ISMS와 ISO22301 비교를 통한 인증 활성화 방안

A Study on Activation of Authentication by Comparing ISMS and ISO22301

이 선 원* • 이 성 엽** • 정 종 수***
Lee, Sun-Won • Lee, Sung-Yeop • Cheung, Chong-Soo

요 약

본 연구에서는 국내의 정보보호관리시스템(ISMS)와 국외의 비즈니스연속성관리시스템(ISO22301)의 비교를 통해 ISO22301의 인증 활성화 방안을 모색하였다. 또한, ISMS와 ISO22301의 정의 및 필요성, 인증, 인증혜택 등을 알아보고 ISO22301 인증 활성화 방안에 대해 연구하였다. 연구 결과 ISMS 인증은 의무이고 인증 혜택도 전문업체 지정 시 가산점, 입찰 과제선정 평가 시 가산점 부여 등 명확한 혜택이 있었으나 ISO22301은 조직의 명성강화 브랜드 보호 등 인증의 혜택보다는 인증의 효과적인 측면이 강하므로 ISMS의 인증 중 입찰 과제선정 평가 시 가산점 부여, 정보보호관련 보험 가입 시 할인 혜택 등 명확한 혜택을 부여한다면 현재 ISO22301 인증 보다 활성화 될 것으로 판단한다.

keywords : ISMS, ISO22301, 인증, PDCA

1. 서 론

최근 ISO22301 인증을 필요로 하는 기업이 점점 늘어나고 있다. 그래서 ISO22301의 인증 활성화 방안 연구를 위해 국내에서 시행하고 있는 ISMS와 국제표준으로 정하고 있는 ISO22301의 정의 및 필요성, 인증대상, 인증심사, 인증혜택 등을 파악한다. ISMS은 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간 일일평균 이용자수 100만명 이상인 자는 의무로서 정하고 인증을 받으면 각종 혜택을 주고 있으나 ISO22301은 대기업, 중소기업을 포함한 모든 크기와 종류의 조직에 포괄적으로 적용하고 있는데도 혜택이 미비하여 본 연구에서는 ISMS와 비교를 통해 ISO22301인증을 활성화 할 수 있는 방안을 제시하고자 한다.

2. ISMS와 ISO22301 정의 및 필요성

ISMS는 기업(조직)이 각종 위협으로부터 주요 정보자산을 보호하기 위해 수립·관리·운영하는 종합적인 체계이며, 정보의 기밀성, 무결성, 가용성을 실현하기 위해 수립, 관리, 운영하는 일련의 과정 및 활동이고 ISO22301은 중단적 사고 발생 시 이에 대한 예방, 발생가능성의 감소, 대비, 대응 및 복구하기 위한 경영시스템을 계획, 수립, 실행, 운영, 모니터, 검토, 유지 및 지속적인 개

* 숭실대학교 일반대학원 기업재난관리학과 박사과정 sunwonh@naver.com
** 숭실대학교 일반대학원 기업재난관리학과 박사과정 tiemori@koreaexim.go.kr
*** 숭실대학교 일반대학원 기업재난관리학과 교수 isobcm@gmail.com

선에 대한 요구사항을 규정하고 있다.

3. ISMS와 ISO22301 인증 비교

ISMS는 ①인증대상은 정보통신망서비스를 제공하는 자(ISP), 집적정보통신시설 사업자(IDC), 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자, ②인증심사의 종류는 최초심사, 사후심사, 갱신심사, ③인증기준은 관리과정과 정보보호대책으로 정보보호대책과정은 총 13개 분야에 대한 인증기준으로써 정책, 조직, 교육 등 관리적 부문과 개발, 보안통제, 운영 통제 등 물리적·기술적 부문에 대한 정책, 준수 및 검토 등 분야별 관리·운영에 대한 라이프사이클을 구성하고 있다.

ISO22301은 ①인증대상은 산업, 상업, 공공 및 비영리로 운영되는 대기업, 중소기업을 포함한 모든 크기와 종류의 조직에 포괄적으로 적용, ②인증심사의 종류는 최초심사, 사후심사, 갱신심사, ③인증절차는 ISO22301 PDCA 구조인 Plan(계획수립), Do(실행 및 운영), Check(모니터링 및 검토), Act(유지 및 개선)으로 구성하고 있다.

3. ISMS와 ISO22301 인증 혜택 비교

표 1 ISMS와 ISO22301의 인증 혜택

구분	ISMS	ISO22301
인증혜택	-공공부문 정보시스템 기획·구축·운영 사업자, SW개발사업자 선정 시 가산점, 보안관제 전문업체 지정 시 가산점 -지식정보보안 컨설팅전문업체 지정 시 가산점 -KISA는 정보보호대상, 입찰 과제선정 평가 시 가산점을 부여 -보험사에서는 정보보호관련 보험 가입 시 할인 혜택	-위험관리 비용절감 보험료 절감 -법/규제 검증 및 준수 공급망 관리 및 서비스 경쟁력 강화 -조직의 명성강화 브랜드 보호 -우수기업인증에 대한 혜택

3. 결론

ISO22301 인증의 우수기업에 대한 혜택 뿐만 아니라 ISMS의 인증 중 입찰 과제선정 평가 시 가산점을 부여하거나 정보보호관련 보험 가입 시 할인 혜택을 준다면 ISO22301 인증 활성화가 기대된다.

감사의 글

이 논문은 행정안전부의 기업재난관리 전문인력 양성사업으로 지원되었습니다.

참고문헌

최승우 (2016) 보안컨설팅 절차 개선 방안에 관한 연구-BCP중심으로

이재철 (2016) ISMS 인증의 기대 효과와 실질적 효과의 차이에 관한 연구

KISA (2016) ISMS 인증제도 안내서, KISA, 2016.3

kfq 한국품질재단 http://www.kfq.or.kr/certi/certi_iso22301.asp