신뢰성응용연구
제14권, 제2호. pp.108-113, 2014

ISO/IEC 27001 : 2013 정보보안경영시스템의 특징과 적용 방안

송경일[1†] · 장중순[2]

[1]한국뷰로베리타스·[2]아주대학교 산업공학과

Characteristics and Implementation of ISO/IEC 27001 : 2013 Information Security Management System

Kyung-Il Song[1†] · Joong-Soon Jang[2]

[1]Division of Certification, Bureau Veritas Korea, [2]Department of Industrial Engineering, Ajou University

The demand against the risk analysis and information security of system from the companies or the agencies which operate an information system is increasing. ISO/IEC 27001 was established by ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). Also this standard is international and authoritative standard of ISMS (Information Security Management System). This paper is to review how the ISO 27001 ISMS Requirement has been established and improved, and to communicate the significant changes from ISO27001 : 2005 to ISO 27001 : 2013 focusing on reasons for revisions. Additionally, This paper shows case study for understanding ISO 27001 : 2013 implementation.

Keywords: ISO/IEC 27001, ISMS(Information Security Management System)

1. 서 론

현대사회의 정보통신과 인터넷의 확산으로 개인의 생활양식 및 기업의 비즈니스가 급격히 바뀌게 되고 정보화 사회가 발전함에 따라 주변의 모든 업무들이 정보시스템에 의존하여 빠르고 편리하게 되었지만 급속한 정보화의 물결과 맞물려 개인정보 유출, 고객의 정보 유출 및 산업기밀 유출 등 다양한 부작용 또한 증가되고 있고, 이러한 부작용을 막기 위해 정보보안체계를 구축하고 있지만 이로 인해 개인의 정신적, 물질적 피해 뿐만 아니라 기업은 물론 국가 경쟁력 저하로 이어지는 막대한 피해를 가져오는 일이 발생하게 되었다. 이러한 정보 유출을 막기 위한 정보보안을 위해서는 정보보호관리체계의 조직 내 구축, 정착 및 유지관리를 통하여 정보의 유출 및 손실을 최소화하여야 한다. 국내의 거의 모든 기업은 인터넷과 정보통신 시스템을 사용하고 있고, 이러한 정보시스템 운영으로 인한 부작용에 대응하기 위해 정보보안을 위한 부서가 있으며 정보보안 활동을 하고 있으나, 지속적으로 발생되는 정보 유출 사건에 의해 정보보안체계의 신뢰성에 대한 문제가 제기되고 있고, 정보보안 활동에 대해 제3자나 거래하는 고객에게 어느 정도의 신뢰성을 줄 수 있는지에 대해 확인 및 평가하기 어려운 것이 실정이다. 이에 따라 기업이나 기관들이 체계적인 보안관리에 중점을 둔 ISO/IEC 27001 정보보안경영시스템(Information Security Management System : ISMS)에 관심을 갖고 시스템 도입을 추진하고 있다. ISO/IEC 27001 정보보안경영시스템은 기업 및 기관의 막연한 정보보안체계를 구체적인 정보보안체계로 갖출 수 있도록 하고 ISO/IEC 27001 정보보안경영시스템 구축 및 인증을 통해 제3자 또는 거래하는 고객 및 상위의 기업에게 정보보안에 대한 신뢰성을 가져다 줄 수 있다.

ISO/IEC 27001은 국제표준 정보보안 경영시스템으로 정보보안 분야에서 가장 권위있는 인증으로, 영국 표준인 BS 7799를 기반으로 하여 2005년 10월에 새로운 국제표준인 ISO/IEC 27001로 승격되었다. ISO/IEC 27001은 조직의 전체적인 비즈니스 위험 환경 내에서 문서화된 ISMS를 수립, 구현, 운영, 모니터링, 검토, 유지 및 개선하기 위한 요구사항을 규정한다. 또한, 이 규격은 개별 조직 또는 조직 일부의 요구에 따른 보안통제의 구현을 위한 요구사항을 규정한다(국제표준화기구, 2005).

† 교신저자 devon.song@kr.bureauveritas.com
2014년 2월 18일 접수; 2014년 4월 19일 수정본 접수; 2014년 5월 9일 게재 확정.

ISO/IEC 27001은 2005년에 최초 제정되고 2013년에 개정되었으며, 2014년 11월부터는 기존에 인증받은 ISO/IEC 27001에 대해서 2013년판의 ISO/IEC 27001 경영시스템으로 전환을 하여야 한다.

정보보안과 보안시스템의 신뢰성에 대한 관심의 증대에 따라 ISO/IEC 27001 정보보안경영시스템에 대한 연구도 점차 증가되고 있다. 박낙규(2012)는 산업보안관리체계 인증취득을 위한 방안에 대해 연구하였고, 장상수와 이호섭(2010)은 정보보안경영시스템 인증심사 시 부적합사항에 대해 분석을 하였으며, 김태달(2007)은 ISO/IEC 27001의 보안성숙도 측정 및 척도 체계에 대해 연구하였다. 또한 Zoran과 Marija (2010)는 정보보안시스템의 방침을 설정하는 방안을 제시하였다. 정보보안경영시스템에 대한 관심의 증대에 따라 관련 연구도 점차 늘어가고 있고, 많은 기업 및 기관들이 ISO/IEC 27001 : 2005 정보보안경영시스템을 구축하고 유지하고 있지만, ISO/IEC 27001 : 2005와 ISO/IEC 27001 : 2013의 차이점 비교 분석 및 ISO/IEC 27001 : 2013 정보보안경영시스템 구축에 관한 연구는 전무한 실정이다.

본 논문은 이러한 ISO/IEC 27001 정보보안경영시스템 규격의 출현과 개정 내용에 대해 살펴보고, ISO/IEC 27001 : 2005와 ISO/IEC 27001 : 2013의 변경된 요구사항 분석을 통하여 이를 기업에서 어떻게 실행으로 옮겨야 할 것인지에 대한 실행 방안을 제시하고자 한다. 제 2장에서는 ISO/IEC 27001 규격에 대한 내용을 간략하게 정리하여 제시하고, 제 3장에서는 ISO/IEC 27001 : 2013 변경된 요구사항을 분석한다. 제 4장에서는 이러한 규격 변경 사항을 반영하여 정보보안경영시스템을 보완하고 실행하기 위한 방안을 다루고, 결론은 제 5장에서 제시한다.

2. ISO/IEC 27001 규격 개요

ISO/IEC 27001 정보보안경영시스템은 전체 경영시스템의 일부분을 차지하며, 사업의 위험성 접근에 기초를 두고 정보보안을 수립, 실행, 운영, 감시, 검토, 유지 및 개선하는 경영시스템이다. 이 규격은 정보자산을 적절하게 보호하고 기타 이해관계자에게 신뢰성을 제공하기 위한 적절하고 알맞은 통제를 보장토록 계획한다. 규정된 요구사항은 포괄적이며, 조직의 형태, 규모 및 특성에 관계없이 모든 조직에 적용될 수 있다.

ISO/IEC 27001 규격은 PDCA 개념에 따라 ISMS 시스템 구축과 실행, 그리고 지속적 향상 달성을 위한 요구사항으로 구성되어 있는데, PDCA의 각 단계별 활동은 다음과 같다.

- P단계 : ISMS 수립 및 관리
- D단계 : ISMS 구현 및 운영
- C단계 : ISMS 모니터 및 검토
- A단계 : ISMS 유지 및 개선

PDCA 모델에 의한 ISMS 주요 요건으로는 경영층 검토, 위험성 평가, 효과성 측정, SOA(Statement of Applicability; 적용성 보고서), 내부감사 등으로 구성되어 있고 부속서 성격으로 Annex A의 Control objectives and controls 관리항목으로 구성되어 있으며, 보안의 3요소인 기밀성, 무결성 및 가용성에 대한 자료 유지에 초점을 맞추고 있다.

기밀성, 무결성 및 가용성은 아래의 <표 1>과 같은 의미를 가지고 있다.

〈표 1〉 기밀성, 무결성 및 가용성의 의미

용어	의미
기밀성	정보의 비밀이 누설되지 않고 유지가 지속적으로 이루어지는 것
무결성	비인가적 대상으로부터 정보의 변조, 삭제 등을 막는 것
가용성	서비스가 계속 유지되 인가된 대상에게 정보가 제공되는 것

Annex A는 정보보호정책, 정보보호조직, 자산관리, 인력자원보안, 물리적 및 환경보안, 통신 및 운영관리, 접근통제, 정보시스템 구축, 개발 및 유지, 정보보호 사고관리, 사업 연속성 관리, 적법성에 대해 관리하도록 항목이 규정되어 있고, Annex A에서 제시하는 관리항목의 목적은 아래의 <표 2>와 같다.

〈표 2〉 관리항목과 그 목적

관리항목	목적
정보보호정책	정보보호관리에 대한 방침과 지원 사항을 제공
정보보호조직	조직 내에서 정보보호를 효과적으로 관리하기 위해 정보보호에 대한 책임을 설정
자산관리	조직의 자산에 대한 적절한 보안책을 유지
인력자원보안	고용 전, 고용 중, 고용 만료로 분류하여 사람에 의한 보안 실시
물리적 및 환경보안	비 인가된 접근, 손상과 사업장 및 정보에 대한 영향을 방지
통신 및 운영관리	정보처리 설비의 정확하고 안전한 운영을 보장
접근통제	정보에 대한 접근통제 실시
정보시스템 구축, 개발 및 유지	정보시스템 내에 보안이 수립되었음을 보장
정보보호 사고관리	정보시스템과 관련된 정보보호 사건에 대해 적절하게 의사소통되고 대응책을 신속하게 수립
사업연속성 관리	사업활동에 방해요소를 완화시키며 주요 실패 및 재해의 영향으로부터 주요 사업활동을 보호
적법성	조직의 정보보호정책이나 지침을 준수

3. ISO/IEC 27001 : 2013 변경 요구사항의 파악과 분석

본 장에서는 ISO/IEC 27001 : 2005가 ISO/IEC 27001 : 2013으로 전환되면서 어떠한 내용이 변경되었는가를 파악하고, 변경사항을 반영하기 위해 ISMS의 보완작업의 방향을 찾고자 한다.

3.1 주요 변경사항

ISO/IEC 27001 : 2013 규격은 2013년 10월에 개정이 되었는데, 개정의 주요 내용은 다음과 같다.

- 리더십의 중요성 강조
- ISMS 내의 책임과 권한을 지정
- 위험성 평가시 위험과 기회를 고려
- 위험성 평가 프로세스를 규정
- 정보보안의 목표 수립시 고려할 사항 규정

ISO/IEC 27001 : 2005와 ISO/IEC 27001 : 2013 규격 요건에 대한 비교를 <표 3>과 같이 나타낼 수 있다. ISO/IEC 27001 : 2013 규격에서는 ISO/IEC 27001 : 2005 규격과 비교하여 보면, 리더십에 대한 조항이 추가되었고, ISO/IEC 27001 : 2005의 4항 정보보안관리 시스템이 ISO/IEC 27001 : 2013의 6항 계획, 7항 지원, 8항 운영으로 구분되면서 위험성 평가에 대한 부분이 보다 명확히 기술되어졌다(국제표준화기구, 2013).

〈표 3〉 ISO/IEC 27001 : 2005와 ISO/IEC 27001 : 2013 요건 비교표

ISO/IEC 27001 : 2005		ISO/IEC 27001 : 2013	
조항	기준	조항	기준
1	범위	1	범위
2	인용규격	2	규범적 참고문헌
3	용어와 정의	3	용어 및 정의
4	정보보안관리 시스템	6 7 8	계획 지원 운영
5	경영책임	4 5	조직의 맥락 리더쉽
6	내부 ISMS 심사 ISMS에 대한 경영검토	9	성과평가
7	ISMS 개선	10	개선

3.2 요건별 변경사항

변경된 요구사항에 대해 각 요건별로 살펴보기로 한다.

3.2.1 4항 조직의 맥락

1) 변경사항

(1) 4.1항 조직과 그 맥락의 이해

ISO/IEC 27001 : 2005에서는 ISMS의 수립을 요구하였으나 ISO/IEC 27001 : 2013에서는 외부 및 내부 이슈의 결정을 강조하고 있다.

(2) 4.2항 이해당사자들의 니즈와 기대의 이해

이해관계자를 식별하고 그들의 보안에 대한 요구사항이 결정되어지도록 요구하고 있다.

(3) 4.4항 정보보안 관리시스템

조직의 사업환경, 내부 및 외부 이해관계자의 요구사항 및 조직 내에서 또는 외부에서 수행되는 활동의 인터페이스와 종속성을 고려하고 문서화하도록 요구하고 있다.

2) 변경배경분석

조직의 목적 및 ISMS의 의도된 결과를 달성하고, 조직에 의해 수행된 활동 및 다른 조직 에 의해 수행된 활동 간의 독립성을 강화하고자 구체적으로 명시하였다.

3.2.2 5항 리더십

1) 변경사항

(1) 5.1항 리더십 및 의무

ISMS가 조직의 프로세스로 통합될 수 있도록 보장 및 의도한 결과를 달성할 수 있음을 보장하도록 명시하고 있다. 또한 지속적 개선을 증진하며 리더십이 타 관련 있는 관리자의 책임에 적용될 수 있도록 지원하도록 규정하고 있다.

(2) 5.2항 정책

보안 요구사항을 달성하는 것에 대한 의지와 지속적 개선에 대한 사항이 강조되었고, 조직 내에서 의사소통 및 이해관계자가 활용할 수 있도록 규정하고 있다.

(3) 5.3항 조직의 역할, 책임 및 권한

ISMS의 성과를 주기적으로 최고경영자에게 보고하도록 명시하고 있다.

2) 변경배경분석

단지 경영에 의한 시스템이 아니라 리더십의 중요성을 강조하고, 가장 높은 레벨에서 개 인 조직을 지휘하거나 통제하는 최고 경영진이 ISMS에 가장 큰 관여를 하여야 한다는 취지를 반영하고 있다.

3.2.3 6항 계획

위험평가 시 위험과 기회에 대해 파악하도록 요구하고 있다. 또한 위험성평가 프로세스가 규정되어야 하고, 위험성 처치 프로세스를 정의하고 있으며, 보안목표를 설정하여 문서화하도록 요구하고 있다.

1) 변경사항

(1) 6.1항 위험 및 기회에 대한 조치

ISMS를 기획 시에는 조직의 상황, 이해관계자 요구사항과 다음의 사항에 대한 위험과 기회를 고려하도록 요구하고 있다.

- ISMS가 달성하고자 하는 결과의 보장
- 예방, 축소 및 원치 않는 영향
- 지속적 개선의 달성

또한, 정보보안 위험성 평가 시, 정보보안의 위험 기준을 수립 및 유지하도록 요구하고 있다.

(2) 6.2항 정보보안 목적 및 그 달성을 위한 계획

ISO/IEC 27001 : 2013에서는 ISO/IEC 27001 : 2005에 비해 정보보안의 목표수립을 매우 강조하고 있는데, 목표수립을 위해 고려할 사항을 다음과 같이 명시하고 있다.

- 정책과 일관성을 가질 것
- 측정 가능할 것
- 정보보안의 요구사항, 위험평가, 위험처리의 결과를 고려할 것
- 의사소통될 것
- 적절히 갱신될 것

2) 변경배경분석

조직은 ISMS의 범위 및 이에 대한 의도된 결과에 대하여 위험 및 기회를 식별하여 이를 통해 ISMS가 목표를 달성함을 보장하고, 적용 가능한 정보보안 요구사항, 위험 평가 및 위처리 결과를 고려하도록 구체적으로 요건 해석의 폭을 제시하였다.

3.2.4 7항 지원

1) 변경사항

(1) 7.2항 역량

인원의 적격성을 결정시, 각 인원은 교육, 훈련과 경험을 바탕으로 적격성이 있다는 것을 보장하여야 함을 요구하고 있다.

(2) 7.3항 인지

조직의 구성원은 ISMS의 효과성에 어떻게 공헌하는지, ISMS를 지키지 못했을 경우에 발생하는 상황에 대해 기술하여 인식하도록 명시하고 있다.

2) 변경배경분석

어떤 자원과 역량 요구사항을 결정하는 조직의 요구는 ISMS를 지원해야한다는 것을 언급하였고, ISMS와 관련된 내부 및 외부 의사소통의 방법을 명시함으로써 ISMS를 유지하기 위해 필요한 지원사항을 구체적으로 언급하였다.

3.2.5 8항 운영

1) 변경사항

(1) 8.1항 운영 계획 및 제어

프로세스 및 필요한 조치를 기획, 이행 및 관리하고 목표를 달성하기 위한 계획을 수립 및 이행하도록 하고 있다.

(2) 8.2항 정보보안 위험 평가

프로세스가 계획대로 이행되었다는 신뢰를 줄 수 있도록 기록을 남기도록 요구하고 있고, 외주처리된 프로세스를 결정하고 그 외주처리된 프로세스가 정보보안에 있어서 관리되고 있다는 것을 보장하도록 명시하고 있다.

(3) 8.3항 정보보안 위험 처리

계획된 주기 및 중대한 변경이 발생시 위험평가를 수행하고, 위험 처리계획을 실행하도록 규정하고 있다.

2) 변경배경분석

계획된 또는 계획되지 않은 변경사항을 파악하고 해결하여 악영향을 완화시키고, 외주처리된 프로세스에 대해서도 명시하여 정보보안을 수행하기 위한 기준을 강화하였음을 알 수 있다.

3.2.6 9항 성과 평가

1) 변경사항

정보보안 활동의 효과성평가가 특히 강조되고 있는데, 그에 대한 모니터링을 위해 조직이 다음의 사항을 결정하도록 명시하고 있다.

- 프로세스와 통제를 포함하여 무엇을 감시하고 측정할 것인가?
- 감시, 측정, 분석 및 평가하는 방법은 수립되어 있는가?
- 감시 및 측정의 시기는 수립되어 있는가?
- 누가 감시 및 측정을 할 것인가?
- 감시 및 측정의 결과는 언제 그리고 누가 하도록 되어 있는가?

2) 변경배경분석

정보보안성과 및 ISMS의 효과를 평가하기 위해 필요한 정보를 결정하고, 이를 바탕으로 누가, 어떻게 측정하고 모니터링하도록 결정함으로써 ISO/IEC 27001 : 2005에 비해 범위 및 수행할 활동을 보다 상세히 요구함으로써 ISMS의 성과 평가의 중요성을 강조하고 있다.

3.2.7 10항 개선

1) 변경사항

부적합이라는 개념이 포함되었고, 부적합 발생시 시정을 하고 부적합의 원인을 제거하기 위한 시정조치의 필요성을 결정하도록 명시하고 있다. ISO/IEC 27001 : 2005 규격에 있던 예방조치에 대한 사항은 삭제되었다.

2) 변경배경분석

부적합에 대한 조치 및 통제활동을 하고, 유사한 잠재 부적합을 파악하여 정보보안의 지속적 개선이 가능하도록 구체적으로 명시하였다.

4. ISO/IEC 27001 : 2013 규격의 적용 방안

4.1 적용 방안

ISO/IEC 27001 : 2013로의 전환에 필요한 적용 여유 기간을 주기 위해 2013년 11월을 기점으로 2014년 10월까지 이 개정 규격의 적용을 위한 준비기간으로 설정되어 있으며, 2014년 11월부터는 ISO/IEC 27001 : 2013 규격에 의거한 심사가 이

루어진다. 이미 ISO/IEC 27001 : 2005 규격의 요건으로 인증을 확보하여 적용하고 있는 업체들은, 2014년 11월부터는 ISO/IEC 27001 : 2013 규격으로 심사를 받을 수 있도록 일정 계획을 수립하여 갱신 심사 또는 신규 심사를 받아서 인증을 확보해야 한다. 개정된 ISO/IEC 27001 : 2013 규격이 제시하는 심사 접근방식과 강조점은 다음과 같다.

- 리더십
- ISMS의 책임과 권한
- 위험성 평가 프로세스 및 위험성 평가시 위험과 기회를 고려

개정된 규격에 따른 정보보안경영시스템을 정착하기 위해 단계별로 실행계획을 세우는 것이 바람직하며, 아래와 같이 6단계로 나누어 실행할 것을 제시한다.

-1단계 : TFT 구성
-2단계 : 변경 사항 파악, 관련 자료 수집 및 교육
-3단계 : 범위 설정
-4단계 : 위험성 평가
-5단계 : 관리체계 구축 또는 재정립
-6단계 : 인증절차 진행

각 단계별 실행 계획을 <표 4>와 같이 정리하였다.

〈표 4〉 단계별 실행 계획

단계	실행 계획
1	ISO/IEC 27001 : 2013 구축에 필요한 팀 구성
2	변경 사항 파악, 관련 자료 수집 및 구성된 팀에 대해 충분한 교육 실시
3	단계별로 구축하기 위한 PDCA별 세부일정 수립
4	위험성 평가 및 문제점 도출
5	문제점에 대한 대응책 수립, 부적합 개선 및 시정조치
6	인증기관의 심사를 통한 인증서 획득

각 단계별 구체적인 활동방안을 아래와 같이 나타내었다.

1단계 : TFT 구성
조직 내에서 효과적이고 효율적으로 정보보안 활동을 수행할 수 있도록 TFT 조직을 구성한다. 정보보안의 전체 책임자와 각 부서별 정보보호 담당자를 지정하여 조직을 구성한다.

2단계 : 시스템 구축 및 ISO/IEC 27001 : 2013 적용을 위해 외부교육기관을 통해 실무추진자 과정이나 내부심사원 과정을 수강한다. 또한 자체적으로 ISMS 인증 및 운영을 담당하는 실무자 간의 워크숍을 실시한다.

3단계 : 범위 설정
ISMS의 적용 범위를 설정한다. 이는 조직의 전체를 대상으로 적용 범위를 설정할지, 또는 중요 정보를 취급하는 특정 부서에 한하여 적용 범위를 설정할지, 또는 외주처리되는 프로세스까지 적용 범위를 설정할지를 결정하도록 한다.

4단계 : 위험성 평가
기밀성, 무결성, 가용성에 의한 자산가치에 대하여 위험성 평가를 실시한다. 평가된 위험성에 대해 위험의 심각성을 결정하도록 한다.

5단계 : 관리체계 구축 및 재정립
보안 정책, 보안 매뉴얼 및 절차서, 보안 지침 및 보안 프로세스를 수립한다. 출입 통제시스템, 보안카메라 등 물리적 보안체계를 구축하고, 네트워크, 컴퓨터, 데이터베이스 등에 대해 보안 솔루션을 구축하도록 한다.

6단계 : 인증절차 진행
인증기관에 연락하여 인증심사를 받기 위한 절차를 진행한다. 인증견적을 위한 신청서를 인증기관에 제출하면 인증기관에서는 심사일수와 심사비용을 알려주게 되고, 심사를 진행하기로 합의가 되면 정해진 심사일수에 따라 심사가 진행되게 된다. 심사는 1단계 문서심사와 2단계 현장심사로 구분되며, 심사 후 인정서 발급되기까지는 부적합 사항 종료 후 보통 1개월 정도 소요된다.

4.2 적용 사례

사례회사인 A보안회사는 1999년에 설립된 보안컨설팅 및 모의해킹, 시스템진단 등의 보안체계에 대한 진단 및 보안체계를 수립 업무를 하는 업체이다. 2013년에 ISO/IEC 27001 : 2005에 의한 ISMS를 구축하였고, 2014년 3월에 ISO/IEC 27001 : 2013에 의거한 심사에 대비하여 시스템을 구축한 상태이다. ISO/IEC 27001 : 2013으로 업그레이드하는 데 소요된 기간은 약 3개월이고, 컨설턴트의 도움없이 회사 자체적으로 구축하였다. A보완회사는 기존에 ISO 9001 : 2008 품질경영시스템 인증을 받은 상태이고, ISO 9001 : 2008 품질경영시스템 절차서에 ISO/IEC 27001 : 2013 정보보안경영시스템 절차서를 추가하여 통합경영시스템으로 구축을 하였다. 구축된 절차서 리스트를 <표 5>와 같이 나타내었다.

아래의 <표 5>를 보면, 총 24개의 절차서 중 ISO 9001과 ISO/IEC 27001의 공통되는 절차서는 9개, ISO 9001에만 해당되는 절차서는 5개, ISO/IEC 27001에만 해당되는 절차서는 10개이고 총 24개의 절차서로 이루어져 있다. ISO/IEC 27001 : 2005와 ISO/IEC 27001 : 2013를 비교시, 추가되는 절차서는 경영책임 및 권한규정과 의사소통관리규정인데, 경영책임 및 권한규정에 리더십에 대한 내용이 기재되어 있고, 의사소통관리규정에는 ISMS와 관련된 내부 및 외부 의사소통과 관련된 내용이 기재되어 있다. 그 외의 정보보안관련 절차서는

기존의 ISO/IEC 27001 : 2005에 이미 구축되어 있는 절차서지만, 절차서의 내용에 있어서는 ISO/IEC 27001 : 2013의 요구사항에 부합하도록 많은 부분이 보완되어 있다고 할 수 있다.

〈표 5〉 ISO 9001 : 2008(품질)과 ISO/IEC 27001 : 2013 (정보보안)의 통합 절차서

No.	절차서명	공통	품질	정보보안
1	문서 및 자료관리규정	○		
2	사내표준관리규정	○		
3	기록관리규정	○		
4	조직 및 업무분담규정	○		
5	경영책임 및 권한규정			○
6	경영검토규정	○		
7	의사소통관리규정			○
8	구매업무관리규정	○		
9	식별 및 추적성관리규정		○	
10	교육훈련규정	○		
11	고객불만처리규정		○	
12	고객만족도관리규정		○	
13	위험성평가규정			○
14	정보보호규정			○
15	통제지원규정			○
16	외주계약규정			○
17	자산관리규정			○
18	정보분류규정			○
19	접근제한규정			○
20	통신 및 운영관리규정			○
21	시정 및 예방조치규정	○		
22	지속적인 개선활동규정	○		
23	영업관리규정		○	
24	구매업무규정		○	

5. 결 론

끊임없이 발전하는 정보화와 인터넷에 인한 편리함도 있지만 각종 개인 정보 유출 및 기업의 기밀 사항 유출 등으로 인해 정신적 및 물질적 피해뿐만 아니라 기업에만 국한되지 않고 국가도 큰 피해를 입게 되며, 결과적으로는 우리 개개인 모두가 피해를 입게 되는 시대가 되었다. 그에 대한 부작용을 막기 위한 많은 방안 중의 하나로 ISO/IEC 27001 정보보안경영시스템의 도입이 기업을 중심으로 확산되고 있는 추세이다. ISO/IEC 27001 규격에서 제시하고 있는 사항을 제대로 실천한다면 정보유출로 인한 부작용이 크게 줄어들 것으로 판단된다. 또한, ISO/IEC 27001 인증을 통해 제 3자나 거래하는 고객 및 상위의 거래 기업에게 정보보안의 신뢰성을 객관적으로 확인시켜 줄 수 있다. 제대로 된 시스템 구축을 위해서는 인증을 받기 위한 형식적인 문서상의 구축이 아닌 최고경영자의 깊은 관심과 리더십이 무엇보다도 필요하다. 그리고 ISMS 구축 및 지속적인 유지관리를 위해서는 항상 최신의 동향 및 정보에 관심을 가져야 하는데, 산업기밀보호센터, 검찰청, 경찰청, 한국인터넷진흥원, 한국정보보호진흥원과 같은 기관의 홈페이지에 방문하면 많은 도움이 될 것으로 판단된다.

본 논문은 ISO/IEC 27001 : 2013 규격의 개요와 변경된 요구사항 분석, 시스템 구축을 위한 방안을 단계별로 제시하였다. 이를 통해 기업체들이 보다 쉽게 개정된 방향을 파악하고 인증을 취득하여 실질적인 정보보안 활동 및 정보보안의 신뢰성을 확보하는데 직접적인 도움이 될 수 있기를 기대한다.

참고문헌

[1] 국제표준화기구 (2005), International Standard ISO/IEC 27001 : 2005, 국제표준화기구.

[2] 국제표준화기구(2013), International Standard ISO/IEC 27001 : 2013, 국제표준화기구.

[3] 박낙규 (2012), 산업보안관리체계 인증 수립 방안 연구, 한국산업기술대학교 산업기술경영대학원.

[4] 장상수 · 이호섭 (2010), 정보보호관리체계(ISMS) 인증심사 결함사항 분석에 관한 연구, *정보보증학회지*, 제20권, 제1호, pp. 31-38.

[5] 김태달 (2007), ISO 27001의 ISMS 보안성숙도 측정 모델링에 관한 연구, *한국컴퓨터정보학회지*, 제12권, 제6호, pp. 153-160.

[6] Zoran Cosic, Marija Boban (2010), Information Security Management - Defining Approaches to Information Security Policies in ISMS, *IEEE International Symposium on Intelligent Systems and Informatics*, Vol. 8, pp. 83-85.