Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 4 pp. 140-149, 2021

https://doi.org/10.5762/KAIS.2021.22.4.140
ISSN 1975-4701 / eISSN 2288-4688

정보보호 관리체계를 위한 주요 통제영역에 대한 연구: 국내 3개 산업을 중심으로

강윤철[1], 안종창[2*]
[1]고려대학교 디지털경영학과, [2]한양대학교 정보시스템학과

A Study on Primary Control Area for Information Security Management System (ISMS): Focusing on the Domestic Three Industries

Youn-Chul Kang[1], Jong-Chang Ahn[2*]
[1]Department of Digital Management, Korea University
[2]Department of Information Systems, Hanyang University

요 약 기업 기밀과 고객 정보를 적절하게 보호하고 유지하기 위해, 조직은 정보보호 관리체계(ISMS), 개인정보보호 관리체계(PIMS), 비즈니스연속성 관리체계(BCMS)와 같은 경영시스템을 도입하여 운영하기 시작하였다. 본 연구는 정보보안을 고려하는 모든 조직이 정보보호 관리체계를 유지하는 것이 바람직하며 ISMS는 정보보안 문화, 실무 및 가이드라인을 고려하는 다양한 조직 안에 각기 다른 형태를 가질 수 있다는데서 출발하였다. 산업분야에 상관없이 적용 가능하고 보편적으로 널리 알려진 국제 정보보호 관리체계 ISO27001을 도입한 조직을 대상으로, 인증 심사에 따른 부적합 사례를 통해 산업별, 조직규모별, 심사유형별 정보보호 관리체계의 주요 통제 영역을 도출하려 하였다. 국내의 경우 산업분야별 인증을 유지하고 있는 곳이 많지 않아 실증 연구를 위한 자료 확보에 어려움이 있지만, 탐색적 연구 대상으로서의 의미가 있는 것으로 보인다. 분석을 통해, 대상 업체들에서 ISO27001:2013이 발표된 2013년부터 2020년까지 각 형태별로 부적합 빈도수가 가장 높았던 요구사항을 주요 통제영역으로 도출하였다. 이를 바탕으로 3개 산업분야, 조직규모, 심사유형에 따라 ISMS의 주요 통제항목에 차이가 있다는 것을 발견하였다.

Abstract Most industries have introduced and operate an information security management system (ISMS) or a personal information security management system (PIMS) to suitably protect and maintain customer's information and company trade secrets. This study starts with the premise that it is desirable for every industry considering information security to maintain an ISMS. ISMS can be of different types among various organizations, taking into consideration culture, practical work procedures, and guidelines for information security. This study intends to derive primary control areas of an ISMS for each industry based on organizational size and audit type by analyzing non-conformity trends and control factors according to certification audits for organizations introduced for international ISMS under ISO27001. This study analyzed improvement effects of ISMS through case analyses. It is meaningful as exploratory research, although it was difficult to acquire data for empirical study because few organizations maintain certification in major industrial sectors. The requirements presented the highest frequency of non-conformity for each type from the 2013-initiated ISO27001; the years 2013 to 2020 were extracted as the primary control area. The study found that for primary control areas of ISMS for each of three industries, organizational size and audit type had differences.

Keywords : Information Security Management System, Personal Information Security Management System, Certification Audit, Information Security Control Area, Non-conformity Trends

"이 논문은 한양대학교 교내연구지원사업으로 연구되었음(HY-2020년도)"
*Corresponding Author : Jong-Chang Ahn(Hanyang Univ.)
email: ajchang@hanyang.ac.kr
Received January 18, 2021 Revised March 16, 2021
Accepted April 2, 2021 Published April 30, 2021

1. 서론

정보보호 관리체계(ISMS: Information Security Management System, 이하 ISMS)는 정보보호가 기업의 비즈니스 경영 목표와 연계될 수 있도록 정보보호 최고책임자(CISO: Chief Information Security Officer)를 지정하고 위험분석을 통한 정보보호정책을 수립하여 정보보호 활동을 전개할 수 있도록 하는 체계이다. ISMS는 정보보호 정책에 따라 수행된 정보보호 활동을 모니터링 및 검토하여 지속적으로 개선할 것을 요구한다. 이를 통해, ISMS를 구축한 조직은 정보보호 정책과 활동의 일관성을 확보하여 보다 효과적인 정보보호 체계를 구축할 수 있도록 한다[1,2]. 국제표준 ISO27001:2013은 ISMS를 의미한다.

본 연구에서는 선행 연구[2,3]를 확장하여 국제인증 ISO27001:2013을 도입하여 운용하고 있는 국내 조직을 대상으로 한다. 이들 조직에 대한 100건 이상의 인증 심사에서 부적합이 도출된 97건의 심사결과 보고서에서 300여건의 부적합 사례를 분석하였다. 이를 통해 주요 산업분야, 조직의 규모 및 심사유형에 따라 주요 통제영역이 어떻게 달라지는지를 분석함으로써, ISMS의 지속적 개선을 위한 방법을 제시하고자 한다.

본 연구는 서론에 이어서 선행연구와 참조모델을 제시한다. 이어서 선행연구 방법론을 참조하여 국내 3개 산업분야에 대한 사례 분석을 수행한다. 사례 분석 결과를 바탕으로 연구의 의의와 한계점, 추가 연구방향을 제시하게 된다.

2. 선행연구와 참조모델

2.1 ISMS 동향과 선행연구

ISMS의 금융관련 동향으로, 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 공개하였다. 이를 2018년부터 전면 적용하였다[2]. 그러나 (구)ISMS 및 (구)PIMS 인증제도의 통합으로 인증기준이 변경됨에 따라[4], 금융권에 적합한 ISMS-P 인증 점검항목 개발이 필요하게 되었다. 통합된 ISMS-P의 인증기준은 102개이며, KISA의 점검항목은 325개이며, 금융보안원의 점검 항목은 384개로 변경되었다. 2021년부터 바뀐 사항이 전면 적용된다. 참고로 2017년 7월 기준 금융보안원에서 ISMS 인증서를 발급한 곳은 시중은행 8개를 비롯해 46개사이다[5]. 2020년 12월 23일 기준으로는 89개사이다[5].

국제 표준인 ISO27001인증을 통해 정보보호 수준이 개선되거나 정보보호 주요 통제영역을 도출할 수 있다는 것을 검증한 국내외 선행연구를 보면 다음과 같다.

Boehmer는 ISO27001을 기반으로 ISMS의 부적합 추이를 포함하여 효과성 및 효율성을 평가하고자 관련 핵심성과지표(Key performance indicator; KPI)를 분석하여 성과측정 메트릭스를 제시하였다[6]. 이 연구[6]는 본 연구의 측정 지표인 인증심사 보고서의 '부적합 수'를 바탕으로 하는 것이 의미가 있다는 점을 시사한다.

Sharma와 Dash 연구[7]에서는 인도에서 ISO27001에 대한 실행이 정보보안 사고에 대해 효과적인 보호체계이고, 금융 분야 조직 운영에 도움이 된다는 가설을 바탕으로 ISO27001 도입의 긍정적인 측면을 제시하였다. 이 과정에서 ISO27001인증 조직 545개 중 15개 조직을 최종 선정하여 연구를 진행 하였다[7]. 이들의 연구는 적은 조직 숫자라도 초기 실증연구 대상으로써 의미가 있다는 점을 본 연구에 시사해 준다. 또한 일반적으로 연구자들은 ISO27001표준 이행의 성공요인을 찾기 위한 성숙도 측정의 기능은 의사 결정을 위한 정보를 제공하는 것이라고 동의했다[7]. 이는 분야 별 주요 통제영역이 다르다면 정보보호 활동에 필요한 예산 및 인적자원 등의 투자 우선순위가 달라질 수 있음을 시사해 준다.

Shojaie 외[8]의 연구에서는 ISO27001의 2005년과 2013년 버전을 비교 분석하여 주요 통제 영역을 데이터, 하드웨어, 소프트웨어, 사람 및 네트워크로 분류하였다. 버전별 차이점을 기술하고 주의 깊게 다루어야 할 영역을 또한 제시하였다[8]. 이 연구[8]는 본 연구가 ISO27001의 2013년 버전을 연구 대상으로 하는데 있어서 준거점을 준다.

Boehmer의 연구[9]는 ISMS에 대한 투자는 가치 사슬의 적절한 보호에 반영 되어야 하며, 그렇지 않으면 투자는 사업에 그리 유용하지 않으며, ISO27001에 따른 ISMS의 위험 접근법은 정보 보안에 대한 투자를 낭비하지 않으려는 회사들에게 중요함을 제시하였다. 이는 주요 통제영역에 필요한 투자를 해야 된다는 점을 시사해 준다.

Drugescu와 Etges의 연구[10]는 적절한 영역의 위험을 완화하고 보안 투자를 극대화하고 자금을 할당하기 위해, 조직은 위험을 정량화하고 우선순위를 정하는 학습 방법을 정의해야함을 제시하였다. 부적합사항이 많이

도출되는 영역은 그만큼 리스크가 높다고 볼 수 있으며, 주요 통제영역으로 관리해야함을 시사해 준다.

정보보호 관리체계 도입의 필요성에 대한 강윤철과 임성택의 연구[3]에서는 특허정보제공 기업을 중심으로 정보보호 관리체계 구축 전/후를 비교함으로써 국제 인증 ISO27001에 따라 물리적, 기술적, 관리적 보안통제는 물론 컴플라이언스(Compliance)에 따른 리스크 통제가 가능하다는 것을 보여주었다. 이 연구[3]는 ISO27001을 바탕으로 하는 본 연구의 출발점으로써의 의미를 제시하고 있다.

강윤철과 안종창의 연구[2]에서는 정보보호 관리체계를 위한 주요 통제영역 연구를 위해 금융 관련 조직을 중심으로 정보보호 관리체계 구축 전/후의 부적합 추이를 분석하였다. 이를 통해 ISO27001인증 절차에 따라 부적합이 감소함을 실증하고 금융 조직에 공통적으로 나타나는 주요 통제항목을 도출하였다. ISMS가 보안의 완전성을 보장하지는 못해도 상대적으로 통제에 필요한 기준을 제시하고 이에 따라 기업이 가진 리스크를 감소시켰음을 보여주었다. 이 연구[2]는 ISO27001의 2005 버전을 통한 연구라는 점에서 본 연구의 방법론에 시사점을 주고 있으며, 분석 결과의 비교를 가능하게 한다는 점에서 의의를 가진다.

선행 국내 문헌들[2,3]은 ISO27001:2005를 기준으로 분석되었다. 본 연구는 선행 문헌의 방법론을 참조하고 주요 산업분야에서 ISO27001:2013 최신 규격을 적용한 기업을 대상으로, 주요하게 다루어야 하는 통제영역의 차이를 비교해 보고자한다.

2.2 연구참조 모델 : ISO/IEC 27001:2013

현재 ISO/IEC 27001:2013으로 표기*되고 ISMS라고도 불리는 국제 ISMS는 정보보안 경영체계라 불리기도 한다. 조직의 정보 자산이 적절히 보호되고 있는지를 인증하는 것으로, 조직이 위험평가를 실시하고 적절한 통제를 구현하여 국제적으로 인지되는 ISMS 규격에 적합한 정보보호를 이행하여 왔음을 입증하는 것이다. 이는 PDCA (Plan-do-check-act) 사이클에 따라 지속적인 개선을 추구하며 조직의 규모에 상관없이 모든 산업분야에 적용 가능하다[11,12].

ISO27001 요구사항의 구성을 살펴보면 최신 버전인 ISO27001:2013 규격의 경우 7개 조항(4조~10조) 및 부속서의 14개 통제 분야, 114개 통제항목으로 구성되어 있다[13]. 14개의 통제 분야는 후술하는 Table 4에 요구사항(requirements) 리스트로 제시되어 있다.

국제 ISMS 즉, ISO27001 인증서는 2013년 개정 이후에도 Fig. 1처럼 매년 꾸준히 증가해 왔으며, 2019년 기준으로 전 세계 약 36,362개, 한국에서는 442개의 ISO27001인증서가 유지되고 있다[12,13]. 산업분야는 Table 1과 같이 39개로 구분되며 인증 수요가 많은 세계 상위 산업분야는 정보기술 분야(33번 코드)를 비롯하여 기타(other) 서비스 분야(35번), 교통/저장장치/통신 분야(31번), 금융 중개/부동산/임대 분야(32번), 건강 및 사회사업(38번)분야 등이다[13].

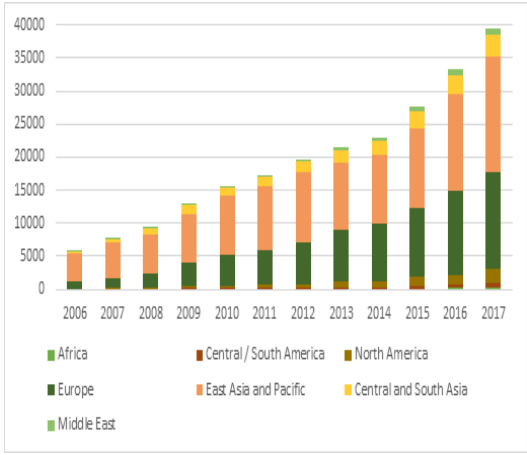


Fig. 1. Trends of world ISO27001 certification (Unit: item)

Table 1. Certification by industrial sector

EA* Code No.	ISO/IEC 27001 by Industrial Sector
1	Agriculture, Fishing and Forestry
2	Mining and quarrying
3	Food products, beverage and tobacco
4	Textiles and textile products
5	Leather and leather products
6	Manufacture of 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

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

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, renting
33	Information technology
34	Engineering services
35	Other Services
36	Public administration
37	Education
38	Health and social work
39	Other social services

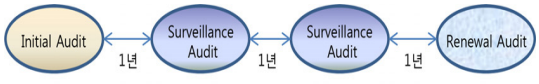
* EA= European Accreditation

3. 사례분석

3.1 IS27001 적용 주요사항

국내에서도 분야 구분 없이 ISMS를 구축하고 해당 국제인증인 ISO27001 인증을 받은 기업들이 증가하고 있으며, 그 중 ISMS를 구축 및 운영하고 있는 97건의 심사, 347건의 부적합 사례를 대상으로 연구를 진행하였다.

기본적으로 ISO 인증심사는 Fig. 2처럼 크게 최초심사, 사후심사 그리고 갱신 심사로 구성된다. 이는 국내 ISMS-P의 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

* Refer to https://isms.kisa.or.kr/

Fig. 2. Type of certification audit

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(Non-conformity, 이하 NC)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. 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[2].

3.2 ISO27001 주요 통제영역 비교

3.2.1 대상 기업 선정 및 측정지표

분석 대상 기업 선정 방법은 ISO27001:2013버전으로 개정 이후 2013년부터 지난 2020년까지 최초 또는 갱신심사 및 사후심사가 진행된 조직 중 조직의 규모에 관계없이 정량적 데이터 수집이 가능한 97개의 인증심사 결과보고서를 바탕으로 선정하였다. 산업분류에 따른 분석은 글로벌에서 인증서를 많이 유지하고 있는 상위 10개 섹터를 기준으로 최소 50개 이상의 부적합 사례가 도출된 3개의 산업분야를 최종 선정하였다. Table 2에 구체적 사항이 제시되어 있다.

Table 2. The industrial sector for the analysis of ISO27001 control area

EA Code No.	Industrial Sector	Number of NC case	Y/N
03	Food products, beverage and	21	

	tobacco		
19	Electrical and optical equipment	63	Y
23	Manufacturing not elsewhere classified	30	
25	Electricity supply	7	
31	Transport, storage and communication	13	
32	Financial intermediation, real estate, renting	18	
33	Information technology	82	Y
34	Engineering services	19	
35	Other Services	56	Y
38	Health and social work	6	

분석 대상 산업의 상세 자료는 실무자 협의를 거쳐 연구 목적에 필요한 최소한의 정보만을 활용하기로 하였다.

국내에서 ISO27001 인증을 유지하고 있는 업체가 2019년 기준 442개지만[12,13] 모든 산업이 고루 정보보안 인증을 유지하고 있지는 않았다. 그러나 Sharma와 Dash의 연구[7](전체 ISO27001 인증 조직 545곳 중 정량적 데이터 수집을 위해 최종 15곳을 선정하여 연구를 수행)처럼 실증적인 연구를 위한 자료 확보가 어려운 점을 감안하면 적은 조직 숫자라도 초기 연구 대상으로서의 의미가 있을 것으로 예상하였다.

측정 지표로는 ISO27001 인증심사 보고서의 '부적합수'를 바탕으로 하였다[2]. 첫째, 주요 산업섹터의 요구사항 별 부적합 비중이 어떻게 다른지 분석해 보기로 하였다. 둘째, 각 조직의 규모(범위 내 인원)에 따라 요구사항별 부적합 비중이 어떻게 다른지 분석해 보기로 하였다. 셋째, 각 조직의 ISO27001:2013 인증 심사 후 최초 또는 갱신 심사에서 발견된 부적합 건수가 매년 사후심사가 진행됨에 따라 얼마나 감소하는지에 대한 통계치를 분석해 보기로 하였다. 즉, '보고된 부적합사항'의 발생 비율을 분석함으로써, 주요 산업섹터의 ISMS에 영향을 끼치는 통제영역들을 도출하였다. 또한, ISO27001:2013 통제영역에 대한 '부적합 추이'의 측정을 통해 주요 산업의 정보보호 수준이 개선되고 있는지를 검증하는 것이다.

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

3.2.2 산업분류에 따른 주요 통제영역

앞서 선정된 주요 산업 별 ISO27001:2013 조직별 평균 부적합 빈도를 분석해보면 Table 3과 같다.

Table 3. Average NC frequency of the major industry sector

EA Code No.	Industrial Sector	Average Number of NC case
19	Electrical and optical equipment	4
33	Information technology	3
35	Other Services	4

부적합사항으로 지적된 통제영역 및 각 항목의 비율을 측정해 보면 Table 4와 같다.

Table 4. Proportion of each ISO27001:2013 control area in the industrial sectors

Requirements	EC19	EC33	EC35
4 Context of the organization	0.0%	0.0%	0.0%
5 Leadership	1.4%	0.0%	0.0%
6 Planning	2.8%	2.1%	1.6%
7 Support	4.2%	6.3%	3.3%
8 Operation	1.4%	2.1%	1.6%
9 Performance evaluation	2.8%	1.1%	1.6%
10 Improvement	0.0%	2.1%	0.0%
A.5 Information security policies	0.0%	1.1%	0.0%
A.6 Organization of information security	1.4%	1.1%	4.9%
A.7 Human resource security	0.0%	3.2%	0.0%
A.8 Asset management	9.7%	5.3%	8.2%
A.9 Access control	22.2%	23.2%	23.0%
A.10 Cryptography	0.0%	1.1%	3.3%
A.11 Physical and environmental security	8.3%	11.6%	3.3%
A.12 Operations security	20.8%	22.1%	31.1%
A.13 Communications security	8.3%	6.3%	8.2%
A.14 System acquisition, development and maintenance	1.4%	0.0%	0.0%
A.15 Supplier relationships	0.0%	0.0%	0.0%
A.16 Information security incident management	0.0%	0.0%	0.0%
A.17 Information security aspects of business continuity management	5.6%	5.3%	0.0%
A.18 Compliance	9.7%	6.3%	9.8%

Table 3처럼 주요 산업별 평균 부적합 수의 차이는 거의 없는 것으로 보이나 각 산업의 요구사항 별 부적합 비율에는 차이가 있는 것으로 나타났다.

Table 4처럼 주요 산업의 통제 요인 별 빈도를 측정해 본 결과, 전반적으로 A.9 접근통제와 A.12 운영보안의 비율이 높게 나타났다. 이를 '묶은 가로막대 형' 차트로 정리해 보면 Fig. 3과 같다.

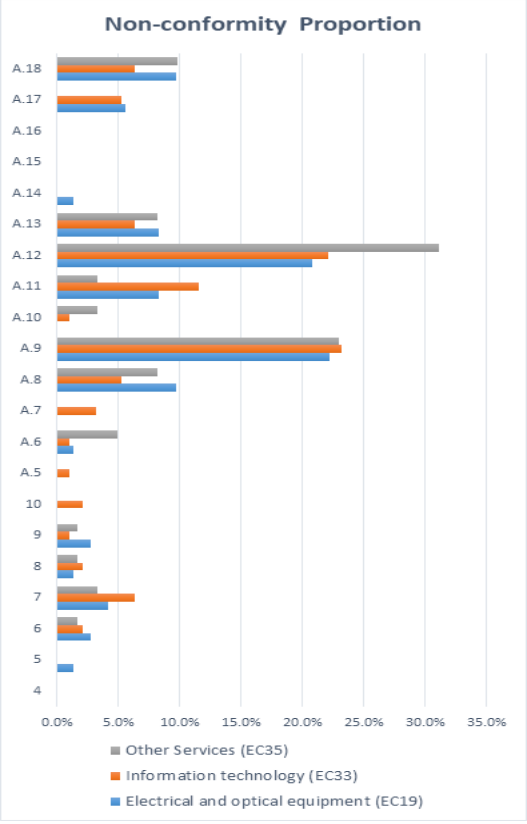


Fig. 3. Primary information security control areas of the major industrial sectors

요구사항 별 주요 산업 간 차이를 살펴보면, 7조 지원과 A.11 물리적 및 환경적 보안 영역에서는 정보기술 산업의 부적합 비중이 가장 높게 나타났다. 5조 리더십, 9조 성과평가 및 A.8 자산관리 영역에서는 전기 및 광학장비 산업의 부적합 비중이 높게 나타났으며 A.18 준거성 영역에서는 전기 및 광학장비 산업과 기타 서비스 산업의 부적합 비중이 높게 나타났다. A.6 정보보안 조직관리와 A.12 운영보안 영역에서는 기타 서비스 산업의 부적합 비중이 상대적으로 높게 나타났다.

각 산업 별로 주요 통제항목을 '원형 대 가로막대 형' 차트로 정리해 보면 Fig. 4, Fig. 5, Fig. 6과 같다.

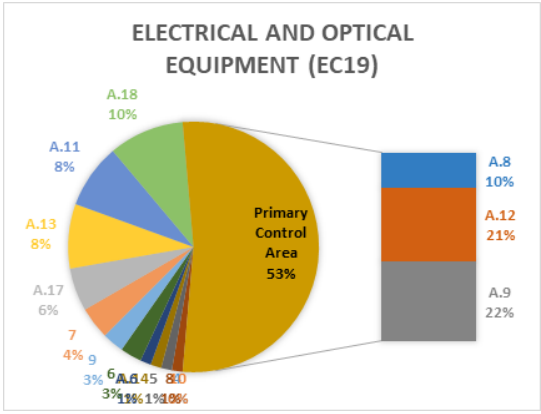


Fig. 4. Primary information security control areas of the electrical and optical equipment sector

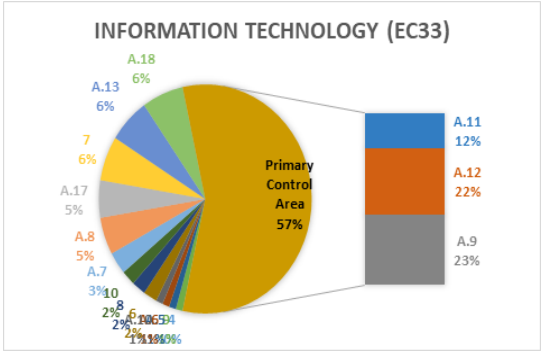


Fig. 5. Primary information security control areas of the Information technology sector

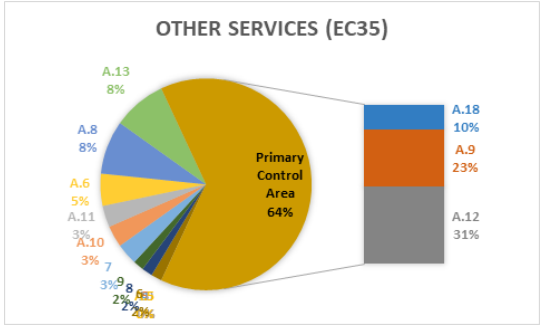


Fig. 6. Primary information security control areas of Other services sector

주요 산업 별 요구사항에 따른 주요 통제영역을 살펴보면 전기 및 광학장비 산업, 정보기술 산업 및 기타 서비스 산업의 경우 공통적으로 'A.9 접근통제' 및 'A.12 운영보안' 영역이 공통적인 주요 통제 영역으로 도출되었다. 전기 및 광학장비 산업의 경우 'A.8 자산관리'가, 정

보기술 산업의 경우 'A.11 물리적 환경적 보안'이, 기타 서비스 산업의 경우 'A.18 준거성'영역이 추가적인 주요 통제 영역으로 도출되었다. Fig. 4, Fig. 5, Fig. 6의 우측에서 이러한 사항을 확인할 수 있다.

3.2.3 조직규모에 따른 주요 통제영역

조직규모에 따른 분석은 앞서 수집한 10개의 산업분야의 조직을 대상으로 수행한 97건의 ISO27001 심사 사례 중 인증범위 내 인원수를 고려한 조직규모는 Table 5와 같이 부적합 빈도에 따라 분류하였다.

Table 5. The number of organization by the organization size and the frequency of nonconformity
(Unit: frequency of audit, no. of members)

Size / NC	1-20	21-50	51-100	101-200	over 200
1-5	15	18	21	10	17
6-10	2	1	3	1	0
11-15	4	3	0	0	0
16-20	0	0	0	0	0
21-50	0	1	0	0	0

이를 규모별 부적합 빈도에 따른 비율로 나타내면 Table 6과 같다.

Table 6. The proportion of organization by the organization size and the frequency of nonconformity
(Unit: No. of audit, No. of members)

Size / NC	1-20	21-50	51-100	101-200	over 200
1-5	71%	78%	88%	91%	100%
6-10	10%	4%	13%	9%	0%
11-15	19%	13%	0%	0%	0%
16-20	0%	0%	0%	0%	0%
21-50	0%	4%	0%	0%	0%

Table 6의 1행 1열의 경우, 범위 내 인원이 20명 이하였던 심사에서 부적합이 5건 이하로 분류된 건이 71%라는 의미이다. 200명 이상의 조직에서는 모두 부적합이 5개 이하로 나타난 반면, 조직규모가 100명 이하였던 심사에서는 부적합이 20개가 넘어가는 경우도 발견되었다. 20명 이하의 조직에서는 11개 이상 15개 이하의 부적합 비율이 나머지 규모보다 상대적으로 높게 나타났다. 이에 따라 규모별 부적합 비율을 분석해 보면, 상대적으로 조직규모가 작을수록 부적합 비율이 높게 나타난다는 것을 알 수 있다. 추가적으로, 조직규모에 따른 요구사항 별 부적합 비율을 측정해 보면 아래 Table 7과 같다.

Table 7. Proportion of each ISO27001:2013 control area by organization size
(Unit: size-members)

Size / Require-ments	1-20	21-50	51-100	101-200	over 200
4	0%	0%	0%	0%	0%
5	0%	1%	0%	0%	0%
6	3%	3%	1%	0%	0%
7	3%	5%	1%	4%	6%
8	1%	2%	0%	0%	0%
9	1%	1%	1%	0%	0%
10	0%	0%	3%	0%	0%
A.5	0%	0%	1%	0%	4%
A.6	4%	4%	3%	0%	0%
A.7	0%	1%	1%	0%	4%
A.8	7%	10%	7%	0%	6%
A.9	26%	19%	30%	25%	23%
A.10	1%	3%	0%	0%	0%
A.11	4%	10%	10%	13%	8%
A.12	26%	20%	24%	50%	25%
A.13	11%	5%	4%	0%	10%
A.14	0%	1%	1%	0%	0%
A.15	0%	0%	0%	0%	0%
A.16	0%	0%	0%	0%	0%
A.17	3%	6%	1%	0%	2%
A.18	9%	7%	7%	8%	13%

이를 '묶은 가로막대 형' 차트로 정리해 보면 Fig. 7과 같다.

A.12 운영보안 영역이 101명 이상 200명 이하의 조직에서 특히 높게 나타나기는 하지만 A.9 접근통제 및 A.12 운영보안 영역은 앞서 산업분야 별 분석과 마찬가지로 공통적인 주요 통제영역으로 도출되었다.

200명 이상의 규모가 큰 조직에서는 상대적으로 A.18 준거성 영역이, 100명 이하로 조직 규모가 작을수록 A.6 정보보안 조직, A.8 자산관리에 대한 부적합 비율이 높게 나타난다는 것을 알 수 있다.

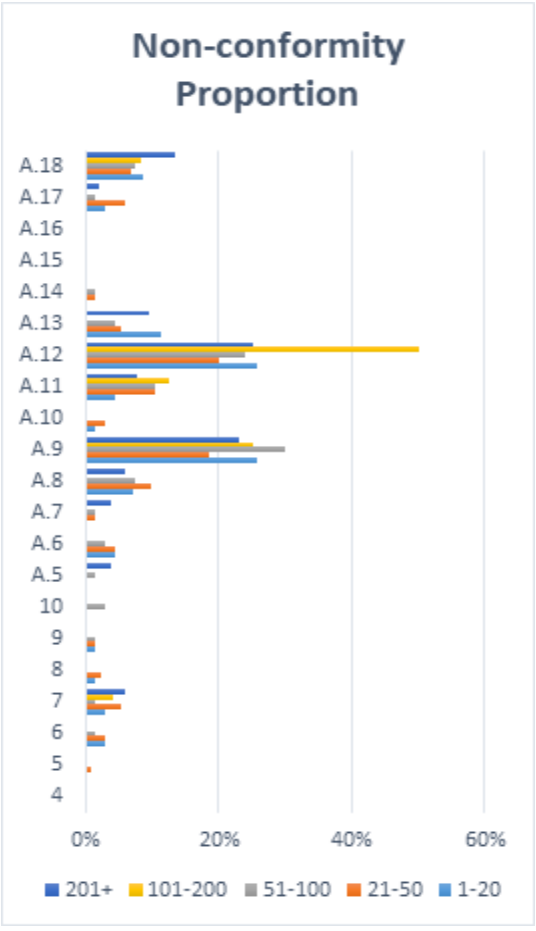


Fig. 7. Proportion of each ISO27001:2013 control area by organization size

3.2.4 심사유형에 따른 주요 통제영역

강윤철과 안종창[2]의 선행연구에서도 나타난 것처럼 ISO27001 인증 업체들을 분석한 결과, ISO27001 인증을 받은 모든 업체에서 최초 및 갱신 심사에서 도출된 부적합 건수가 Fig. 8과 같이 대체적으로 사후심사에서는 감소하고 있음을 알 수 있었다. Fig. 8에서 X축은 최초/갱신 심사, 사후심사와 같은 심사 유형을 나타내며, Y축은 발견된 경부적합(Minor Nonconformity)건수를 의미한다.

심사 유형에 따라 주요 통제 영역에 차이가 있는지를 비교하기 위해 각 요구사항 별 부적합 비율을 분석해보면 Fig. 9와 같다.

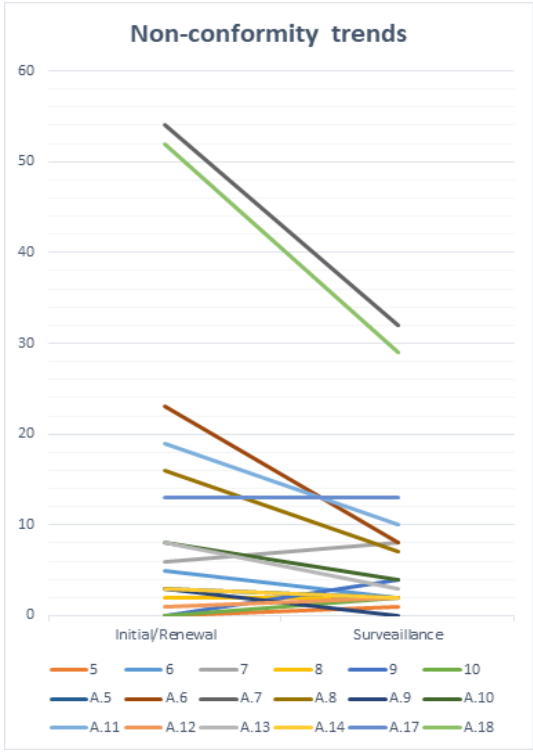


Fig. 8. Non-conformity trends after introducing ISMS

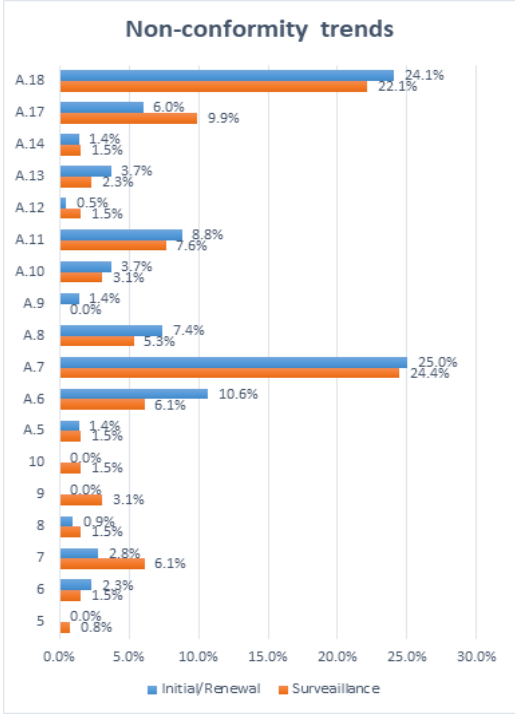


Fig. 9. Non-conformity trends after introducing ISMS

A.7 인적자원보안과 A.18 준거성 영역은 최초/갱신 및 사후심사 공통적으로 높게 나타났다. 특히 사후심사의 경우 Fig. 9처럼 지속적인 투자 및 유지활동이 미흡할 경우, 7조 지원, 9조 성과 평가, 10조 개선, A.17 업무연속성관리 영역에 대한 통제가 미흡한 것으로 나타났다.

4. 결론

4.1 연구의 의의

본 연구에서는 ISMS를 구축하는데 있어 고려해야하는 요소들을 살펴보고, 실제 주요 산업에 ISMS를 수립하고 운영할 때 주의 깊게 통제해야 하는 영역에 대해 분석하였다.

주요 발견 사항은 첫째, 산업분야에 따른 주요 통제항목에 차이가 있음을 확인할 수 있었다. 산업분야 공통으로는 A.9 접근통제 및 A.12 운영보안이 주요 통제영역으로 도출 되었다. 전기 및 광학장비(EC19) 산업의 경우 A.8 자산관리, 정보기술(EC33) 산업의 경우 A.11 물리적 및 환경적 보안, 기타 서비스(EC35) 산업의 경우 A.18 준거성이 추가적인 ISMS의 주요 통제 영역으로 도출되었다.

둘째, 조직규모에 따라서 주요 통제 영역이 일부 달라지는 것을 확인할 수 있었다. 조직규모가 작을수록 부적합 비율이 높게 나타났다. 200명 이상의 규모가 큰 조직은 상대적으로 준거성(A.18) 영역이, 100명 이하로 조직규모가 작을수록 정보보안 조직(A.6)과 자산관리(A.8)에 대한 부적합 비율이 높게 나타났다.

셋째, 심사유형에 따라서도 주요 통제 영역에 차이가 있는 것을 확인할 수 있었다. 인적자원보안(A.7)과 준거성(A.18) 영역은 최초/갱신 심사와 사후심사에 공통적으로 부적합 비율이 높게 나타났다. 사후심사의 경우 지속적인 투자 및 유지활용이 미흡할 때, 7개 조항 중에서 지원, 성과평가, 개선, 업무연속성관리 영역에 대한 통제가 미흡한 것으로 나타났다.

연구의 시사점으로, ISMS 적용 결과는 국제 인증에 따른 물리적, 기술적, 관리적 보안통제를 통해 주요 산업의 정보보안 리스크 통제가 가능함을 보여주는 사례라 할 수 있다. 물론 심사는 프로세스 접근법에 따라 샘플링 기법을 통해 증적자료(Audit evidence)를 확인하고 합리적 보증(Reasonable Assurance)을 하는 것이지 요구사항의 100% 준수라는 완벽한 보안을 보장(guarantee)하는 것은 아니다. 그렇지만 분석된 통계 자료는 ISMS가 산업 전반의 보안을 100% 보장하지는 못해도, 상대적으로 통제에 필요한 기준을 제시하고 있다. 이에 따라 기업이 가진 리스크를 감소시킬 수 있다는 것을 보여주고 있다.

특히, 산업분야 공통의 주요 통제영역, 광학장비 산업, 정보기술 산업, 기타 서비스 산업 섹터에서의 도출된 추가적인 주요 통제 영역은 해당 산업에 실무적인 시사점을 주고 있다.

4.2 연구의 한계와 추가 연구

연구의 한계점으로, 비교 대상 기업들이 동일 인증을 획득하여 공통 통제영역을 기준으로 분석이 가능하였으나, 선정 업체들이 각 산업 전체를 대표한다고 볼 수는 없어 주요 통제항목에 대한 추정만 가능한 상태이다. 향후 연구에서는 통계적으로 유의미한 결과를 얻기 위해 충분히 많은 사례를 수집하고, 보다 객관적으로 검증이 가능하도록 연구모델을 보완할 필요가 있다.

ISO 국제인증체계는 특성상 제조업, 서비스업 등 관련 산업 특성에 상관없이 모든 산업 분야에 적용할 수 있어, 한국은 물론 다른 국가와의 차이에 대해서도 비교 분석이 가능하다. 이에 따라 본 연구와 관련한 향후 연구 방향으로 다음 두 가지를 제시하고자 한다.

첫째, 글로벌 기업 전체를 대상으로 한 분석이다. 국제 ISMS(ISO27001) 인증이 ISO27001:2013규격으로 2013년 10월 1일 개정 발행되고 시간이 어느 정도 경과했다. 이에 따라 충분한 사례를 수집하여 글로벌 전체를 기준으로 통계적으로 유의미한 각 산업, 조직규모 및 심사유형 별 분석이 가능할 것으로 보인다.

둘째, ISMS 도입에 따른 정보보호 수준 개선효과를 객관적으로 측정하기 위해 사용자들의 만족도를 측정하기 위한 지표개발이다. 현 시점에서는 ISO27001:2013 규격을 기준으로 주요 통제영역을 도출한 본 연구가 의미가 있으나, 실제 내부 사용자들의 ISMS의 효과성에 대한 만족도를 측정하기 위한 지표를 개발하여 실무에서의 변화된 사항을 분석해 볼 수 있을 것이다.

References

[1] White Paper for National Information Security, Korea Internet and Security Agency (KISA), Korea, pp.183-185, 2016.

[2] Y. C. Kang, J. C. Ahn, "A Study on Primary Control Area for Information Security Management System (ISMS): Focusing on the Finance-related Organizations",

Journal of Internet Computing and Services, Vol.19, No.6, pp.9-20, 2018.
DOI: http://doi.org/10.7472/jksii.2018.19.6.9

[3] Y. C. Kang, S. T. Rim, "The Necessity of Introducing ISMS: Focusing on the Patent Information Provider", *Korea Institute of Information Security & Cryptology*, Vol.23, No.4, pp.7-14, 2013. Available From: https://www.koreascience.kr/article/JAKO201329438851081.page (accessed Apr. 20, 2021)

[4] S. W. Hong, J. P. Park, "Effective Management of Personal Information & Information Security Management System(ISMS-P) Authentication systems", *Journal of the Korea Academia-Industrial cooperation Society*, Vol.21, No.1, pp.634-640, 2020.
DOI: https://doi.org/10.5762/KAIS.2020.21.1.634

[5] ISMS Certification-related Documentation, Financial Security Institute, Korea, 2021. Available From: https://isms.kisa.or.kr/main/isms/issue/?certificationMode=list&crtfYear=2017 (accessed Apr. 20, 2021)

[6] 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, Cap Esterel, France, pp.224-231, Aug. 2008.
DOI: https://doi.org/10.1109/SECURWARE.2008.7

[7] N. K. Sharma, 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. Available From: https://ideas.repec.org/a/fej/articl/v9cy2012i5p57-71.html (accessed Apr. 20, 2021)

[8] B. Shojaie, H. Federrath, I. Saberi, "Evaluating the Effectiveness of ISO 27001:2013 Based on Annex A", *2014 9th International Conference on Availability, Reliability and Security*, IEEE, Fribourg, Switzerland, pp.259-264, Sep. 2014.
DOI: https://doi.org/10.1109/ARES.2014.41

[9] W. Boehmer, "Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001", *2009 International Conference on Availability, Reliability and Security*, Fukuoka, Japan, pp.392-399, 2009.
DOI: https://doi.org/10.1109/ARES.2009.128

[10] C. Drugescu, R. Etges, "Maximizing the Return on Investment on Information Security Programs: Program Governance and Metrics", *Information Systems Security*, Vol.15, No.6, pp.30-40, 2007.
DOI: https://doi.org/10.1080/10658980601051482

[11] ISO/IEC27001:2005 Requirement, ISO, 2005. Available From: https://www.iso.org/standard/54534.html (accessed Apr. 20, 2021)

[12] The ISO Survey of Management System Standard Certifications (2006-2012), ISO, 2013. Available From: http://www.pjr.com/downloads/iso_survey.pdf (accessed Oct. 15, 2020)

[13] The ISO Survey of Management System Standard Certifications 2019, ISO, 2019.

강 윤 철(Youn-Chul Kang) [정회원]

- 2009년 2월 : 고려대학교 경영정보학과 (경영학사)
- 2011년 2월 : 한양대학교 정보시스템학과 (공학석사)
- 2014년 2월 : 고려대학교 디지털경영학과 (경영학박사수료)

〈관심분야〉
ISO국제인증, 정보보호관리체계, 정보보안, 개인정보보호, 위험관리, 업무연속성관리, 금융/의료 클라우드 보안

안 종 창(Jong-Chang Ahn) [정회원]

- 1994년 2월 : 고려대학교 경제학과 (경제학사)
- 2002년 8월 : 세종대학교 소프트웨어대학원 인터넷S/W학과 (공학석사)
- 2007년 8월 : 한양대학교 정보기술경영학과 (공학박사)
- 2020년 8월 : 옥스포드대학교 (경영학박사)
- 1996년 1월 ~ 2010년 8월 : (주)데이콤, SK브로드밴드 매니저
- 2010년 9월 ~ 현재 : 한양대학교 정보시스템학과 부교수

〈관심분야〉
정보시스템(IS) 사용자 행태, 지식경영, 전자상거래, IS 감리