Interactive PDF

ISO/IEC 27001: 2022 개정

지난 2022년 10월, 새로운 ISO/IEC 27001 표준 문서가 발표되었습니다. 따라서 정보보호경영시스템(ISMS)에 대한 업데이트 및 정보 보안 재정비가 필요한 시점입니다.

본 문서를 통해 이번에 변경된 표준이 귀사의 ISMS 인증 전환을 어떻게 지원하는지 개략적으로 알아보시기 바랍니다. 변경사항에 대해 자세히 알아보려면 BSI의 온디맨드 교육을 시청하세요.

편집상 변경 사항

신규 요구 사항

새로운 보안 기준 4가지

Clause 5
Organizational controls
조직적 통제

Clause 6
People controls
사람에 대한 통제

Clause 7
Physical controls
물리적인 통제

Clause 8
Technological controls
기술적인 통제

개정된 부록 A 보안 통제

통제 수가 114개에서 93개로 감소

24 통합

58 개정

11 신규

기준 및 위험 관리를 지원하기 위한 5개의 통제 속성

통제 유형

정보 보안 속성

사이버 보안 개념

운영 역량

보안 도메인

새로운 표준은 3년간의 전환 기간을 허용하며, 오늘날의 사이버 및 정보 보안 환경을 다루도록 설계되었습니다.
따라서 아직 전환을 시작하지 않았다면 지금 바로 첫 걸음을 내딛어 보십시오.

원활하고 효과적으로 전환을 완료할 수 있는 방법을 알아보려면 **BSI 에 문의주십시오.**

편집상 변경 사항

- 새로운 ISO Harmonized 구조와 일치합니다.

  ISO 표준의 기본 원칙은 모두 함께 적용될 수 있다는 것입니다. 이번 업데이트로 ISO/IEC 27001를 다른 표준과 함께 이행할 수 있게 되었습니다. 즉, 보다 프로세스 중점적인 접근 방식을 채택함으로써 표준과 상호작용하는 이해관계자에게 명확성을 제공하고, 표준 이행 전반에 걸쳐 간편하고 일관적인 접근 방식이 가능하게 되었습니다.

- 원활한 번역을 위해 일부 영어 문장 구조 재배치
- Harmonized approach에 일치하도록 일부 넘버링 재구성
- 부록 A 또는 ISO/IEC 27002에 더 이상 존재하지 않는 통제 목표에 대한 참조 삭제
- 신규 조항 6.3 – 변경 계획

신규 요구 사항

- 표준 이행 및 ISMS 유지에 필요한 프로세스 및 상호작용 정의
- 조직 내 정보 보안과 관련있는 역할에 대한 설명
- 정보 보안 목표 모니터링
- 조항 7.4의 일부로 조직에서 커뮤니케이션 방법을 정하도록 함
- 운영 프로세스의 기준을 설정하고, 해당 기준에 따른 프로세스 통제 이행
- 조직에서 제 3자 프로세스 뿐만 아니라, 정보 보안과 관련된 모든 외부 제품, 프로세스 및 서비스를 통제

새로운 보안 기준 4가지

Clause 5
Organizational controls

조직적 통제

구체적인 기준보다 넓은 조직적 문제에 대한 통제를 의미합니다. 예를 들어 경영 정책, 공급망 내 정보 보안 등이 해당됩니다.

- 통제 37개
- 기존 34개
- 신규 3개

Clause 6
People controls

사람에 대한 통제

개인과 관련된 통제로, 교육부터 고용 계약 조건에 이르기까지 다양한 문제를 다룹니다.

- 통제 8개
- 기존과 동일

Clause 7
Physical controls

물리적인 통제

물리적인 보안 대상에 대한 통제를 다룹니다. 물리적인 출입, 장비의 안전한 폐기 및 재사용 등을 포함합니다.

- 통제 14개
- 기존 13개
- 신규 1개

Clause 8
Technological controls

기술적인 통제

기술과 관련한 통제를 다룹니다. 예를 들어 보안 인증 또는 구성 관리 등이 해당됩니다.

- 통제 34개
- 기존 27개
- 신규 7개

부록 A 개정판 보안 통제: 114개에서 93개로 통제 영역 감소

24 통합

일부 통제가 통합된 이유

이전 표준에서 분리할 수 없거나 밀접하게 관련된 24개 영역에 대한 통제를 통합하였습니다. 이는 ISO/IEC 27001의 핵심인 프로세스 중심의 harmonized approach에 따라 통합되었습니다.

예를 들어, 2013 버전에는 액세스 및 액세스 통제에 대해 3개의 개별 통제가 있었는데, 2022 버전에서는 단일 통제로 통합하여 액세스 통제의 개발, 이행 및 유지 관리 프로세스를 완전하게 정의합니다.

통합이 중요한 이유

이러한 일부 통제의 제거 및 통합은 특정 통제의 세부 사항이 해당 통제에 대한 프로세스, 기준 및 상호작용을 명확하게 정의해야 하는 요구 사항에 이미 포함되기 때문에 진행되었습니다. 즉, 표준의 중요 부분, 조직의 맥락, 계획 및 운영을 먼저 검토하는 것이 필수적입니다.

먼저 프로세스와 상호 작용을 결정한 후에 새로 통합된 통제 집합을 다뤄야 합니다.

58 개정

개정된 통제 종류

현재 기업 환경과 관계된 위협을 반영하기 위해 58개의 통제를 개정하고 업데이트하였습니다. 특히 원격 근무가 위험 관리의 중요한 부분이 되었기 때문에 관련 통제의 이름을 변경하고 그 내용을 적절하게 업데이트했습니다.

필요 조치

개정된 통제의 심각성은 다양하나, 모든 통제에 대한 검토를 통해 일부 통제는 광범위하게 업데이트되었습니다. 새로운 비즈니스 운영 방식과 현재 직면하는 위협에 대응하기 위해서는 이러한 개정 사항을 이행해야 하므로, 업데이트된 지침을 반드시 확인해야 합니다.

11 신규

신규 도입된 통제 내용

지난 10년 동안 클라우드 컴퓨팅 및 개인정보보호 요구 사항 등 새롭게 대두된 위험 영역을 해결하기 위해 신규 통제를 도입했습니다. 또한, 아래와 같이 IT부서와 조직 자체의 위협 분석 및 비즈니스 연속성과 같이 중요성이 더 강화된 프로세스를 공식화하는 통제를 새롭게 개발했습니다.

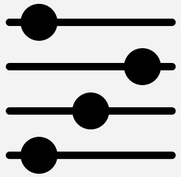
- 조직적 통제
  - 위협 분석
  - 클라우드 서비스 사용을 위한 정보 보안
  - 비즈니스 연속성을 위한 ICT 준비
- 물리적 통제
  - 물리적 보안 모니터링
- 기술적 통제
  - 구성 관리 정보 삭제
  - 데이터 마스킹
  - 데이터 손실 예방
  - 모니터링 활동
  - 웹 필터링
  - 안전한 코딩

모범 사례 (Best Practice)

ISO/IEC 27002의 최신 버전에서는 모범 사례 및 규정 준수 유지 방법을 포함하여 각각의 신규 통제를 위한 정보를 제공합니다.

기준 및 위험 관리를 지원하기 위한 5개의 통제 속성

해당 통제 속성이 기준과 위험 관리에 도움이 되는 원리는 다음과 같습니다



통제 유형

세 가지의 기본 통제 유형은 예방(애초에 취약점이 발생하지 않도록 방지), 탐지(취약점이 발생할 때 경고), 그리고 제거(취약점 이후 복구)입니다. 귀사의 정보보호 경영 시스템이 이 세 가지 측면을 어떻게 균형맞추고 있는지 이해하면 전체적인 위험 관리의 접근방식을 이해할 수 있습니다.

정보 보안 속성

정보 보안의 세 가지 원칙은 기밀성, 무결성, 그리고 가용성입니다. 새로운 표준의 모든 통제에는 이 세 가지 원칙 중 하나 이상을 지원하는지 여부를 나타내기 위한 태그(#)가 지정되어 있습니다. 이를통해 비즈니스에 적합한 기밀성, 무결성, 가용성의 균형을 확보하기 위해 통제를 잘 이행하고 있는지 평가하는 것이 훨씬 쉬워졌습니다.

사이버 보안 개념

이 속성을 활용하면 귀사의 통제 기능이 단순한 보호 이상으로 회복탄력적인 보안 시스템의 역할을 하는지 여부에 따라 통제를 분류할 수 있습니다. 여기에는 기존 위협 및 새로운 위협 식별, 자산 보호, 의심스러운 활동 감지, 침해 또는 공격에 대한 대응 및 복구가 포함됩니다.

운영 역량

조직의 정보 자산을 보호하기 위해 발휘할 수 있는 조직 운영 역량은 다양합니다. 이 속성에 따라 통제 이행 사항을 필터링하면 조직적 위험을 해결하기 위한 통제 조합을 지원하는 데 필요한 운영 역량이 무엇인지 이해할 수 있습니다.

보안 도메인

보안 도메인 역시 거버넌스, 및 에코시스템, 보호, 방어 및 회복탄력성으로 그룹화할 수 있습니다. 이 속성에 따라 통제 이행 사항을 필터링하면 조직적 위험에 대응하여 각 도메인 별로 균형맞춰 이행되었는지 확인할 수 있습니다.