cpl.thalesgroup.com

THALES
Building a future we can all trust

대한민국 정보보호 및 개인정보보호 관리체계 인증(ISMS-P) 획득

대한민국 ISMS-P: 대한민국 정보보호 및 개인정보보호 관리체계 인증(ISMS-P)은 한국인터넷진흥원(KISA)이 만든 정보 보안 및 개인정보 관리 표준입니다. 이 표준은 한국 내 기업 및 단체가 정보 자산을 보호할 수 있도록 돕기 위해 제정된 것으로, 개인정보보호법 및 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에 따라 준수를 의무화하고 있습니다.

개요

2018년 11월, 과학기술정보통신부(MSIT)와 방송통신위원회, 행정안전부는 '개인정보보호 관리체계 인증**(PIMS)**'과 **'정보보호 관리체계 인증(ISMS)'**으로 개별 운영되던 인증 체계를 하나로 통합하여 **'정보보호 및 개인정보보호 관리체계 인증'(ISMS-P)**이라는 새로운 인증 제도를 만들었습니다.

이 두 관리 체계를 통합한 목적은 다음과 같습니다.

- 정보 보안과 개인정보 보호를 통합하는 최신 보안 트렌드 반영
- 두 시스템 간 연결성 강화
- 중복된 요구사항으로 인한 조직의 규정 준수 부담 완화

한국 정부는 '정보통신망 이용촉진 및 정보보호에 관한 법률' 제47조에 따라 과학기술정보통신부(MSIT)의 산하기관인 한국인터넷진흥원(KISA)이 주관하는 개인정보 및 정보보호 관리체계 인증(ISMS-P) 제도를 도입했습니다.

- ISMS 제도는 조직이 정보 자산을 일관되고 안전하게 보호할 수 있도록 설계된 엄격한 관리 요건을 규정하고 있는데, 이는 ISO/IEC 27001의 관리 목표와 상당 부분 겹치지만 동일하지는 않습니다.
- 일반적인 ISO/IEC 27001 평가와 비교했을 때 ISMS는 요구 사항에 대한 보다 상세한 심사 항목을 갖추고 있습니다.
- ISMS의 인증 기관은 KISA로, 인증 유효기간은 3년이며, 인증을 받은 기업은 매년 심사를 통과해야 인증 자격을 유지할 수 있습니다.

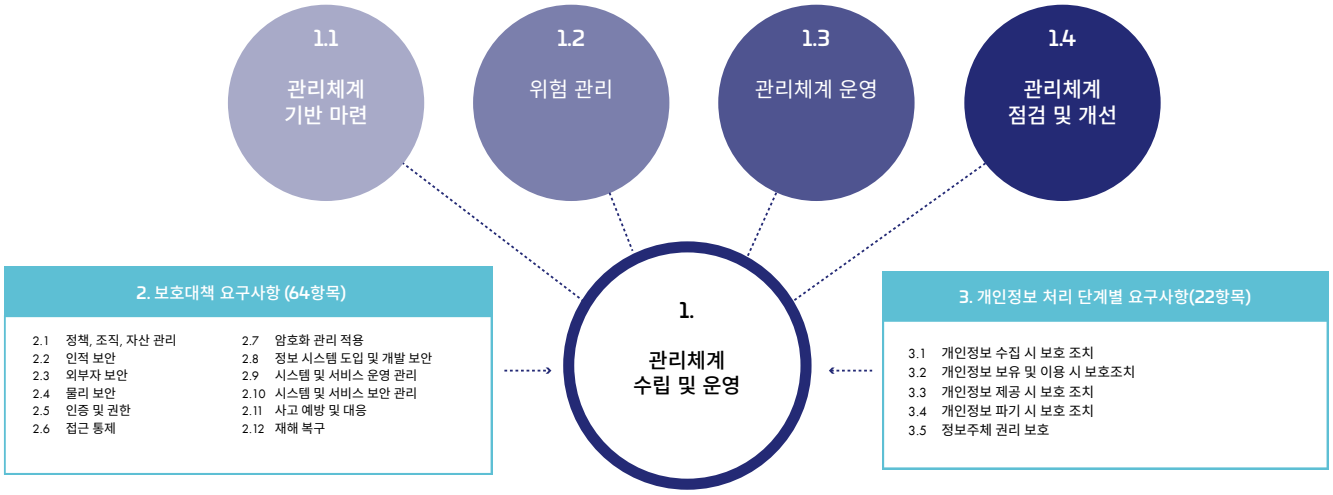
새로운 통합 인증인 **ISMS-P**는 K-ISMS의 104개 인증 항목과 K-PIMS의 82개 인증 항목 대신, 정보 보안 관련 항목 80개와 개인정보 보호 관련 항목 22개로 구성됩니다.

정보 보안 관련 관리 항목 80개

- 관리체계 수립 및 운영 [16]
- 보호대책 요구사항 [64항목]

개인정보 보호 관련 관리 항목 22개

- 개인정보 처리 단계별 요구사항 [22항목]



ISMS-P 인증 의무 대상자

KISA는 다음과 같은 의무 대상자에게 인증 획득을 의무화하고 있습니다.

정보통신망서비스 사업자(ISP)

- 「전기통신사업법」 제6조 1항에 따른 허가를 받은 자

집적정보통신시설 사업자

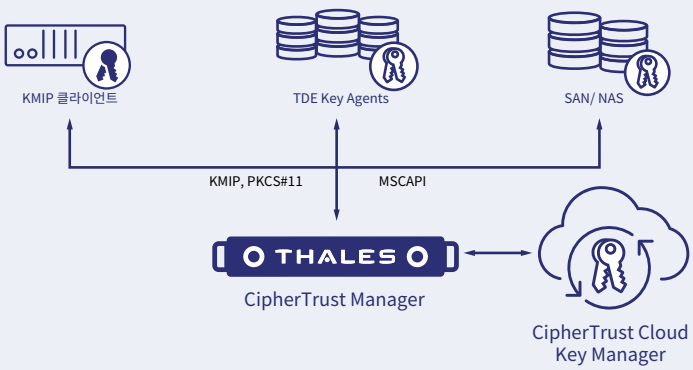
- 「정보통신망법」 제46조에 따른 집적정보통신시설 사업자

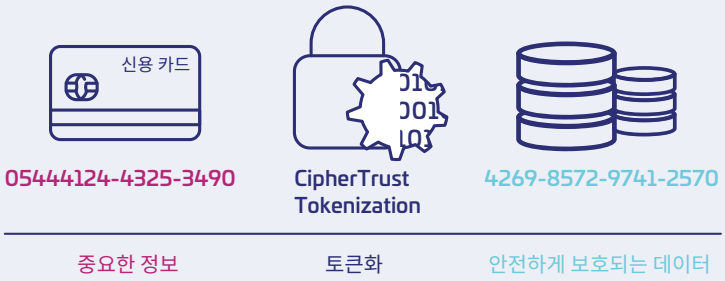
다음 조건 중 하나에 해당하는 자

- 「의료법」 제3조 4항에 따라 '상급종합병원'으로 분류되는 병원 중 연간 매출액 또는 세입이 약 1,952억 원(미화 1억 5천만 달러) 이상인 병원
- 직전 연도 12월 31일 기준으로 재학생 수가 1만 명 이상인 「고등교육법」 제2조에 따른 학교
- 정보통신서비스 부문 매출액이 최근 3개월간 미화 1천만 달러 이상이거나 정보통신서비스 일일 평균 이용자 수가 100만 명 이상인 정보통신망서비스 사업자(단, 「전자금융거래법」 제2조 3호에 따른 금융회사는 제외)

탈레스의 지원 방식

탈레스는 조직의 규제 준수 의무 이행에 관한 폭넓은 경험을 바탕으로 조직이 '정보보호 및 개인정보보호 관리체계 인증**(ISMS-P)**'에 대응할 수 있는 통합 솔루션을 제공합니다.

ISMS-P 요구 사항	권장사항
2.7 암호화 적용 **2.7.2 암호키 관리** • 암호키의 안전한 생성·이용·보관·배포·폐기를 위한 관리 절차를 수립·시행하고, 필요시 복구방안을 마련해야 한다. • 암호키 생성, 이용, 보관, 배포, 폐기에 대하여 다음과 같은 내용의 정책과 절차를 수립해야 한다. • 개인정보 및 중요 정보를 저장, 전송, 전달할 때는 암호화 정책에 따라 암호화를 수행해야 한다.	**암호키 보호** 탈레스의 **Luna HSM(하드웨어 보안 모듈)**은 안전한 암호화 처리, 키 생성 및 보호, 부호화 등을 위한 강력한 변조 방지 환경을 제공합니다. FIPS 140-2 레벨 3 인증을 받은 폼팩터로 제공되는 Luna HSM은 다양한 배포 시나리오를 지원합니다. 또한, Luna HSM은 다음을 수행합니다. • 루트 및 인증 기관(CA) 키를 생성 및 보호함으로써 다양한 사용 사례에 대한 PKI를 지원합니다. • 애플리케이션 코드에 서명하므로 소프트웨어의 위변조를 방지하고 보안을 유지할 수 있습니다. • IoT 애플리케이션 및 기타 네트워크 배포에 사용되는 전용 전자 기기의 자격 증명 및 인증을 위한 디지털 인증서 생성 **키 관리** **CipherTrust Manager**는 모든 CipherTrust 데이터 보안 플랫폼 제품의 키를 중앙에서 관리하고, IBM Security Guardium 데이터 암호화, Microsoft SQL TDE, Oracle TDE, KMIP 호환 암호화 제품을 비롯한 타 업체 기기의 키와 인증서를 안전하게 저장하고 관리할 수 있게 해줍니다. CipherTrust Manager는 키 관리를 통합함으로써 여러 시스템에 걸쳐 일관된 정책을 시행하도록 촉진하며, 교육 및 유지 관리 비용을 절감합니다. 또는 표준 기반 API를 사용하여 키 관리 기능이 내장된 애플리케이션의 배포를 간소화하고, 관리 작업의 테스트와 개발을 자동화합니다. CipherTrust 키 관리 솔루션은 다음과 같이 다양한 사용 사례를 지원합니다. • **CipherTrust Cloud Key Manager**는 Amazon Web Services 및 Microsoft Azure, Salesforce, IBM Cloud의 **BYOK(Bring Your Own Key)** 관리를 간소화합니다. 이 솔루션은 클라우드 키 수명주기를 종합적으로 관리 및 자동화하여 보안 팀의 업무 효율성을 높이고 클라우드 키 관리를 간소화합니다. • **CipherTrust의 Transparent Database Encryption 키 관리**는 Oracle, Microsoft SQL, Microsoft Always Encrypted와 같은 광범위한 데이터베이스 솔루션을 지원합니다. • **CipherTrust KMIP 서버**는 전체 디스크 암호화(FDE), 빅데이터, IBM DB2, 테이프 아카이브, VMware vSphere, vSAN 암호화 등과 같은 KMIP 클라이언트를 중앙에서 관리합니다. 

ISMS-P 요구 사항	권장사항
3.2 개인정보 보유 및 이용 시 보호조치 **3.2.3 개인정보 표시제한** • 개인정보를 조회 및 출력 (인쇄, 화면 표시, 파일 생성 등) 할 때는 목적을 명시하고, 목적에 따라 출력 항목 최소화, 개인정보 표시제한, 출력물 보호조치 등을 수행해야 한다. • 또한 빅데이터 분석, 테스트 등 데이터 처리 과정에서 개인정보가 과도하게 이용되지 않도록 업무에 필수적인 정보가 아닌 개인정보는 삭제하거나 또는 식별할 수 없도록 조치해야 한다.	**동적 데이터 마스킹을 통한 CipherTrust 토큰화** • CipherTrust 토큰화 솔루션은 동적 데이터 마스킹을 사용하는 볼트리스 토큰화 (Vaultless Tokenization)와 볼티드 토큰화(Vaulted Tokenization)라는 두 개의 편리한 솔루션으로 완벽한 유연성을 구현하여 애플리케이션 수준의 토큰화 서비스를 제공합니다. 두 솔루션 모두 데이터 센터, 빅데이터 환경, 클라우드 등에 보관된 중요한 자산을 보호하고 익명화합니다. • CipherTrust 볼트리스 토큰화는 유휴 데이터를 보호하는 동시에 정책 기반의 동적 데이터 마스킹 기능을 통해 사용 중인 데이터를 보호합니다. 또한 중앙 집중식 관리 및 서비스와 결합된 RESTful API를 통해 필드당 단 한 줄의 코드로 토큰화를 구현할 수 있습니다. 볼트리스 토큰화 서비스는 분산 클러스터를 지원하는 전용 토큰화 서버에서 제공되므로 업무를 완전히 분리할 수 있습니다. 편리한 토큰화 구성 워크플로를 갖춘 운영 대시보드가 포함된 토큰화 관리 및 구성은 그래픽 사용자 인터페이스에서 이루어집니다. • CipherTrust 볼티드 토큰화 솔루션은 다양한 기존 형식과 사용자 맞춤형 토큰화 형식을 정의할 수 있는 기능을 통해 무중단 형식 보존 토큰화 서비스를 제공합니다. 볼티드 토큰화는 매우 중요한 데이터에 최상의 보안을 제공하며, 인스턴스를 서버별로 설치하거나 다수의 클라이언트를 지원하는 웹 서비스 형태로 설치할 수 있습니다. 

핵심 사항 요약

데이터 보안 강화 및 ISMS-P 요구사항 충족

- 데이터 보안 간소화 및 규제 준수 소요 시간 단축
- 암호화 또는 토큰화를 통해 중요한 데이터를 보호
- 데이터에 대한 액세스 제어 및 키 관리 중앙화

탈레스 소개

여러분이 개인 정보를 보호하기 위해 이용하는 서비스의 운영 업체들은 자사의 데이터를 보호하기 위해 탈레스의 솔루션을 이용하고 있습니다. 기업이 데이터 보안과 관련해 결단을 내려야 하는 상황이 점차 늘고 있습니다. 탈레스의 솔루션을 사용하면 암호화 전략을 수립하거나, 클라우드로 전환하거나, 규제 준수 의무를 이행하는 등 어떠한 순간에도 디지털 트랜스포메이션을 안전하게 수행할 수 있습니다.