2025년 2학기

중간 대체

REPORT

과목명 : 정보보호관리평가

학 과 : 정보보안공학과

학 번 : 202121556

이 름 : 곽지현

ISO/IEC 27001

ISO/IEC 27001은 국제표준화기구(ISO)와 국제전기기술위원회(IEC)가 공동 제정한 정보보호 관리체계(Information Security Management System, ISMS) 분야의 대표적인 국제표준이다. 이 표준은 조직이 비즈니스 위험 기반 접근 방식을 바탕으로 정보보안을 수립, 운영, 모니터링, 검토, 개선할 수 있도록 지원하는 경영 시스템을 정의한다.

조직은 보유한 정보자산의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 유지하기 위한 보안 관리 체계를 수립하며, 업무, 구조, 위치, 자산, 기술적 특성 등을 고려하여 정보보호 관리체계의 적용 범위를 설정할 수 있다. ISO/IEC 27001은 조직의 규모나 업종에 관계없이 보편적으로 적용 가능하다.

ISO/IEC 27001의 목적

ISO/IEC 27001의 주요 목적은 조직 전반에 정보보호 관리체계를 구축하여 정보보안 리스크를 체계적으로 관리하고, 보호 수준을 지속적으로 향상시키는 데 있다. 이를 통해 기업은 데이터 보안 위험을 효과적으로 관리하고 있음을 대내외에 입증할 수 있다.

ISO/IEC 27001 인증은 조직이 국제 표준과 정보보호 모범 사례의 요구사항을 충족하고 있음을 보여주며, 정보보호 위험에 선제적으로 대응하고 사이버 위협으로 인한 비즈니스 중단을 예방하는 기반이 된다. 더불어, 관련 법규 준수와 이해관계자 신뢰 확보에도 기여하게 된다. 이러한 이유로 많은 글로벌 기업들이 협력사나 고객의 요청에 따라 해당 인증을 획득하고 있다.

ISO/IEC 27001 도입은 사이버 공격에 대한 대응력과 회복력을 높이며, 정보의 정확성·기밀성·무결성을 확보하고, 구성원 간 정보보호 책임을 명확히 하여 조직 전반의 보안 의식을 강화한다. 이는 단순한 보안 강화 차원을 넘어, 기업의 대외 경쟁력과 지속가능성을 높이는 전략적 수단이 되며, 특히 데이터 기반 산업에서는 고객 신뢰 확보와 글로벌 거래의 핵심 기반이 된다. 또한, 보안 사고를 예방함으로써 장기적인 비용 절감 효과도 기대할 수 있다.

ISO/IEC 27001의 주요 구성 요소 및 구조

ISO/IEC 27001은 정보보호 관리체계를 구축·운영하기 위한 요구사항을 제시하며, 경영시스템 표준의 공통 프레임워크에 기반한 구조를 갖는다. 이 표준은 조직의 운영 환경 분석부터 계획 수립, 실행, 평가, 개선에 이르는 일련의 절차와, 정보보호 통제를 위한 부속서(Annex A)로 구성된다.

핵심 요구사항은 기술 중심의 단발성 대응을 넘어서, 전략적이고 지속 가능한 정보보호 운영을 목표로 한다. 이 구조는 Plan-Do-Check-Act(PDCA) 사이클을 바탕으로, 조직의 환경을 진단하고 정보보호 목표와 계획을 수립한 후 통제를 실행하고 그 효과를 평가하며, 결과를 바탕으로 개선하는 과정을 포함한다. 이를 통해 조직은 정보보호 절차를 내재화하고 체계적으로 강화할 수 있다.

부속서 A(Annex A)는 조직이 수행한 위험 평가 결과에 따라 필요한 보안 통제를 선택적으로 적용할 수 있도록 총 93개의 통제 항목을 제시한다. 2022년 개정판에서는 기존 114개 항목을 통합·간소화하고, 현대 보안 환경을 반영해 재구성되었다.

모든 통제 항목은 조직, 인원, 물리, 기술의 네 가지 주제 영역으로 분류되며, 각각은 정보보호의 다양한 분야를 포괄한다.

조직 통제는 보안 정책 수립, 자산 관리 체계 마련, 외부 공급자와의 보안 계약 등과 같이, 조직 차원에서 수립되는 절차와 관리 구조를 포함한다. 이러한 통제는 정보보호를 위한 전사적 운영 기반을 마련하는 데 필수적이다.

인원 통제는 인사보안, 임직원의 보안 인식 교육, 사용자 행위 책임의 명확화 등을 통해 인적 요소로 인한 보안 위험을 최소화하는 데 중점을 둔다.

물리적 통제는 정보시스템이 위치한 공간과 장비를 보호하기 위한 조치로, 시설 접근 제한, 장비 보호, 환경적 위협으로부터의 보호 수단 등을 포함한다.

기술적 통제는 정보 시스템 자체에 대한 보안 대책으로, 접근 권한 관리, 암호화 기술의 적용, 네트워크와 시스템 보안, 애플리케이션 개발 단계의 보안 기능 구현 등을 포함한다.

이러한 구성은 개별 기술에 의존하지 않고, 정보보호를 조직 전체의 경영시스템 안에서 통합적이고 지속 가능한 방식으로 운영할 수 있도록 한다. ISO/IEC 27001은 국제 표준으로서 신뢰성과 유연한 적용 가능성을 동시에 갖추고 있다.

ISO/IEC 27001 기반 ISMS 구축 절차

ISO/IEC 27001 기반의 정보보호 관리체계(ISMS)는 PDCA(Plan-Do-Check-Act) 사이클을 중심으로 설계되며, 조직이 정보보호 수준을 지속적으로 향상시키기 위한 실행 중심의 관리 프로세스를 제공한다.

이 사이클은 문서화에 머무르지 않고, 조직의 실제 운영과 정보보안 활동이 유기적으로 연계되도록 설계되어 있다. 각 단계는 개별적인 작업이 아닌 상호 연결된 흐름으로, 위험 식별에서 통제 실행과 점검, 개선에 이르기까지 전 과정에서 지속적인 관리 활동이 필요하다.

그림. ISO/IEC 27001 기반 정보보호관리체계의 PDCA 사이클 구조
출처: 한국표준협회(KSA), [https://ksa.or.kr/ksa_kr/7011/subview.do]
※ 국내 ISMS 가이드라인(KISA 등)도 유사한 PDCA 기반의 절차로 구성되어 있어, 실무 적용 시 활용할 수 있다.

계획(Plan) 단계에서는 조직의 ISMS 적용 범위를 정의하고, 최고경영자의 정보보호 정책 수립과 함께 정보자산 목록 작성, 위협 및 취약점 식별, 위험 평가, 대응 전략 수립, 통제대책 선정, 정보보호 목표 설정 및 실행계획 수립 등을 통해 성과 측정 기준을 마련한다.

실행(Do) 단계에서는 수립된 보안 정책과 통제를 실제로 이행한다. 방화벽 구축, 접근권한 설정, 보안 솔루션 도입 등의 기술적 조치뿐 아니라, 보안 인식 교육, 보안 조직 구성, 일상적인 보안 운영 등 실무 활동을 통해 위험을 통제한다.

점검(Check) 단계에서는 운영 상태와 효과성을 평가한다. 내부 보안 감사, 사고 대응 체계 점검, 모니터링 체계 운영 등을 통해 정책과 절차의 이행 여부를 확인하고, 경영진 검토를 통해 개선 사항을 도출한다.

조치(Act) 단계에서는 점검 결과 확인된 문제점에 대해 시정조치를 실시하고, 새로운 위협 환경이나 조직 변화에 따라 ISMS 범위와 통제를 갱신한다. 정책 개정, 통제 보완, 적용 범위 조정 등을 통해 관리체계를 개선하고, 그 결과는 다음 Plan 단계에 반영되어 PDCA 사이클이 지속적으로 순환된다.

이러한 절차는 조직이 정적인 통제 수준을 넘어, 동적인 위험 관리 체계를 통해 정보보호 역량을 강화하고 지속 가능한 ISMS를 운영할 수 있도록 한다. ISO/IEC 27001은 각

단계에서 필요한 문서화 요건을 명확히 제시하며, 정보자산 목록, 위험 평가 보고서, 정책 및 절차서, 운영 기록, 내부감사 결과 등은 인증 심사 시 핵심적인 평가 자료로 활용된다.

기업 실무에서의 ISO/IEC 27001 적용 예시

ISO/IEC 27001을 기업 현장에서 구현할 때에는 관리적 통제와 기술적 통제를 균형 있게 운영하는 것이 핵심이다. 관리적 통제는 조직의 정책, 절차, 사람에 관한 보안 조치를 의미하며, 기술적 통제는 시스템과 기술을 활용한 보안 대책을 의미한다.

관리적 통제의 대표적인 실무 적용 사례로는, 최고경영자의 참여 아래 정보보호 정책을 수립하고 전사에 공표하는 것을 시작으로, 정보보호 전담조직(CISO 조직)을 구성하고 부서별 보안 책임자와 역할을 명확히 설정하는 것이 포함된다. 전 직원을 대상으로 정보보안 교육 및 인식 제고 프로그램을 정기적으로 실시해 인적 보안을 강화하며, 정보자산 관리 절차를 수립해 자산 목록을 체계적으로 관리하고 중요도에 따라 분류한다. 또한, 협력사·외주업체와의 계약에 보안 요구사항을 명시하고, 주기적인 평가를 통해 외부자 보안 리스크를 통제한다. 더불어 정기적인 위험 평가 및 리스크 처리 활동을 운영하고, 보안 사고 대응 절차와 비상시 사업연속계획(BCP)도 문서화하여 대비한다.

기술적 통제의 대표적인 실무 적용 사례로는, 중요 시스템 및 데이터베이스에 대해 접근 통제를 강화하여 사용자 계정과 권한을 엄격히 관리하는 것이 있다. 직무 기반 접근 권한 부여 원칙을 설정하고, 다단계 인증(MFA)을 도입해 인증 보안을 강화한다. 데이터 저장 및 전송 과정에서는 암호화 기술을 적용하여 정보 유출을 방지하며, 네트워크 보안을 위해 방화벽, 침입탐지시스템(IDS/IPS)을 설치하고, 보안 로그 수집·분석 시스템(SIEM)을 운영해 이상 징후를 탐지한다. 애플리케이션 개발 시에는 보안 코딩 가이드라인을 준수하고, 변경 시 취약점 점검을 통해 개발 보안을 확보한다. 물리적 보안 측면에서는 서버실에 출입통제 시스템(스마트카드·생체인증)을 적용하고, CCTV 모니터링, 비상 전원 확보 및 데이터 백업·복구 체계를 구축한다. 또한, 보안 사고 대응팀(CERT)을 운영하여 사고 발생 시 신속하게 대응하고, 정기적으로 모의 침투 테스트 및 재해복구 훈련을 실시해 기술적 통제의 실효성을 점검한다.

이처럼 관리적 통제는 사람과 절차를 중심으로 보안 기반을 마련하는 활동이며, 기술적 통제는 IT 인프라 측면에서 보안을 강화하는 조치이다. ISO/IEC 27001을 효과적으로 구현하기 위해서는 두 통제가 유기적으로 작동해야 하며, 강력한 암호화 기술도 운영 정책과 키 관리 절차 같은 관리적 기반이 뒷받침되어야 효과를 발휘할 수 있다.
실제 인증 심사에서는 관리 문서와 기술 구현 간의 정합성, 그리고 변경 이력 관리의 체계성도 중요한 평가 항목이 된다.

KISA의 ISMS-P와 ISO/IEC 27001을 비교/분석

KISA의 ISMS-P와 ISO/IEC 27001은 모두 조직의 정보보호 수준을 체계적으로 향상시키기 위한 관리체계 인증 제도이지만, 적용 범위와 세부 통제 항목, 인증 목적 등에서 차이를 보인다.

ISMS-P는 한국인터넷진흥원(KISA)과 과학기술정보통신부가 운영하는 국내 정보보호 및 개인정보보호 관리체계 인증 제도이다. ISMS(정보보호 관리체계)와 PIMS(개인정보보호 관리체계)를 통합한 것으로, 정보보호뿐만 아니라 개인정보의 수집, 이용, 보관, 파기 등 개인정보 생명주기 전반에 걸친 보호 조치를 포함하고 있다. 이에 따라 개인정보를 다량 보유하거나 처리하는 사업자, 특히 통신, 금융, 온라인 플랫폼 사업자 등은 ISMS-P 인증을 통해 법적 요건과 보안 요건을 동시에 충족해야 한다.

반면 ISO/IEC 27001은 국제표준화기구(ISO)와 국제전기기술위원회(IEC)가 공동 제정한 정보보호 관리체계에 대한 국제 표준으로, 조직의 정보자산 전반에 대한 기밀성, 무결성, 가용성을 확보하는 데 중점을 둔다. 업종이나 규모에 관계없이 다양한 조직에서 활용 가능하며, 국제 거래 또는 대외 신뢰도 확보가 필요한 경우 ISO/IEC 27001 인증이 선호된다.

인증 기준을 비교해보면, ISO/IEC 27001은 2022년 개정판 기준으로 총 93개의 통제 항목(Annex A)을 포함하고 있다. 반면 ISMS-P는 정보보호 80개 항목과 개인정보보호 22개 항목을 포함해 총 102개의 심사 항목으로 구성된다. 여기서 ISMS 인증은 개인정보 항목을 제외한 80개 항목만 심사 대상이 되며, ISMS-P는 102개 전체 항목을 충족해야 한다. 두 인증 체계는 정보보호 영역에서 상당 부분 유사한 기준을 공유하고 있으며, 실제로 ISMS-P의 보호대책 중 64개 항목은 ISO/IEC 27001의 통제 항목과 대응된다. 따라서 기존에 ISO/IEC 27001이나 ISMS 인증을 보유한 조직은 추가 항목만 이행함으로써 ISMS-P 인증으로 전환할 수 있다.

또한 평가 관점에서도 차이가 존재한다. ISO/IEC 27001은 위험 기반 접근 방식에 따라 조직이 자율적으로 통제를 설계하고 적용할 수 있도록 유연한 구조를 제공하며, 전반적인 정보보호 체계의 지속적인 개선에 초점을 맞춘다. 반면 ISMS-P는 개인정보 보호법, 정보통신망법 등 국내 관련 법률의 준수 여부를 보다 엄격하게 평가하며, 법적 규제 대응력을 확보하고자 하는 조직에 적합하다.

결과적으로, ISO/IEC 27001은 국제 신뢰 확보와 글로벌 비즈니스 확장을 목표로 하는 조직에 적합하며, ISMS-P는 국내 개인정보 보호 규제 대응이 필요한 조직에 적합하다. 두 인증 체계는 상호 보완적으로 활용될 수 있으며, 조직의 특성과 운영 환경에 따라 적절한 선택이 필요하다. 특히 국내외 고객을 동시에 대상으로 하는 기업이라면, 두 인증을 병행함으로써 내부 보안 역량 강화는 물론 이해관계자의 신뢰 확보에도 유리하다. 이러

한 접근은 정보보호 수준을 제고하는 동시에 경쟁력 있는 보안 거버넌스를 갖추는 전략적 수단이 될 수 있다.

ISMS-P와 ISO/IEC 27001 비교표

구분	ISMS-P (KISA)	ISO/IEC 27001 (국제표준)
인증 주관	한국인터넷진흥원(KISA)	ISO / IEC (국제표준화기구, 국제전기기술위원회)
인증 범위	정보보호 + 개인정보 보호 전 생명주기	정보자산 보호 (기밀성, 무결성, 가용성) 중심
대상 조직	개인정보를 다수 보유·처리하는 조직 (예: 금융, 통신, 플랫폼 등)	업종·규모에 무관한 전 세계 조직 대상
법적 의무성	국내 특정 사업자에 대해 인증 의무 부과 (정보통신망법 등)	법적 의무 없음 (대외 인증 수단으로 활용)
심사 항목 수	총 102개 항목 (정보보호 80 + 개인정보보호 22)	총 93개 통제 항목 (Annex A 기준, 2022 개정판)
법률 연계성	국내 개인정보보호법, 정보통신망법 등과 직접 연계	국제 기준 기반, 국내 법과 직접 연계되지 않음
유연성	고정된 항목 기반 심사	위험 기반 통제 설계로 유연성 제공
인증 목적	국내 규제 준수 및 개인정보 보호 강화	국제 표준 기반 신뢰도 확보, 글로벌 거래 대응
상호 연계성	ISO/IEC 27001 기준과 통제 항목 상당수 호환	ISMS-P의 정보보호 항목과 대부분 일치

※ 위 비교표는 두 인증 제도의 주요 차이점을 시각적으로 정리한 것으로, 조직의 법적 요구사항과 대외 신뢰 확보 목적에 따라 적절한 선택 또는 병행 취득 전략을 수립하는 데 도움이 된다.