.H. Cho, and W.K. Kim, "A Design and Implementation of Information Security Management and Audit System for Government Agencies," Journal of Internet Computing and Services, Vol. 7, No. 5, pp. 81-94, 2006. http://www.jics.or.kr/digital-library/423

[6] H.K. Kim, K.H. Lee, and J.I. Lim, "A Study on the Impact Analysis of Security Flaws between Security Controls: An Empirical Analysis of K-ISMS using Case-Control Study", KSII Transactions on Internet and Information Systems, Vol. 11, No. 9, pp. 4588-4608, 2017. DOI: 10.3837/tiis.2017.09.022

[7] H.S. Jo, S.J. Kim, and D.H. Won, "Advanced Information Security Management Evaluation System," KSII Transactions on Internet and Information Systems, Vol. 5, No. 6, pp. 1192-1213, 2011. https://doi.org/10.3837/tiis.2011.06.006

[8] J.S. Kim, S.Y. Lee, and J.I. Lim, "Comparison of The ISMS Difference for Private and Public Sector", Journal of the Korea Institute of Information Security and Cryptology, Vol. 20, No. 2, pp. 117-129, 2010. https://academic.naver.com/article.naver?doc_id=181695427

[9] H.K. Kim, G.M. Gho, and J.I. Lee, "Comparison for Corporate Information Security Institution State and Certification Criteria of Information Security Management System According to the Revision for the Law of Information and Communication Network", Journal of the Korea Institute of Information Security and Cryptology, Vol. 23, No. 4, pp. 53-58, 2013. https://academic.naver.com/article.naver?doc_id=61862547

[10] S.S. Jang and H.S. Lee, "A study on the analysis for flaw item of Information Security Management Sysem (ISMS) certification audit", Journal of the Korea Institute of Information Security and Cryptology, Vol. 20, No. 1, pp. 31-38, 2010. https://academic.naver.com/article.naver?doc_id=41633109

[11] W. Boehmer, "Appraisal of The Effectiveness and Efficiency of an Information Security Management System based on ISO 27001", 2008 2nd International Conference on Emerging Security Information, Systems and Technologies, IEEE, 2008. https://doi.org/10.1109/SECURWARE.2008.7

[12] N.K. Sharma and P.K. Dash, "Effectiveness of ISO 27001, As an Information Security Management System: An Analytical Study of Financial Aspects", Far East Journal of Psychology and Business, Vol. 9, No. 5, pp. 57-71, 2012. https://ideas.repec.org/a/fej/articl/v9cy2012i5p57-71.html

[13] B. Shojaie, H. Federrath, and I. Saberi, "Evaluating the effectiveness of ISO 27001:2013 based on Annex A", 2014 9th International Conference on Availability, Reliability and Security, IEEE, 2014. https://doi.org/10.1109/ARES.2014.41

[14] ISO/IEC27001:2005 Requirement, ISO, 2005. http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27001.pdf

[15] The ISO Survey of Management System Standard Certifications(2006-2012), ISO, 2013. http://www.pjr.com/downloads/iso_survey.pdf

◐ 저 자 소 개 ◑

강 윤 철(Youn-chul Kang)
2009년 고려대학교 경영정보학과(경영학사)
2011년 한양대학교 일반대학원 정보시스템학과(공학석사)
2014년 고려대학교 대학원 디지털경영학과(경영학박사수료)
관심분야 : ISO국제인증, 정보보호관리체계, 정보보안, 개인정보보호, 위험관리, 업무연속성관리, etc.
E-mail : kcode000@hotmail.com

안 종 창(Jong-chang Ahn)
1994년 고려대학교 경제학과(경제학사)
2002년 세종대학교 대학원 인터넷소프트웨어학과(공학석사)
2007년 한양대학교 대학원 정보기술경영학과(공학박사)
2010년~현재 한양대학 정보시스템학과 부교수
관심분야 : 지식경영, 전자상거래론, 정보시스템 사용자 행태, 미디어 사용자 행태, etc.
E-mail : ajchang@hanyang.ac.kr