AWS 인증, 프로그램, 보고서 및 제3자 증명

2017년 1월

고지 사항

이 문서는 정보 제공 목적으로만 제공됩니다. 본 문서의 발행일 당시 AWS의 현재 제품 및 실행방법을 설명하며, 예고 없이 변경될 수 있습니다. 고객은 본 문서에 포함된 정보나 AWS 제품 또는 서비스의 사용을 독립적으로 평가할 책임이 있으며, 각 정보 및 제품은 명시적이든 묵시적이든 어떠한 종류의 보증 없이 "있는 그대로" 제공됩니다. 본 문서는 AWS, 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 보증, 표현, 계약 약속, 조건 또는 보증을 구성하지 않습니다. 고객에 대한 AWS의 책임 및 의무는 AWS 계약에 준거합니다. 본 문서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

목차

요약

AWS는 외부 인증 기관 및 독립 감사 기관과 협력하여 고객에게 AWS에서 확립 및 운영하는 정책, 프로세스 및 컨트롤에 대한 다양한 정보를 제공합니다.

CJIS

AWS는 FBI의 CJIS(Criminal Justice Information Services) 표준을 준수합니다. AWS는 CJIS 보안 정책에 따라 필요한 직원의 신원 조회를 허용 또는 수행하는 것을 비롯하여 고객과 CJIS 보안 협약을 체결합니다.

법 집행 기관 고객(및 CJI를 관리하는 파트너)은 활동 로깅((AWS CloudTrail)), 전송 및 저장 데이터 암호화(자체 키 가져오기 옵션을 포함하는 S3의 서버 측 암호화), 종합적 키 관리 및 보호(AWS Key Management Service 및 CloudHSM), 통합 권한 관리(IAM 연합 ID 관리, 멀티 팩터 인증) 등 AWS의 첨단 보안 서비스 및 기능을 이용하여 CJI 데이터의 보안 및 보호를 개선하기 위해 AWS 서비스를 활용하고 있습니다.

AWS에서는 CJIS 정책 분야에 부합되는 보안 계획 템플릿 형식으로 Criminal Justice Information Services(CJIS) 워크북을 작성했습니다. 또한, 고객이 이 과정에서 클라우드를 채택하도록 돕기 위해 CJIS 백서를 개발했습니다.

CJIS 허브 페이지(https://aws.amazon.com/compliance/cjis/)를 방문하십시오.

CSA

2011년, Cloud Security Alliance(CSA)가 클라우드 공급자 내에서 보안 관행의 투명성을 장려하기 위한 이니셔티브인 STAR를 출범했습니다. CSA Security, Trust & Assurance Registry(STAR)는 공개적으로 액세스 가능한 무료 레지스트리로, 다양한 클라우드 컴퓨팅 상품이 제공하는 보안 컨트롤을 문서화하여 사용자가 현재 사용하고 있거나 계약을 고려 중인 클라우드 공급자의 보안을 평가하는 데 도움을 줍니다. AWS는 CSA STAR 등록자이며 CSA(Cloud Security Alliance) 공동 평가 이니셔티브 질문서(CAIQ)를 작성했습니다. CSA가 발행한 이 CAIQ는 AWS의 서비스 지향 인프라에 어떤 보안 컨트롤이 있는지 참조하고 기록하는 데 이용할 수 있습니다. CAIQ에는 클라우드 소비자 및 클라우드 감사 기관에서 클라우드 공급자에게 물어야 할 298개 질문이 담겨 있습니다.

CSA 공동 평가 질문서를 참조하십시오.

Cyber Essentials Plus

Cyber Essentials Plus는 조직이 흔히 발생하는 사이버 공격에 대한 운영 보안을 입증할 수 있도록 영국 정부가 도입한 인증 체계입니다.

이 인증 체계는 AWS가 영국 정부의 "사이버 보안 10단계(10 Steps to Cyber Security)"의 맥락에서 흔히 발생하는 인터넷 기반 위협의 위험을 경감하기 위해 구현하는 기초 제어를 증명합니다. 이 인증 체계는 영국중소기업연맹(Federation of Small Businesses), 영국산업연합(Confederation of British Industry), 그리고 이 인증을 유지하는 비즈니스에 인센티브를 제공하는 다수의 보험사를 포함해 업계의 지원을 받고 있습니다.

Cyber Essentials는 필요한 기술적 제어를 규정하며, 관련 보장 프레임워크는 인증된 평가자에 의해 수행되는 연간 외부 평가를 통해 Cyber Essentials Plus 인증에서 어떻게 개별 프로세스가 작용하는지 보여줍니다. 인증의 지역적 성격 때문에 인증 범위가 EU(아일랜드) 리전에 제한됩니다.

DoD SRG 레벨 2 및 4

국방부(DoD) 클라우드 보안 모델(SRG)은 클라우드 서비스 공급자(CSP)가 DoD 잠정 권한 부여를 획득하고 이후에 DoD 고객이 활용하도록 하기 위한 공식적인 평가 및 권한 부여 프로세스를 규정합니다. SRG에 따른 잠정 권한 부여는 AWS의 DoD 표준 준수를 증명하는 재사용 가능한 인증을 제공하여 DoD 작업 담당자가 AWS에서의 작업을 위해 시스템 중 하나를 평가 및 인증하는 데 필요한 시간을 단축시킵니다. AWS는 현재 SRG 레벨 2 및 4의 잠정 권한 부여를 획득했습니다.

레벨 2, 4, 5 및 6에 정의된 보안 제어 기준에 대한 자세한 내용은 http://iase.disa.mil/cloud_security/Pages/index.aspx에서 확인할 수 있습니다.

DoD 허브 페이지(https://aws.amazon.com/compliance/dod/)를 방문하십시오.

FedRAMPSM

AWS는 FedRAMPsm(연방 위험 및 인증 관리 프로그램)를 준수하는 클라우드 서비스 공급자입니다. AWS는 FedRAMPsm 공인 평가대행기관(Third Party Assessment Organization, 3PAO)의 테스트를 완료했으며, FedRAMPsm의 중등도 요구 사항 준수를 입증하여 HHS(미국 보건복지부)로부터 두 가지 기관 영업허가권(ATO)을 받았습니다. 모든 미국 정부 기관은 FedRAMPsm 리포지토리에 저장된 AWS 기관 ATO 패키지를 활용하여 해당 기관의 애플리케이션 및 작업에 대해 AWS를 평가하고, AWS 사용 권한을 제공하고, 워크로드를 AWS 환경으로 이전할 수 있습니다. 이 두 가지 FedRAMPsm 기관 ATO에는 모든 미국 리전(AWS GovCloud(미국) 리전과 AWS 미국 동부/서부 리전)이 포함됩니다.

위에서 언급한 리전의 인증 대상 범위에는 다음 서비스가 포함됩니다.

- **Amazon Redshift** – Amazon Redshift는 신속하며 완벽하게 관리되는 페타바이트 규모의 데이터 웨어하우스 서비스로 효율적인 비용으로 간편하게 모든 데이터를 기존 비즈니스 인텔리전스 도구를 사용하여 분석할 수 있게 해 줍니다. 자세한 내용은 여기를 참조하십시오.
- **Amazon Elastic Compute Cloud(Amazon EC2)** – Amazon EC2는 클라우드에서 크기를 조정할 수 있는 컴퓨팅 파워를 제공합니다. 개발자가 보다 쉽게 웹 규모 컴퓨팅 작업을 할 수 있도록 설계되었습니다. 자세한 내용은 여기를 참조하십시오.
- **Amazon Simple Storage Service(S3)** – Amazon S3는 언제든지 웹 상의 어디서나 용량에 관계없이 데이터를 저장하고 검색하는 데 사용할 수 있는 단순한 웹 서비스 인터페이스를 제공합니다. 자세한 내용은 여기를 참조하십시오.
- **Amazon Virtual Private Cloud(VPC)** – Amazon VPC는 고객이 정의하는 가상 네트워크에서 VPC 리소스를 시작할 수 있도록 AWS에서 논리적으로 격리된 공간을 프로비저닝합니다. 자세한 내용은 여기를 참조하십시오.
- **Amazon Elastic Block Store (EBS)** – Amazon EBS는 가용성과 안정성이 뛰어나고 예측 가능한 스토리지 볼륨을 제공합니다. 이 볼륨을 실행 중인 Amazon EC2 인스턴스에 연결하여 인스턴스 내의 디바이스로 표시할 수 있습니다. 자세한 내용은 여기를 참조하십시오.

- **AWS Identity and Access Management(IAM)** – IAM를 통해 사용자의 AWS 서비스와 리소스에 대한 액세스를 안전하게 통제할 수 있습니다. 또한, AWS 사용자 및 그룹을 만들고 관리하며 AWS 리소스에 대한 액세스를 허용 및 거부할 수 있습니다. 자세한 내용은 여기를 참조하십시오.

AWS FedRAMPsm 규정 준수에 대한 자세한 내용은 AWS FedRAMPsm FAQ(https://aws.amazon.com/compliance/fedramp/)를 참조하십시오.

FERPA

가족 교육권 및 개인 정보 보호법(FERPA)(20 U.S.C. § 1232g; 34 CFR Part 99)은 학생 교육 기록 정보를 보호하는 연방법입니다. 이 법은 미국 교육부의 관련 프로그램에 따라 기금 지원을 받는 모든 학교에 적용됩니다. FERPA는 학부모에게 자녀 교육 기록에 대한 특정 권리를 부여합니다. 이러한 권리는 학생이 18세가 되거나 고등학교보다 상위 학교로 진학하면 학생에게 이전됩니다. 권리를 이전받은 학생은 "유자격 학생"입니다.

AWS는 FERPA가 적용되는 단체 및 그 업무 관련자가 보안 AWS 환경을 이용해 보호된 교육 정보를 처리, 유지 관리 및 저장할 수 있도록 합니다.

또한, AWS는 교육 정보의 처리 및 저장을 위해 AWS를 활용할 수 있는 자세한 방법을 알고자 하는 고객에게 FERPA에 초점을 맞춘 백서를 제공합니다.

FERPA Compliance on AWS 백서는 기업이 AWS를 사용하여 FERPA 규정 준수를 촉진하는 시스템을 운영하는 방법을 개략적으로 설명합니다.

FIPS 140-2

Federal Information Processing Standard(FIPS) Publication 140-2는 미국 정부 보안 표준으로서, 기밀 정보를 보호하는 암호 모듈의 보안 요건을 규정하고 있습니다. FIPS 140-2 요구 사항이 적용되는 고객을 지원하기 위해, AWS GovCloud(미국)의 SSL 종료는 FIPS 140-2 검증 하드웨어를 사용하여 작동합니다. AWS는 AWS GovCloud(US) 고객과 협업하여 고객이 AWS GovCloud(US) 환경을 이용할 때 규정 준수를 원활히 관리하는 데 필요한 정보를 제공합니다.

FISMA 및 DIACAP

AWS는 미국 정부 기관에서 FISMA(연방 정보 보안 관리법)를 준수하고 준수 상태를 유지할 수 있도록 지원합니다. AWS 인프라는 소유자 승인 프로세스의 일환으로 독립 평가 기관으로부터 다양한 정부 시스템에 대한 평가를 받았습니다. 많은 연방, 민간 및 국방부(DoD) 조직은 NIST 800-37과 국방부 정보 보증 자격증 및 인가 프로세스(DIACAP)에 정의된 위험 관리 프레임워크(RMF) 프로세스에 따라 AWS 클라우드에서 호스팅되는 시스템에 대한 보안 인증을 획득했습니다.

GxP

GxP는 의약품, 의료 기기 및 의료 소프트웨어 애플리케이션과 같은 식품 및 의료 제품을 제조하는 생명 과학 조직에 적용되는 규제와 지침을 지칭하는 약어입니다. GxP 요구 사항은 소비자를 위해 식품 및 의료 제품의 안전을 보장하고, 제품 관련 안전에 대한 의사 결정에 사용된 데이터의 무결성을 보장하는 하는 것을 전반적인 목적으로 합니다.

AWS는 GxP 시스템에 AWS 클라우드를 사용하는 종합적인 접근 방식이 자세히 나와 있는 GxP 백서를 발행했습니다. 본 백서는 AWS 제품을 GxP 맥락에서 사용하기 위한 지침을 제공하며, 해당 콘텐츠는 AWS 제약 및 의료 기기 고객뿐 아니라 검증된 GxP 시스템에서 현재 AWS 제품을 사용하고 있는 소프트웨어 파트너와 함께 개발하였습니다.

GxP에 대한 자세한 내용은 AWS에서 AWS 영업 및 비즈니스 개발 팀에 문의하십시오.

자세한 내용은 GxP 규정 준수 FAQ(https://aws.amazon.com/compliance/gxp-part-11-annex-11/)를 참조하십시오.

HIPAA

AWS는 미국 건강 보험 이전 및 책임법(HIPAA)의 적용을 받는 기관 및 제휴 기관이 보호 대상 건강 정보를 처리, 유지, 저장하는 데 안전한 AWS 환경을 활용하도록 지원하며 이러한 고객과의 비즈니스 제휴 계약을 체결합니다. 또한, 건강 정보의 처리 및 저장을 위해 AWS를 활용할 수 있는 자세한 방법을 알고자 하는 고객에게 HIPAA에 초점을 맞춘 백서를 제공합니다. Architecting for HIPAA Security and Compliance on Amazon Web Services 백서에는 기업에서 AWS를 이용하여 HIPAA 및 HITECH(Health Information Technology for Economic and Clinical Health) 규정 준수 촉진 시스템을 운영하는 방법이 나와 있습니다.

고객은 HIPAA 계정으로 지정된 계정에서 원하는 AWS 서비스를 사용할 수 있지만, PHI를 처리, 저장 및 전송할 때는 BAA에 정의된 HIPAA 적격 서비스를 사용해야 합니다. 현재 HIPAA 적격 서비스로는 9가지가 있습니다.

- Amazon DynamoDB
- Amazon Elastic Block Store(EBS)
- Amazon Elastic Cloud Compute(EC2)
- Elastic Load Balancing(ELB)
- Amazon Elastic MapReduce(EMR)
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service(Amazon RDS)(MySQL 및 Oracle 엔진만 사용)
- Amazon Simple Storage Service(S3)

AWS는 HIPAA 적격 서비스가 HIPAA에서 요구하는 보안, 제어 및 관리 프로세스를 명확히 지원할 수 있도록 표준 기반의 위험 관리 프로그램을 따릅니다. 이러한 서비스를 사용하여 PHI를 저장 및 처리하면 고객과 AWS 모두 유틸리티 기반 운영 모델에 적용되는 HIPAA 요구 사항을 충족할 수 있습니다. AWS는 고객의 요구에 따라 새로운 적격 서비스의 우선 순위를 정하고 이를 추가합니다.

자세한 내용은 HIPAA 규정 준수 FAQ 및 Architecting for HIPAA Security and Compliance on Amazon Web Services를 참조하십시오.

IRAP

IRAP(정보 보안 공인 평가자 프로그램)은 호주 정부 고객이 적절한 제어를 실시 중인지 검증하고 ASD ISM(호주 신호 관리 위원회 정보 보안 매뉴얼)의 요구 사항을 충족하기 위한 적절한 책임 모델을 결정할 수 있게 해줍니다.

Amazon Web Services는 AWS 시드니 리전에서 미분류 정보(DLM)의 처리, 저장 및 전송과 관련하여 모든 관련 ISM 제어가 실시 중인지 확인하는 외부 평가를 완료했습니다.

자세한 내용은 IRAP 규정 준수 FAQ(https://aws.amazon.com/compliance/irap/) 및 AWS의 ASD(호주 신호 관리 위원회) 클라우드 컴퓨팅 보안 규정 준수를 참조하십시오.

ISO 9001

AWS는 ISO 9001 인증을 획득했으며, AWS의 ISO 9001 인증은 AWS 클라우드에서 품질 관리 IT 시스템을 개발, 마이그레이션 및 운영하는 고객을 직접적으로 지원합니다. 고객은 AWS의 규정 준수 보고서를 자체 ISO 9001 프로그램 및 업계별 품질 프로그램(예: 생명 과학 업계의 GxP, 의료 장비 업계의 ISO 13485, 항공 우주 업계의 AS9100 및 자동차 업계의 ISO/TS 16949)에 대한 근거로 활용할 수 있습니다. 품질 시스템 요구 사항이 없는 AWS 고객도 ISO 9001 인증이 제공하는 추가적인 보증과 투명성으로 인한 혜택을 누릴 수 있습니다.

ISO 9001 인증은 지정된 범위의 AWS 서비스 및 운영 리전(아래 참조)에 대한 품질 관리 시스템과 다음 서비스에 적용됩니다.

- AWS CloudFormation
- AWS Cloud HSM(하드웨어 보안 모듈)
- Amazon CloudFront
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- Amazon DynamoDB

- Amazon EC2 VM Import/Export
- AWS Elastic Beanstalk
- Amazon Elastic Block Store(EBS)
- Amazon Elastic Cloud Compute(EC2)
- Amazon EC2 Container Service(ECS)
- Amazon Elastic File System(EFS)
- Elastic Load Balancing(ELB)
- Amazon Elastic MapReduce(EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management(IAM)
- AWS Key Management Service(KMS)
- Amazon Redshift
- Amazon Relational Database Service(RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service(SES)
- Amazon Simple Queue Service(SQS)
- Amazon Simple Storage Service(S3)
- AWS Storage Gateway
- Amazon Simple Workflow Service(SWF)
- Amazon Virtual Private Cloud(VPC)
- AWS WAF - 웹 애플리케이션 방화벽
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces

- 기반이 되는 물리적 인프라 및 AWS 관리 환경

AWS의 ISO 9001 인증은 미국 동부(버지니아 북부), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), AWS GovCloud(미국), 남아메리카(상파울루), EU(아일랜드), EU(프랑크푸르트), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 아시아 태평양(도쿄) 등의 AWS 리전을 포함합니다.

ISO 9001:2008은 제품 및 서비스 품질 관리에 대한 글로벌 표준입니다. 9001 표준은 국제 표준화 기구(ISO) 기술 위원회에서 정한 품질 관리 및 품질 보증에 대한 8가지 원칙을 기반으로 하는 품질 관리 시스템에 대해 설명합니다. 이 표준에는 다음 항목이 포함됩니다.

- 고객 중심
- 리더십
- 인력 투입
- 프로세스 접근 방식
- 관리에 대한 시스템 접근 방식 도입
- 지속적인 개선
- 정보를 기반으로 한 의사 결정
- 공급업체와 상호 이익이 되는 관계 정립

AWS ISO 9001 인증은 https://d0.awsstatic.com/certifications/iso_9001_certification.pdf에서 다운로드할 수 있습니다.

AWS는 ISO 9001 인증에 대한 추가 정보와 FAQ를 제공합니다. https://aws.amazon.com/compliance/iso-9001-faqs/.

ISO 27001

AWS는 AWS 인프라, 데이터 센터 및 다음 서비스에 적용되는 ISMS(정보 보안 관리 시스템)에 대한 ISO 27001 인증을 획득했습니다.

- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail

- AWS Directory Service
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store(EBS)
- Amazon Elastic Cloud Compute(EC2)
- Amazon EC2 Container Service(ECS)
- AWS Direct Connect
- Amazon EC2 VM Import/Export
- AWS CloudHSM(하드웨어 보안 모듈)
- Elastic Load Balancing(ELB)
- Amazon Elastic File System(EFS)
- Amazon Elastic MapReduce(EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management(IAM)
- AWS Key Management Service(KMS)
- Amazon Redshift
- Amazon Relational Database Service(RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service(SES)
- Amazon Simple Queue Service(SQS)
- Amazon Simple Storage Service(S3)
- Amazon Simple Workflow Service(SWF)
- AWS Storage Gateway
- Amazon Virtual Private Cloud(VPC)

- AWS WAF - 웹 애플리케이션 방화벽
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- 기본 물리적 인프라(GovCloud 포함) 및 AWS 관리 환경

ISO 27001/27002는 일반적으로 널리 적용되는 글로벌 보안 표준으로서, 끊임없이 변화하는 위협 시나리오에 적합한 정기적인 위험 평가를 기반으로 하여 기업 및 고객 정보를 관리하는 체계적인 접근법에 대한 모범 사례 및 요건을 규정합니다. 기업이 인증을 획득하기 위해서는 기업 및 고객 정보의 기밀성, 무결성, 가용성에 영향을 미치는 정보 보안 위험 관리에 대한 체계적이고 지속적인 접근법을 갖추고 있음을 증명해야만 합니다. 보안 관리 및 관행에 대한 중요한 정보를 제공하려는 Amazon의 헌신적인 노력이 이 인증을 통해 한층 강화됩니다.

AWS의 ISO 27001 인증은 미국 동부(버지니아 북부), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), AWS GovCloud(미국), 남아메리카(상파울루), EU(아일랜드), EU(프랑크푸르트), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 아시아 태평양(도쿄) 등의 AWS 리전을 포함합니다.

AWS ISO 27001 인증은 https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf 에서 다운로드할 수 있습니다.

AWS는 ISO 27001 인증에 대한 추가 정보와 FAQ를 제공합니다. https://aws.amazon.com/compliance/iso-27001-faqs/.

ISO 27017

ISO 27017은 국제 표준화 기구(ISO)에서 제정한 최신 실천 강령입니다. 이 강령은 특히 클라우드 서비스와 관련된 정보 보안 제어를 구현하는 지침을 제공합니다.

AWS는 AWS 인프라, 데이터 센터 및 다음 서비스에 적용되는 ISMS(정보 보안 관리 시스템)에 대한 ISO 27017 인증을 획득했습니다.

- Amazon CloudFront

- Amazon DynamoDB
- Amazon EC2 Container Service(ECS)
- Amazon Elastic Block Store(EBS)
- Amazon Elastic Compute Cloud(EC2)
- Amazon Elastic File System(EFS)
- Amazon Elastic MapReduce(EMR)
- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service(RDS)
- Amazon Route 53
- Amazon Simple Email Service(SES)
- Amazon Simple Queue Service(SQS)
- Amazon Simple Storage Service(S3)
- Amazon Simple Workflow Service(SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud(VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk

- AWS Identity and Access Management(IAM)
- AWS Key Management Service(KMS)
- AWS Storage Gateway
- AWS WAF(웹 애플리케이션 방화벽)
- Elastic Load Balancing
- VM 가져오기/내보내기

AWS ISO 27017 인증은 https://do.awsstatic.com/certifications/iso_27017_certification.pdf에서 다운로드할 수 있습니다.

AWS는 https://aws.amazon.com/compliance/iso-27017-faqs/에서 ISO 27001 인증에 대한 추가 정보와 자주 묻는 질문을 제공합니다.

ISO 27018

ISO 27018은 클라우드에서 개인 정보를 보호하는 데 초점을 맞춘 최초의 국제 실천 강령입니다. ISO 정보 보안 표준 27002를 기반으로 하는 이 강력은 퍼블릭 클라우드 개인 식별 정보(PII)에 적용되는 ISO 27002 제어를 구현하는 지침을 제공합니다. 또한 기존의 ISO 27002 제어 집합이 대응하지 못하는 퍼블릭 클라우드 PII 보호 요구 사항을 충족하기 위한 추가 제어 집합 및 관련 지침도 제공합니다.

AWS는 AWS 인프라, 데이터 센터 및 다음 서비스에 적용되는 ISMS(정보 보안 관리 시스템)에 대한 ISO 27018 인증을 획득했습니다.

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service(ECS)
- Amazon Elastic Block Store(EBS)
- Amazon Elastic Compute Cloud(EC2)
- Amazon Elastic File System(EFS)
- Amazon Elastic MapReduce(EMR)

- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service(RDS)
- Amazon Route 53
- Amazon Simple Email Service(SES)
- Amazon Simple Queue Service(SQS)
- Amazon Simple Storage Service(S3)
- Amazon Simple Workflow Service(SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud(VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management(IAM)
- AWS Key Management Service(KMS)
- AWS Storage Gateway
- AWS WAF(웹 애플리케이션 방화벽)
- Elastic Load Balancing
- VM 가져오기/내보내기

AWS ISO 27018 인증은 https://d0.awsstatic.com/certifications/iso_27018_certification.pdf에서 다운로드할 수 있습니다.

AWS는 https://aws.amazon.com/compliance/iso-27018-faqs/에서 ISO 27018 인증에 대한 추가 정보와 자주 묻는 질문을 제공합니다.

ITAR

AWS GovCloud(미국) 리전은 미국 ITAR(미국 국제 무기 거래 규정) 준수를 지원합니다. 포괄적 ITAR 규정 준수 프로그램 관리의 일환으로 ITAR 수출 규정에 구속되는 기업은 보호 대상 데이터에 대한 액세스를 미국 거주민으로 제한하고 해당 데이터의 물리적 위치를 미국 영토로 제한함으로써 의도하지 않은 부적절한 수출을 통제해야 합니다. AWS GovCloud(미국)는 미국에 물리적으로 위치한 환경을 제공하고 그에 대한 액세스를 미국 거주민인 AWS 직원으로 제한하기 때문에 적격 기업만 ITAR에 따라 보호되는 문서와 데이터를 전송, 처리 및 저장할 수 있습니다. 독립적인 제3자의 감사 결과 AWS GovCloud(미국) 환경은 고객 수출 규정 준수 프로그램이 이러한 요건을 충족할 수 있도록 지원하는 적절한 제어 체계를 갖추고 있음을 인증받았습니다.

MPAA

미국 영화 협회(Motion Picture Association of America, MPAA)에서는 보호된 미디어 및 콘텐츠를 안전하게 저장, 처리 및 전송하기 위한 모범 사례를 수립했습니다(http://www.fightfilmtheft.org/facility-security-program.html). 미디어 회사는 위험 요인과 자사의 콘텐츠 및 인프라의 보안을 평가하는 방법으로 이러한 모범 사례를 활용합니다. AWS는 MPAA 모범 사례에 부합됨을 입증했으며 AWS 인프라는 해당되는 모든 MPAA 인프라 컨트롤과 호환됩니다. MPAA에서 "인증"을 제공하지는 않지만 미디어 업계 고객은 AWS MPAA 문서를 사용해 자사의 위험 평가 및 AWS의 MPAA 타입 콘텐츠 평가를 강화할 수 있습니다.

자세한 정보는 AWS 규정 준수 MPAA 허브 페이지(https://aws.amazon.com/compliance/mpaa/)를 참조하십시오.

MTCS 티어 3 인증

MTCS(Multi-Tier Cloud Security)는 싱가포르의 현행 보안 관리 표준(SPRING SS 584:2013)으로, ISO 27001/02 정보 보안 관리 시스템(ISMS) 표준을 기반으로 합니다. 인증 평가를 위해 다음을 수행해야 합니다.

- 회사의 위협 및 취약성에 대한 영향을 고려한 정보 보안 위험을 체계적으로 평가
- 회사 및 아키텍처 보안 위험을 해결할 수 있는 정보 보안 규제 항목 및 기타 위험 관리 형식을 포괄적으로 설계 및 구현
- 정보 보안 규제 항목이 지속적으로 AWS 정보 보안 요구 사항을 충족하도록 포괄적인 관리 프로세스 채택

MTCS 허브 페이지(https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/)를 참조하십시오.

NIST

2015년 6월에 NIST(National Institute of Standards and Technology)는 지침 800-171, "Final Guidelines for Protecting Sensitive Government Information Held by Contractors"를 발표했습니다. 이 지침은 비연방 시스템에서의 CUI(Controlled Unclassified Information) 보호에 적용됩니다.

AWS는 이미 이러한 지침을 준수하고 있으며, 고객은 즉각적으로 NIST 800-171을 효과적으로 준수할 수 있습니다. NIST 800-171은 NIST 800-53 요구 사항의 하위 집합을 규정합니다. AWS는 이미 이 지침에 의거하여 FedRAMP 프로그램으로 감사를 받았습니다. FedRAMP Moderate 보안 제어 기준은 800-171의 Chapter 3에 규정된 권장 요구 사항보다 엄격하며, CUI 데이터를 보호하는 FISMA Moderate 시스템에서 요구되는 것보다 강력한 보안 제어를 다수 포함합니다. 세부 매핑은 NIST Special Publication 800-171에서 확인할 수 있습니다(페이지 D2(PDF 기준 37페이지)부터 시작).

PCI DSS 레벨 1

AWS는 신용카드 업계(PCI)의 데이터 보안 표준(DSS)에 따라 레벨 1 정책을 준수합니다. 고객은 PCI 정책 준수 기술 인프라상에서 애플리케이션을 실행하여 클라우드에서 신용카드 정보를 저장, 처리, 전송할 수 있습니다. 지난 2013년 2월, PCI 보안 표준 위원회에서는 PCI DSS 클라우드 컴퓨팅 가이드라인을 발표했습니다. 이 가이드라인은 카드 소지자 데이터 환경을 관리하는 고객에게 클라우드에서 PCI DSS 규제 항목을 유지하기 위해 고려해야 할 사항을 제공합니다. AWS는 고객을 위해 PCI DSS 클라우드 컴퓨팅 가이드라인을 AWS PCI 규정 준수 패키지에 통합했습니다. AWS PCI 규정 준수 패키지에는 AWS가 PCI DSS 버전 3.1에 대해 레벨 1 서비스 공급업체에 적용되는 표준에 대해 성공적으로 검증받았음을 나타내는 AWS PCI 규정 준수 증명(AoC)과 클라우드에서 AWS와 고객이 함께 져야 할 규정 준수 책임을 설명하는 AWS PCI 책임 요약이 포함됩니다.

다음 서비스는 PCI DSS 레벨 1 범위에 속합니다.

- Auto Scaling
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store(EBS)
- Amazon Elastic Compute Cloud(EC2)
- Elastic Load Balancing(ELB)
- Amazon Elastic MapReduce(EMR)
- Amazon Glacier

- AWS Key Management Service(KMS)
- AWS Identity and Access Management(IAM)
- Amazon Redshift
- Amazon Relational Database Service(RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service(S3)
- Amazon Simple Queue Service(SQS)
- Amazon Simple Workflow Service SWF
- Amazon Virtual Private Cloud(VPC)
- 기본 물리적 인프라(GovCloud 포함) 및 AWS 관리 환경

AWS PCI DSS 레벨 1 인증에 해당하는 최신 서비스 범위와 리전은 https://aws.amazon.com/compliance/pci-dss-level-1-faqs/에 나와 있습니다.

SOC 1/ISAE 3402

Amazon Web Services는 SOC 1(Service Organization Controls 1), Type II 보고서를 발행합니다. 이 보고서에 대한 감사는 미국 공인회계사 협회(AICPA): AT 801(구 SSAE 16) 및 ISAE 3402(International Standards for Assurance Engagements No. 3402)에 따라 이루어집니다. 이러한 이중 표준 보고서는 미국 및 국제 감사 기관의 광범위한 재무 감사 요건을 모두 충족할 수 있도록 고안되었습니다. SOC 1 보고서 감사는 AWS의 제어 목표가 적절하게 설계되어 있고, 고객 데이터를 보호하도록 정의되어 있는 개별 제어 기능들이 효과적으로 작동하고 있다는 점을 증명하고 있습니다. 이 보고서는 SAS 70(Statement on Auditing Standards No. 70) Type II 감사 보고서를 대체합니다.

다음은 AWS SOC 1 제어 목표입니다. 이 보고서는 이러한 각 목표와 독립 감사자가 각 제어 기능에 대해 실시한 테스트 절차의 결과를 뒷받침하는 제어 활동을 식별합니다.

목표 영역	목표 설명
보안 조직	정보 보안 정책이 구현되었고 조직 전체에 전달되었음을 합리적으로 보증하는 규제 항목입니다.
직원 사용자 액세스	Amazon 직원 사용자 계정이 적시에 추가, 수정 및 삭제되고 정기적으로 검토되는 절차가 확립되었음을 합리적으로 보증하는 규제 항목입니다.
논리적 보안	정책 장치가 내부 및 외부 데이터에 대한 무단 액세스를 적절하게 제한하도록 마련되고 고객 데이터에 대한 액세스를 다른 고객과 적절하게 분리함을 합리적으로 보증하는 규제 항목입니다.
안전한 데이터 처리	고객의 시작점과 AWS 스토리지 위치 사이의 데이터 처리가 안전하게 보호되고 정확하게 매핑됨을 합리적으로 보증하는 규제 항목입니다.
물리적 보안 및 환경 보호	데이터 센터에 대한 물리적 액세스가 권한 있는 사람으로 제한되고, 데이터 센터 시설의 오작동 또는 물리적 재해를 최소화하는 장치가 마련되어 있음을 합리적으로 보증하는 규제 항목입니다.
변경 관리	기존 IT 리소스 변경(비상/비정기적 및 구성 변경 포함)이 기록, 인증, 테스트, 승인 및 문서화됨을 합리적으로 보증하는 컨트롤입니다.
데이터 무결성, 가용성 및 중복성	전송, 저장 및 처리를 포함한 모든 단계에서 데이터 무결성이 유지됨을 합리적으로 보증하는 규제 항목입니다.
인시던트 처리	시스템 인스턴스가 기록, 분석 및 해결됨을 합리적으로 보증하는 컨트롤입니다.

SOC 1 보고서는 서비스 조직에서 사용자 엔터티의 재무 제표 감사와 관련된 컨트롤에 집중할 수 있도록 고안되었습니다. AWS의 고객층과 AWS 서비스 사용 범위가 넓기 때문에 고객 재무 제표에 대한 컨트롤의 적용 가능성은 고객에 따라 다릅니다. 따라서 AWS SOC 1 보고서는 광범위한 사용 및 감사 시나리오를 수용할 수 있는 다양한 IT 일반 컨트롤뿐 아니라 재무 감사 시 필요한 특정한 주요 컨트롤도 포함하도록 고안되었습니다. 따라서 고객이 AWS 인프라를 활용하여 재무 보고 프로세스에 반드시 필요한 데이터를 포함한 중요 데이터를 저장하고 처리할 수 있습니다. AWS는 이 중요한 감사 보고서의 고객 피드백과 사용을 파악하기 위해 이러한 컨트롤 선택을 정기적으로 재평가합니다.

AWS는 SOC 1 보고를 위해 꾸준히 노력하고 있으며, 정기 감사 프로세스를 계속 실시해 나갈 것입니다. SOC 1 보고서 범위는 다음과 같습니다.

- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- Amazon Elastic Beanstalk
- Amazon Elastic Block Store(EBS)
- Amazon ElastiCache
- Amazon Elastic Compute Cloud(EC2)
- Amazon ELB(Elastic Load Balancing)
- Amazon Elastic MapReduce(EMR)
- Amazon Glacier
- AWS Identity and Access Management(IAM)

- AWS Key Management Service(KMS)
- Amazon Redshift
- Amazon Relational Database Service(RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Email Service(SES)
- Amazon Simple Storage Service(S3)
- Amazon Simple Workflow(SWF)
- Amazon Simple Queue Service(SQS)
- AWS Storage Gateway
- Amazon Virtual Private Cloud(VPC)
- Amazon WorkSpaces

SOC 2

AWS는 SOC 1 보고서 외에도 Service Organization Controls 2(SOC 2), Type II 보고서를 발행합니다. 컨트롤 평가 면에서 SOC 1과 유사한 SOC 2 보고서는 미국 공인 회계사 협회(AICPA) 트러스트 서비스 원칙에 규정된 기준으로 컨트롤 평가를 확장하는 인증 보고서입니다. 이러한 원칙에는 보안, 가용성, 처리 무결성, 기밀성 및 AWS와 같은 서비스 조직에 적용할 수 있는 개인 정보 보호와 관련된 주요 사례 규제 항목이 정의되어 있습니다. AWS SOC 2는 AICPA의 신뢰 서비스 원칙 기준에 규정된 보안 및 가용성 원칙 기준에 부합하는 제어 기능의 설계 및 운영 효율성 평가입니다. 이 보고서는 미리 정의된 주요 사례의 업계 표준을 기반으로 AWS 보안 및 가용성에 추가적인 투명성을 제공하며 더 나아가 고객 데이터 보호에 대한 AWS의 약속을 보여 줍니다. SOC 2 보고서 범위에는 SOC 1 보고서와 동일한 서비스가 포함됩니다. 위의 총체적인 서비스에 대한 SOC 1 설명을 참조하십시오.

SOC 3

AWS는 Service Organization Controls 3(SOC 3) 보고서를 발행합니다. SOC 3 보고서는 AWS SOC 2 보고서의 공개 요약본입니다. 이 보고서에는 제어 운영에 대한 외부 감사 기관의 의견(SOC 2 보고서에 포함된 AICPA 보안 신뢰 원칙 기준), 제어 효과에 관한 AWS 경영진의 주장, 그리고 AWS 인프라 및 서비스 개요 정보가 수록되어 있습니다. AWS SOC 3 보고서는 총체적인 서비스를 지원하는 전세계의 모든 AWS 데이터 센터를 포함합니다. 이것은 AWS가 SOC 2 보고서의 요청 단계 없이도 외부 감사자의 보장을 받았음을 고객에게 입증하는 명백한 증거입니다. SOC 3 보고서 범위에는 SOC 1 보고서와 동일한 서비스가 포함됩니다. 위의 총체적인 서비스에 대한 SOC 1 설명을 참조하십시오. 여기에서 AWS SOC 3 보고서를 참조하십시오.

참고 문헌

추가 정보는 다음 출처를 참조하십시오.

- AWS 위험 및 규정 준수 개요
- 규정 준수 관련 주요 질문에 대한 AWS의 답변
- CSA 공동 평가 질문서

문서 수정

날짜	설명
2017년 1월	새 템플릿으로 마이그레이션되었습니다.
2016년 1월	첫 게시