ISO 27001의 11가지 분야

장정훈

ISO 27001?

- ISO 27001은 영국의 BS 7799를 기반으로 구성되어 있는, 일종의 보안 인증이자 보안 프레임워크이다.

ISO 27001?

- ISO 27001에서는 평가 항목을 11가지로 정의한다.
  - A.5 ~ A.15 조항으로 이루어짐

11가지 평가 분야

	구분	세부 평가 항목
1	A.5 보안 정책(Security Policy)	2
2	A.6 정보 보안 조직(Organization of Information Security)	11
3	A.7 자산 분류 및 통제(Asset management)	5
4	A.8 인력 자원 보안(Human Resource Security)	9
5	A.9 물리적 및 환경적 보안(Physical and Environmental Security)	13

11가지 평가 분야

	구분	세부 평가 항목
6	A.10 통신 및 운영 관리 (Communications & Operations Management)	32
7	A.11 접근 제어(Access control)	25
8	A.12 정보 시스템의 구축과 개발 및 운영 (Information System Acquisition, Development & Maintenance)	16
9	A.13 정보 보안 사고의 관리 (Information security incident management)	5
10	A.14 사업의 연속성(Business continuity management)	5
11	A.15 준거성(Regulatory compliance)	10

A.5 보안 정책

- 보안 정책, 지침, 절차 등을 문서화하는 것에 대한 내용을 담고 있다.

- A.5.1 정보 보안 정책
  - 2가지

A.6 정보 보호 조직

- 정보 보호 체계를 유지하기 위한 조직, 보안 절차를 수행하는 조직, 외부 조직과의 연계 등에 관련된 내용을 담고 있다.

- A.6.1 내부 조직
  - 8가지

- A.6.2 외부 조직
  - 3가지

A.7 자산 분류 및 통제

- 조직의 자산(회사의 기밀, 기술과 같은 정보 자산 포함)에 다한 적절한 보안 정책을 유지하기 위한 내용을 담고 있다.

- A.7.1 자산에 대한 책임
  - 3가지

- A.7.2 정보의 분류
  - 2가지

A.8 인력 자원 보안

- 사람에 의한 보안의 중요성을 강조하며 고용 전, 고용 중, 고용 만료로 분류하고 있다.

- A.8.1 고용 전
  - 3가지

- A.8.2 고용 중
  - 3가지

- A.8.3 고용의 만료 또는 변경
  - 3가지

A.9 물리적 및 환경적 보안

- 비인가된 물리적 접근을 차단하여 조직의 자산이 손실, 파손되는 것을 막고, 조직의 지속적인 활동을 보장하기 위한 내용을 담고 있다.

- A.9.1 보안 영역
  - 6가지

- A.9.2 장치 보안
  - 7가지

A.10 통신 및 운영관리

- 정보 처리 설비의 정확하고 안전한 운영을 보장하기 위한 내용을 담고 있다.

- A.10.1 운영 절차 및 책임
  - 4가지
- A.10.2 외주 용역 관리
  - 3가지
- A.10.3 시스템 계획 및 적용
  - 2가지
- A.10.4 모바일 코드 및 악성 코드에 대한 보호
  - 2가지

A.10 통신 및 운영관리

- A.10.5 백업
  - A.10.5.1 보안 정책에 따라 주기적으로 백업을 해야 한다.
- A.10.6 네트워크 보안 관리
  - 2가지
- A.10.7 매체 관리
  - 4가지
- A.10.8 정보의 교환
  - 5가지
- A.10.9 전자상거래 서비스
  - 3가지
- A.10.10 모니터링
  - 6가지

A.11 접근 제어

- 사용자에 대한 접근 권한에 대한 통제 사항을 담고 있다.

- A.11.1 사업 목적상 접근 제어
  - 사업과 관련하여 접근 제어 정책을 수립하고, 문서화하고, 검토해야 한다.

- A.11.2 사용자 접근 관리
  - 4가지

- A.11.3 사용자의 책임
  - 3가지

A.11 접근 제어

- A.11.4 네트워크 접근 제어
  - 7가지
- A.11.5 운영체제 접근 제어
  - 6가지
- A.11.6 응용 프로그램 제어
  - 2가지
- A.11.7 모바일 컴퓨팅
  - 2가지

A.12 정보 시스템의 구축과 개발 및 운영

- 정보 시스템 보안 관리와 관련한 일련의 사항을 담고 있다.

- A.12.1 정보 시스템과 관련된 요구사항
  - 새로운 정보 시스템에 대한 사업적 요건과 기존의 시스템에 대한 개선점은 정보 보호 통제를 고려한다.

- A.12.2 응용 프로그램의 올바른 정보처리
  - 4가지

- A.12.3 암호화 통제
  - 2가지

A.12 정보 시스템의 구축과 개발 및 운영

- A.12.4 시스템 파일의 보안
  - 3가지

- A.12.5 개발 및 변경과 관련된 보안
  - 5가지

- A.12.6 기술적 취약점 관리
  - 정보 시스템에 대한 기술적 취약점은 주기적으로 확인하고, 관련 위험에 대한 평가가 이루어져야 한다.

A.13 정보 보호 사고의 관리

- 정보 시스템과 관련된 정보 보호 사건이나 약점 등에 대해 적절히 의사소통하고 대응책을 신속하게 수립하기 위한 내용을 담고 있다.

- A.13.1 정보 보호 관련 사건 및 취약점 보고
  - 2가지

- A.13.2 정보 시스템에 대한 침입 관리 및 개선
  - 2가지

A.14 사업의 연속성

- 정보 시스템의 붕괴나 자연재해로부터 시스템을 적절히 복구하여 사업의 연속성을 보장하기 위한 내용을 담고 있다.

- A.14.1 사업 연속성 측면에서의 보안
  - 5가지

A.15 준거성

- 법을 위반하지 않기 위한 정보 보호의 법적 요소를 담고 있다.

- A.15.1 법적인 요건에 대한 정합성
  - 6가지

- A.15.2 보안 정책, 표준, 기술적 적합성
  - 2가지

- A.15.3 정보 시스템 감사에 대한 고려
  - 2가지

토스, 국제표준 정보보호 인증 'ISO/IEC 27001' 및 'ISO/IEC 27701' 취득

2020. 04. 27 · by 토스

토스, 주요 국제표준 정보보호 인증 2건 취득