eBook

ISO/IEC 27001:2022 - 정보 보안, 사이버 보안 및 개인정보 보호 표준에 따른 데이터 보안 규정 준수

탈레스 솔루션이 ISO/IEC 27001 규정 준수에 효과적인 이유

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

국제표준화기구(ISO)는 독립적인 비정부 국제 기구로, 170개의 국가 표준화 기관을 보유하고 있습니다. ISO/IEC 27001은 국제표준화기구와 국제전기기술위원회(IEC)가 공동으로 제정하여 세계에서 가장 많이 알려진 정보 보안 경영 시스템(ISMS) 표준입니다. ISO/IEC 27001 표준은 모든 기업에게 정보 보안 경영 시스템을 구성, 구현, 유지 및 지속적으로 개선하는 데 필요한 지침을 제시합니다.

기업이 ISO/IEC 27001을 따른다는 것은 기업에서 소유하거나 처리하는 데이터의 보안과 관련된 위험을 관리할 수 있는 시스템을 구축하고 있으며, 이 국제 표준에 명시되어 있는 실무와 원칙이 해당 시스템에 모두 적용되어 있다는 것을 의미합니다.

ISO/IEC 27001은 어떻게 바뀌었습니까?

ISO/IEC 27001은 2005년에 처음 제정된 이후 2013년 9월 25일에 ISO/IEC 27001:2013으로, 그리고 2022년 10월 25일에 ISO/IEC 27001:2022로 다시 개정되었습니다. 이러한 과정에서 끊임없이 변화하는 기술 및 정보 보안 환경을 반영하여 업데이트되었습니다. 2022년에 일어난 가장 큰 변경사항은 부속서 A입니다.

ISO/IEC 27001 부속서 A는 기업이 ISO/IEC 27001 6.1.3(정보 보안 위험 처리)을 준수하고 있다는 사실을 입증하기 위해 사용하는 보안 통제를 분류하여 열거하고 있습니다. 오늘날 사이버 보안 및 정보 보안 환경에 따라 ISO/IEC 27002:2013에서 총 24개의 통제가 병합되었고, 58가지 통제가 개정되었습니다.

	ISO/IEC 27001: 2013	ISO/IEC 27001: 2022
부속서 A 통제 범주	114가지 통제 항목 14가지 통제 영역	93가지 통제 항목 4가지 통제 영역 • 조직 통제 항목 - 37가지 • 인원 통제 항목 - 8가지 • 물리적 통제 항목 - 14가지 • 기술적 통제 항목 - 34가지

어떤 기업들이 ISO/IEC 27001:2022 인증을 받을 수 있습니까?

ISO 표준은 전 세계 사이버 보안 전문가들에게 동의를 얻어 국제적으로 널리 인정받고 있습니다. ISO 인증은 모든 경제 분야(모든 유형의 서비스 및 제조업을 비롯한 1차 산업, 민간, 공공 및 비영리 단체)에 걸쳐 기업들에게 제공됩니다.

ISO/IEC 27001:2022 규정을 위반할 경우 어떤 처벌을 받게 됩니까?

ISO/IEC 27001은 규정 위반에 따른 처벌이 없는 국제 표준입니다. 하지만 ISO/IEC 27001:2022 인증은 기업이 정보 보안 모범 사례를 이행하여 선의의 노력을 입증함으로써 데이터 유출 발생 시 GDPR과 같은 규정에서 부과하는 벌금을 방어할 수 있는 수단을 제공합니다.

ISO/IEC 27001 규정 준수에 탈레스가 어떤 도움이 될 수 있습니까?

탈레스는 부속서 A에 명시된 필수 정보 보안 통제 요건을 해결하여 기업이 ISO/IEC 27001:2022를 준수할 수 있도록 지원합니다.

ISO/IEC 27001:2022 요구사항	탈레스 솔루션
정보 분류	
5.12: 정보 분류: 정보는 정보 보안 요건에 따라 분류되어야 합니다.	CipherTrust Data Discovery & Classification은 온프레미스 환경과 클라우드 환경의 중요한 정형/비정형 데이터를 식별합니다. 기본적으로 제공되는 템플릿은 규제 데이터를 빠르게 식별하고 보안 위험을 강조하여 규정 준수 공백을 찾아내는 데 효과적입니다.
데이터 보안	
5.3: 업무 분장 서로 상충되는 업무와 상충되는 책임 영역은 분리되어야 합니다. **5.33: 기록 보호** 손실, 파괴, 변조, 무단 액세스 및 무단 배포로부터 기록을 보호해야 합니다. **5.34: 프라이버시 및 PII 보호** 관련 법규와 규정 및 계약 여건에 따라 프라이버시 유지와 PII 보호에 관한 요구사항을 식별하여 충족합니다. **8.7: 멀웨어 차단** 적절한 사용자 인지도를 통해 멀웨어 차단을 구현 및 지원해야 합니다. **8.10: 정보 삭제** 정보 시스템, 장치 및 기타 저장 매체에 저장된 정보는 더는 필요하지 않을 경우 삭제되어야 합니다. **8.11: 데이터 마스킹** 액세스 제어에 관한 기업의 주제별 정책을 비롯한 기타 관련 주제별 정책에 따라 사용되어야 합니다. **8.12: 데이터 유출 방지** 데이터 유출 방지 조치는 시스템과 네트워크, 기타 중요 정보를 처리, 저장, 전송하는 장치에 적용되어야 합니다. **8.24: 암호화 사용** 암호화 키 관리를 포함해 암호화를 효과적으로 사용할 수 있는 규칙을 정의하고 시행해야 합니다.	CipherTrust Data Security Platform은 데이터 검색, 보호 및 제어를 하나의 플랫폼으로 단일화하여 데이터 중심 보안 제품과 솔루션을 통합한 제품입니다. CipherTrust Platform은 파일, 볼륨 및 데이터베이스에 저장된 데이터를 보호할 수 있는 기능을 다양하게 제공합니다. 예를 들면 다음과 같습니다. • CipherTrust Transparent Encryption은 중앙 집중식 키 관리 및 권한 있는 사용자 액세스 제어와 함께 저장 데이터를 암호화합니다. 또한 역할을 완전히 분리하기 때문에 권한이 있는 사용자와 프로세스에서만 암호화가 해제된 데이터를 볼 수 있습니다. 따라서 프라이버시를 보장하는 동시에 온프레미스, 멀티 클라우드, 빅 데이터 및 컨테이너 환경 등 모든 환경에 저장되어 있는 중요 데이터를 보호합니다. • CipherTrust Tokenization은 동적 데이터 마스킹을 사용해 데이터베이스에 저장된 중요한 정보를 가명화하는 동시에 분석 과정이나 보고서에서 중요한 데이터를 노출시키지 않고 집계된 데이터를 분석할 수 있도록 지원합니다. • CipherTrust Enterprise Key Management는 클라우드 및 엔터프라이즈 환경에서 다양한 사용 사례를 통해 키 관리를 간소화하고 강화합니다. 탈레스 키 관리 도구 및 솔루션은 FIPS 140-2 인증 가상 또는 하드웨어 어플라이언스를 이용해 중요한 환경에 대한 보안을 강화하는 동시에 내부에서 개발한 암호화는 물론이고 타사 애플리케이션의 경우에도 중앙에서 키를 관리할 수 있습니다. 또한 암호화 키를 파괴하여 암호화된 정보를 효과적으로 삭제할 수 있습니다. • CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP)은 프로세스에서 비정상적인 I/O 활동 유무를 지속적으로 모니터링하여 랜섬웨어가 엔드포인트와 서버를 완전히 장악하기 전에 악의적인 활동을 알리거나 차단합니다. 또한 랜섬웨어 탐지를 목적으로 현재 진행 중인 프로세스를 모니터링하여 과도한 데이터 액세스, 데이터 유출, 무단 암호화, 악의적인 사용자 사칭과 같은 활동을 찾아내고, 그러한 활동이 탐지되면 사용자에게 알리거나 차단합니다. Thales Luna Hardware Security Modules (HSMs)는 암호화 키를 보호하고, FIPS 140-2 Level 3 인증으로 강력한 변조 방지 환경을 제공하여 안전한 암호화 처리, 키 생성 및 보호, 암호화 등을 지원합니다. Luna HSM은 온프레미스, 서비스형 클라우드, 하이브리드 환경에서 사용할 수 있습니다. Luna HSM: • 루트 키와 인증 기관(CA) 키를 생성하고 보호하여 다양한 사용 사례에서 PKI를 지원합니다. • 애플리케이션 코드에 서명하여 소프트웨어가 안전하고, 조작되지 않은 정품임을 보장합니다. • IoT 애플리케이션을 비롯한 기타 네트워크 배포 시 전용 전자 장치의 자격 증명과 인증에 필요한 디지털 인증서를 생성합니다. Thales High Speed Encryptors (HSEs)는 네트워크에 상관없이 전송 데이터 암호화(계층 2, 3, 4)를 제공하여 사이트 사이에서, 혹은 온프레미스와 클라우드 사이에서 데이터 이동 시 데이터 보안을 보장합니다. 탈레스의 네트워크 암호화 솔루션은 일체의 성능 저하 없이 데이터 유출을 제한하며, 데이터, 비디오, 음성 및 메타데이터를 도청하거나, 감시하거나, 공공연하게 또는 은밀하게 감청하지 못하도록 효과적으로 보호합니다.

ISO/IEC 27001:2022 요구사항	탈레스 솔루션
액세스 제어 및 인증	
5.15: 액세스 제어 정보와 기타 관련 자산에 대한 물리적/논리적 액세스를 제어할 수 있는 규칙을 마련하고 시행해야 합니다. **5.17: 인증 정보** 인증 정보의 할당 및 관리를 관리 프로세스에 따라 제어해야 합니다. **5.18: 액세스 권한** 정보에 대한 액세스 권한을 정책에 따라 프로비저닝, 검토, 수정, 제거해야 합니다. **6.7: 원격 근무** 직원이 원격으로 근무할 때는 보안 조치를 시행해야 합니다. **8.3: 정보 액세스 제한** 정보와 기타 관련 자산에 대한 액세스는 액세스 제어에 대한 기존의 주제별 정책에 따라 제한해야 합니다. **8.4: 소스 코드에 대한 액세스** 소스 코드, 개발 도구 및 소프트웨어 라이브러리에 대한 읽기/쓰기 액세스를 관리해야 합니다. **8.5: 보안 인증** 보안 인증 기술과 절차를 시행해야 합니다.	**Thales OneWelcome** IAM 솔루션은 역할과 컨텍스트에 따라 내/외부 사용자의 액세스를 제한합니다. 세분화된 액세스 정책과 권한 부여 정책은 강력한 인증(MFA)을 기반으로 적격 사용자가 올바른 리소스에 적시에 액세스할 수 있도록 권한을 부여하는 데 효과적입니다. 따라서 무단 액세스 위험이 최소화됩니다. • **SafeNet Trusted Access**는 클라우드 기반의 액세스 관리 솔루션으로, 가장 폭넓은 하드웨어/소프트웨어 인증 방법 및 폼팩터와 함께 시중의 다중 요소 인증을 제공합니다. • **Thales converged badge solutions**는 모든 기업 보안 애플리케이션을 단일 사용자 배지로 통합하여 물리/논리적 액세스 관리를 간소화합니다. 예를 들어 건물 및 출입 제한 구역에 대한 물리적 접근, 카드 소지자에 대한 시각적 식별, PKI-인증서 기반 인증 및/또는 FIDO 인증을 이용한 중요한 디지털 리소스에 대한 보안 액세스 등이 있습니다. • **지원되는 인증 방법**이 광범위하기 때문에 수많은 사용자들의 요건을 충족할 뿐만 아니라 기업이 강력한 다중 요소 인증을 통해 사용자와 중요한 디지털 리소스를 보호하는 데도 효과적입니다. **Thales OneWelcome Consent & Preference Management** 모듈은 기업이 최종 소비자에게서 동의를 구할 수 있도록 지원합니다. 일례로 금융 기관은 동의를 받은 데이터의 가시성을 투명하게 확보하여 활용 가능한 데이터에 대한 액세스를 관리할 수 있습니다. **CipherTrust Transparent Encryption**은 중요한 데이터를 암호화할 뿐만 아니라 권한 있는 사용자 액세스 관리 정책을 세분화하여 사용자, 프로세스, 파일 유형, 일시 등 다양한 매개변수를 기준으로 적용합니다. 또한 역할을 완전히 분리하기 때문에 권한이 부여된 사용자와 프로세스에서만 암호화되지 않은 데이터를 볼 수 있습니다.
클라우드 보안	
5.23: 클라우드 서비스 이용을 위한 정보 보안 클라우드 서비스 구매, 사용, 관리 및 종료를 위한 프로세스를 마련해야 합니다. **5.30: 비즈니스 연속성을 위한 ICT 준비** 비즈니스 연속성 목표에 따라 ICT 준비를 계획, 시행, 유지 및 테스트해야 합니다.	**CipherTrust Cloud Key Manager**는 타사 클라우드 공급업체에서 BYOK 시스템에 따라 중요한 데이터를 보호할 목적으로 호스팅한 키를 기업이 완전히 통제하는 온프레미스 환경을 유지하여 클라우드 보안 위험을 줄일 수 있습니다. **CipherTrust Transparent Encryption**은 관리자 역할을 완전히 분리하기 때문에 권한이 부여된 사용자와 프로세스에서만 암호화되지 않은 데이터를 볼 수 있습니다. 데이터 액세스 시 타당한 사유를 제공하지 않을 경우 무단 사용자는 타사 클라우드에 저장된 중요 데이터에 평문으로 액세스하지 못합니다. **Thales Data Security 솔루션**은 가장 광범위한 데이터 보호 기능을 제공하는데, 대표적으로 클라우드 기반의 Luna Cloud HSM 서비스와 Cipher Trust Key Management 서비스에 고가용성과 백업을 기본적으로 제공하는 **Thales Data Protection on Demand (DPoD)**가 있습니다.

ISO/IEC 27001:2022 요구사항	탈레스 솔루션
애플리케이션 보안	
8.25: 보안 개발 수명 주기 소프트웨어와 시스템에 대한 보안 개발 규칙을 마련하여 적용해야 합니다. **8.26: 애플리케이션 보안 요구사항** 애플리케이션을 개발하거나 구매할 경우에는 정보 보안 요구사항을 구분하고, 지정하고, 승인해야 합니다.	**CipherTrust Platform Community Edition**은 DevSecOps 팀이 하이브리드 및 멀티 클라우드 애플리케이션에 데이터 보호 통제 수단을 쉽게 배포할 수 있도록 지원합니다. 이 솔루션에는 CipherTrust Manager Community Edition, Data Protection Gateway 및 CipherTrust Transparent Encryption for Kubernetes에 대한 라이선스가 포함됩니다. **CipherTrust Secrets Management**는 최첨단 시크릿 관리 솔루션으로, DevOps 도구와 클라우드 워크로드에서 시크릿, 자격 증명, 인증서, API 키, 토큰 등 시크릿에 대한 액세스를 보호하고 자동화합니다. **CipherTrust Application Data Protection**은 암호화 키 관리는 물론이고 중요한 데이터에 대한 애플리케이션 계층 암호화까지 가능한 개발자 친화적인 소프트웨어 도구를 제공합니다. 데이터를 생성하거나 처음 처리할 때 즉시 적용되며, 데이터 수명 주기 상태, 즉 전송 중이든, 사용 중이든, 백업 중이든, 복사 중이든 상관없이 암호화 상태를 유지하여 애플리케이션 계층에서 가장 강력한 수준의 보안을 제공합니다. **Thales Data Protection on Demand (DPoD)**는 클라우드 기반 마켓플레이스로서 Luna HSM 및 CipherTrust 솔루션을 서비스로 제공합니다. 기업 내부 팀은 검증과 인증을 마친 데이터 보안 솔루션을 자체 제품에서 손쉽고 안전하게 이용할 수 있습니다.

탈레스 소개

탈레스는 각국 정부와 세계 유명 기업들이 신뢰하는 데이터 보안 분야의 글로벌 리더로서 고객이 가장 중요한 데이터를 보호할 수 있도록 지원하고 있습니다. 개인정보를 중요시하는 사람들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 기업은 데이터 보안과 관련된 결정적인 순간에 직면하곤 합니다. 탈레스를 사용하면 이러한 순간(암호화 전략 구축, 클라우드 이전, 규정 준수 요건 충족)에도 끊임없는 디지털 혁신이 가능합니다.

cpl.thalesgroup.com

문의 – 지사 위치와 연락처 정보는 cpl.thalesgroup.com/contact-us에서 확인할 수 있습니다.