Amazon Web Services: 위험 및 규정 준수

2015년 8월

(이 문서의 최신 버전은
http://aws.amazon.com/compliance/aws-whitepapers/

참조)

이 문서는 IT 환경을 지원하는 기존 규제 프레임워크에 AWS를 통합하려는 고객에게 필요한 정보를 제공하기 위해 작성되었습니다. 이 문서에는 AWS의 규제를 평가하는 기본 방식이 포함되어 있으며 고객이 규제 환경을 통합할 수 있도록 지원하는 정보가 제공됩니다. 또한 일반적인 클라우드 컴퓨팅 규정 준수 질문에 대한 AWS 관련 정보를 다룹니다.

목차

위험 및 규정 준수 개요

AWS와 해당 고객은 IT 환경에 대한 규제를 공유하므로 두 당사자 모두 IT 환경을 관리할 책임이 있습니다. 이 공동의 책임에서 AWS가 책임져야 할 부분에는 매우 안전하게 관리되는 플랫폼에서 서비스를 제공하고 고객이 사용할 수 있는 다양한 보안 기능을 지원하는 일이 포함됩니다. 고객의 책임에는 사용 목적에 맞게 안전하고 관리되는 방식으로 IT 환경을 구성하는 일이 포함됩니다. 고객이 IT 환경의 용도와 구성을 AWS에 알리지 않더라도 AWS는 고객과 관련된 보안 및 규제 환경을 알려야 합니다. AWS는 다음과 같은 방법으로 이를 수행합니다.

- 이 문서에 설명된 산업 인증 및 독립적인 외부 기관의 인증 획득
- 백서와 웹 사이트 콘텐츠를 통한 AWS 보안 및 규제 관행에 대한 정보 게시
- NDA에 해당하는 AWS 고객에게 인증서, 보고서 및 기타 문서 직접 제공(필요한 경우)

AWS 보안에 대한 자세한 내용은 AWS 보안 센터를 참조하십시오. AWS 보안 프로세스 개요 백서에서는 AWS의 일반적인 보안 규정 및 서비스별 보안을 다룹니다.

책임 공유 환경

IT 인프라를 AWS 서비스로 이전할 경우 고객과 AWS 간에 책임 공유 모델이 만들어집니다. 이 공유 모델을 통해 고객사는 운영 부담을 덜 수 있습니다. 그 이유는 AWS에서 호스트 운영 체제 및 가상화 계층부터 서비스 운영 시설의 물리적 보안에 이르기까지 구성 요소를 운영, 관리, 규제하기 때문입니다. 고객의 책임 및 관리 범위에는 AWS가 제공하는 보안 그룹 방화벽의 구성과 게스트 운영 체제(업데이트 및 보안 패치 포함) 및 기타 관련 애플리케이션 소프트웨어가 포함됩니다. 사용하는 서비스, 서비스를 IT 환경에 통합하는 과정 및 준거법과 규제에 따라 책임 범위가 다르기 때문에 고객은 선택하고자 하는 서비스에 대해 신중해야 합니다. 고객은 호스트 기반 방화벽, 호스트 기반 침입 탐지/방지, 암호화 및 키 관리와 같은 기술을 활용하여 보안을 강화하고 더 엄격한 규정 준수 요건을 충족할 수 있습니다. 또한 이 책임 공유를 통해 고객은 업종별 인증 요건을 충족하는 솔루션을 배포할 수 있는 유연성과 규제 능력을 보유할 수 있습니다.

이 고객/AWS 책임 공유 모델은 IT 규제에까지 확대 적용됩니다. AWS와 해당 고객 간에 IT 환경 운영 책임을 공유하는 것과 마찬가지로 IT 규제 관리, 운영 및 검증 책임도 공유합니다. AWS는 이전에 고객이 관리했던 AWS 환경에 배포된 물리적 인프라와 관련된 컨트롤을 관리함으로써 고객의 운영 부담을 덜어줄 수 있습니다. 고객마다 AWS에서 구축된 방법이 다르므로 고객은 특정 IT 컨트롤 관리를 AWS로 전환하여 새롭게 배포된 제어 환경을 이용할 수 있습니다. 그런 다음 고객은 제공된 AWS 제어 및 규정 준수 설명서(이 문서의 AWS 인증 및 외부 기관 검증 섹션에 설명)를 참조하여 필요한 제어 평가 및 검증 절차를 실시할 수 있습니다.

다음 섹션은 AWS 고객이 분산된 제어 환경을 효과적으로 평가 및 검증할 수 있는 방법에 대한 접근법을 설명합니다.

강력한 규정 준수 거버넌스

늘 그렇듯이 AWS 고객은 IT 배포 방식에 관계 없이 전체 IT 제어 환경에 대한 적절한 거버넌스를 지속적으로 유지해야 합니다. 이와 관련한 주요 사례에는 필요한 규정 준수 목표 및 요건 이해(관련 소스에서), 그러한 목표와 요건을 충족하는 제어 환경 구성, 조직의 위험 허용 범위에 따라 필요한 검증 이해, 제어 환경의 운영 효과 확인 등이 포함됩니다. AWS 클라우드 기반 배포를 통해 대기업에 다양한 유형의 컨트롤과 다양한 확인 방법을 적용할 수 있는 여러 옵션을 제공할 수 있습니다.

강력한 고객 규정 준수와 거버넌스에는 다음과 같은 기본 접근법이 포함될 수 있습니다.

1. AWS에서 제공하는 정보와 기타 정보를 함께 검토하여 전체 IT 환경을 최대한 이해한 다음 모든 규정 준수 요건을 문서화합니다.
2. 대기업의 규정 준수 요건을 충족하는 제어 목표를 수립하고 구현합니다.
3. 외부 당사자가 소유한 컨트롤을 식별하고 문서화합니다.
4. 모든 제어 목표가 충족되었으며 모든 주요 컨트롤이 효과적으로 설계 및 운영되고 있는지 확인합니다.

이러한 방식으로 규정 준수 거버넌스에 접근할 경우 기업들이 제어 환경을 더 잘 이해하게 되고 수행할 확인 활동을 명확하게 기술할 수 있게 됩니다.

AWS 컨트롤 평가 및 통합

AWS는 백서, 보고서, 인증 및 기타 제3자 증명을 통해, IT 제어 환경에 관한 광범위한 정보를 고객에게 제공합니다. 고객은 이 문서를 통해 사용하는 AWS 서비스에 관련된 컨트롤과 이러한 컨트롤이 검증을 어떻게 거쳤는지 쉽게 이해할 수 있습니다. 또한, 이 정보는 고객이 확장된 IT 환경에서 컨트롤이 효과적으로 작동하고 있는지를 검토하고 검증하는 데에도 도움이 됩니다.

전통적으로 제어 목표와 컨트롤의 설계 및 운영 효과는 내부 및/또는 외부 감사자가 프로세스 검토 및 증거 평가를 통해 검증합니다. 컨트롤을 검증하기 위해서 일반적으로 고객 또는 고객이 지정한 외부 감사자가 직접 관찰/확인을 수행합니다. AWS와 같은 서비스 공급자를 이용할 경우 기업들은 제어 목표와 컨트롤의 설계 및 운영 효과를 합리적으로 보증하기 위해 제3자 증명 및 인증을 요구합니다. 따라서 고객의 주요 컨트롤을 AWS에서 관리할 수 있지만 제어 환경은 모든 컨트롤이 효과적으로 작동하고 있는지를 검토해야 하는 통합된 프레임워크일 수 있습니다. AWS의 제3자 증명 및 인증은 더 수준 높은 제어 환경 검증을 제공할 뿐 아니라, 고객이 AWS 클라우드에서 IT 환경에 대해 직접 특정 검증 작업을 수행해야 하는 부담을 줄여줄 수도 있습니다.

AWS IT 제어 정보

AWS는 다음 두 가지 방법으로 고객에게 IT 제어 정보를 제공합니다.

1. **구체적인 제어 정의.** AWS 고객은 AWS에서 관리하는 주요 컨트롤을 식별할 수 있습니다. 주요 컨트롤은 고객의 제어 환경에 매우 중요하며, 연례 재무 감사와 같은 규정 준수 요건을 준수하기 위해 이러한 주요 컨트롤의 외부 운영 효과 증명이 필요합니다. 이러한 목적으로 AWS는 서비스 조직 규제 1(SOC 1) 유형 II 보고서에 다양하고 구체적인 IT 컨트롤을 게재합니다. SOC 1 보고서(구 SAS(Statement on Auditing Standards) 제70호)라는 서비스 조직 보고서는 미국 공인회계사 협회(AICPA)에서 개발한 감사 표준으로 널리 통용되고 있습니다. SOC 1 감사는 AWS에서 정의한 제어 목표 및 제어 활동(인프라 AWS 관리의 일부에 대한 제어 목표 및 제어 활동 포함)의 설계 및 운영 효과 모두를 심층적으로 감사합니다. "Type II"란 보고서에 설명된 각 컨트롤에 대해 외부 감사자가 설계 정확도 평가를 수행할 뿐 아니라 운영 효과 테스트도 실시한다는 사실을 나타냅니다. AWS에서 지정한 외부 감사자는 독립성과 역량을 갖추고 있으므로 보고서에서 식별된 컨트롤이 AWS의 제어 환경에서 높은 수준의 신뢰성을 제공해야 합니다. AWS의 컨트롤은 사베인-옥슬리법(SOX) 제404조 재무 제표 감사 등 여러 규정 준수 목적에 맞게 효과적으로 설계 및 운영됩니다. SOC 1 Type II 보고서 활용은 일반적으로 다른 외부 인증 기관에서 허용됩니다(예: ISO 27001 감사자가 고객 평가를 완료하기 위해 SOC 1 Type II 보고서를 요구할 수 있음).

그 밖에 특정 제어 활동은 AWS의 신용카드 업계(PCI) 및 연방 정보 보안 관리법(FISMA) 규정 준수와 관련이 있습니다. 아래 설명된 대로 AWS는 FISMA Moderate 표준과 PCI 데이터 보안 표준을 준수합니다. 이러한 PCI 및 FISMA 표준은 상당한 권위가 있으며 AWS가 게재된 표준을 준수하는지 독립적으로 검증합니다.

2. **일반 제어 표준 준수.** AWS 고객이 광범위한 제어 목표 충족을 요구할 경우 AWS의 산업 인증 평가가 수행될 수 있습니다. AWS는 AWS ISO 27001 인증을 통해 다양하고 포괄적인 보안 표준을 준수하고, 안전한 환경 유지 모범 사례를 따릅니다. AWS는 PCI 데이터 보안 표준(PCI DSS)을 통해 신용카드 정보를 취급하는 기업에 중요한 제어 요건을 준수합니다. AWS는 FISMA 표준을 준수함으로써 미국 정부 기관에서 요구하는 다양하고 구체적인 제어 요건을 준수합니다. 이러한 일반 표준을 준수하여 고객에게 규정 준수 관리 시 고려할 수 있는 확립된 컨트롤과 보안 프로세스의 포괄적인 특성에 대한 깊이 있는 정보를 제공합니다.

AWS 보고서, 인증 및 외부 기관 인증은 이 문서의 후반부에서 더 자세히 설명합니다.

AWS 글로벌 리전

데이터 센터는 전 세계 여러 리전에 클러스터 형태로 구축됩니다. 이 문서의 작성일 현재, 미국 동부(버지니아 북부), 미국 서부(오리건), 미국 서부(캘리포니아 북부), AWS GovCloud(미국, 오리건), EU(아일랜드), EU(프랑크푸르트), 아시아 태평양(싱가포르), 아시아 태평양(도쿄), 아시아 태평양(시드니), 남아메리카(상파울루)의 10개 리전이 있습니다.

AWS 위험 및 규정 준수 프로그램

AWS는 고객이 거버넌스 프레임워크에 AWS 컨트롤을 통합할 수 있는 위험 및 규정 준수 프로그램에 대한 정보를 제공합니다. 이 정보는 고객이 프레임워크의 중요한 부분으로 포함된 AWS를 통해 전체 제어 및 거버넌스 프레임워크를 문서화할 수 있도록 지원합니다.

위험 관리

AWS 관리 팀은 위험 식별과 위험을 완화 또는 관리할 수 있는 컨트롤 구현을 포함하는 전략적 비즈니스 계획을 개발했습니다. AWS 관리 팀은 최소한 1년에 두 번 이상 전략적 비즈니스 계획을 재평가합니다. 이 프로세스에서는 관리 팀이 책임 영역 내의 위험을 식별하고 그러한 위험을 해결할 수 있도록 고안된 적절한 대책을 구현해야 합니다.

또한 AWS 제어 환경은 다양한 내부 및 외부 위험 평가를 거칩니다. AWS 규정 준수 및 보안 팀에서는 COBIT(Control Objectives for Information and related Technology) 프레임워크를 토대로 정보 보안 프레임워크 및 정책을 수립하고, ISO 27002 규정과 미국 공인회계사 협회(AICPA) 신뢰 서비스 원칙, PCI DSS v3.1, 미국 국립표준기술연구소(NIST) 간행물 제800-53호 개정 3판(연방 보안 시스템에 대한 권장 보안 조치)에 따라 ISO 27001 인증 프레임워크를 실질적으로 반영했습니다. AWS는 보안 정책을 유지하고, 직원에게 보안 교육을 제공하며, 애플리케이션 보안 검토를 수행합니다. 이러한 검토는 정보 보안 정책에 대한 일치성뿐 아니라 데이터의 기밀성, 무결성 및 가용성도 평가합니다.

AWS 보안 팀은 정기적으로 모든 인터넷 연결 서비스 endpoint IP 주소를 검사하여 취약성이 있는지 확인합니다(이러한 검사에는 고객 인스턴스가 포함되지 않음). AWS 보안 팀은 확인된 취약성을 해결하기 위해 해당 당사자에게 취약성을 알립니다. 또한 독립적인 보안 회사에서 정기적으로 외부 취약성 위협 평가를 수행합니다. 이러한 평가 결과 확인된 내용과 권장사항이 범주화되어 AWS 책임자에게 전달됩니다. 이러한 검사는 기본 AWS 인프라의 상태와 실현가능성을 확인하는 방식으로 수행되며, 특정 규정 준수 요건을 충족하는 데 필요한 고객의 자체 취약성 검사를 대체하기 위한 의도로 제공되지 않습니다. 고객은 검사가 고객의 인스턴스에 국한되고 AWS Acceptable Use Policy를 위반하지 않는 범위에서 클라우드 인프라 검사를 수행할 수 있는 권한을 요청할 수 있습니다. AWS 취약성/침투 테스트 요청 양식을 통해 요청을 제출하여 이러한 유형의 검사에 대한 사전 승인을 얻을 수 있습니다.

제어 환경

AWS는 Amazon의 전체 제어 환경의 다양한 측면을 활용하는 정책, 프로세스 및 제어 활동을 포함하는 포괄적인 제어 환경을 관리합니다. 이 제어 환경은 AWS 서비스 제품군을 안전하게 제공하기 위해 마련되었습니다. 이 집합적인 제어 환경은 AWS 제어 프레임워크의 운영 효과를 지원하는 환경을 구성 및 관리하는 데 필요한 인력, 프로세스 및 기술을 포괄합니다. AWS는 선도적인 클라우드 컴퓨팅 산업 기관에서 확인한 적용 가능한 클라우드 관련 컨트롤을 AWS 제어 프레임워크에 통합했습니다. AWS는 고객이 제어 환경을 관리할 수 있도록 더 효과적으로 지원하는 주요 사례를 구현하기 위해 이러한 산업 그룹을 지속적으로 모니터링합니다.

Amazon의 규제 환경은 회사의 경영진에서부터 시작됩니다. 경영진과 선임 책임자는 회사의 우선 순위와 핵심 가치 형성에 중요한 역할을 합니다. 모든 직원은 회사의 기업 행동강령 및 윤리강령을 제공받고 정기적으로 교육을 받습니다. 준수성 감사는 직원들이 확립된 정책을 이해하고 따르도록 하기 위해 수행됩니다.

AWS 조직 구조는 비즈니스 운영을 계획, 실행 및 규제할 수 있는 프레임워크를 제공합니다. 이 조직 구조는 적절한 인력 구성, 운영 효율성, 업무 분담을 위한 역할과 책임을 할당합니다. 또한 경영진에서는 주요 관계자를 위해 보고 부서와 적절한 보고 라인을 구성했습니다. 기업의 고용 확인 프로세스의 일환으로 직원을 위한 법률 및 규정에서 허용하는 범위 내에서 직원의 직위와 AWS 시설에 대한 접근 권한에 상응하는 교육, 이전 채용 기록, 경우에 따라 배경 조회가 수행됩니다. 기업은 체계적인 온보딩 프로세스에 따라 직원이 Amazon 도구, 프로세스, 시스템, 정책 및 절차를 익힐 수 있도록 돕습니다.

정보 보안

AWS는 고객 시스템 및 데이터의 기밀성, 무결성, 가용성을 보호할 수 있도록 고안된 공식적인 정보 보안 프로그램을 구현했습니다. AWS는 공개 웹 사이트에 AWS에서 고객이 데이터를 안전하게 보호하도록 도울 수 있는 방법을 설명한 보안 백서를 게시합니다.

AWS 보고서, 인증 및 외부 기관 검증

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

FedRAMP SM

AWS는 FedRAMPsm(연방정부의 위험 및 인증 관리 프로그램)를 준수하는 클라우드 서비스 공급자입니다. AWS는 FedRAMPsm 공인 평가대행기관(3PAO: Third Party Assessment Organization)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 개의 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.
- Amazon Elastic Compute Cloud(Amazon EC2). Amazon EC2는 클라우드에서 크기 조정이 가능한 컴퓨팅 파워를 제공하며 개발자가 웹 규모의 컴퓨팅 작업을 보다 쉽게 할 수 있도록 설계되었습니다.
- 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.
- Amazon Virtual Private Cloud(VPC). Amazon VPC를 사용하면 자신이 정의한 가상 네트워크에서 AWS 리소스를 시작할 수 있는 논리적으로 격리된 AWS 섹션을 프로비저닝할 수 있습니다.
- 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.
- AWS Identity and Access Management(IAM). IAM은 사용자의 AWS 서비스와 리소스에 대한 액세스 권한을 안전하게 제어할 수 있게 해 줍니다. 또한, AWS 사용자 및 그룹을 만들고 관리하며 AWS 리소스에 대한 액세스를 허용 및 거부할 수 있습니다.

AWS FedRAMP[sm] 규정 준수에 대한 자세한 내용은 AWS FedRAMP[sm] FAQ를 참조하십시오.

FIPS 140-2

FIPS(Federal Information Processing Standard) 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(미국) 고객과 협력하여 AWS GovCloud(미국) 환경 사용 시 규정 준수를 관리하는 데 도움이 되는 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. 미연방의 수많은 대민 조직과 DoD(국방부) 조직에서 NIST 800-37 및 DIACAP(국방부 정보 보호 인증 및 승인 프로세스)에 정의된 RMF(위험 관리 체계) 프로세스에 따라 AWS 호스팅 시스템에 대한 보안 인증을 받았습니다.

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. Creating HIPAA-Compliant Medical Data Applications with AWS 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 서비스는 Amazon EC2, Amazon EBS, Amazon S3, Amazon Redshift, Amazon Glacier, Amazon Elastic Load Balancer의 여섯 가지가 있습니다.

AWS는 HIPAA 적격 서비스가 HIPAA에서 요구하는 보안, 제어 및 관리 프로세스를 명확히 지원할 수 있도록 하기 위해 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.

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 인증을 통한 보호 및 투명성을 활용할 수 있습니다. ISO 9001 인증은 지정된 범위의 AWS 서비스 및 운영 리전(아래 참조)에 대한 품질 관리 시스템과 다음 서비스에 적용됩니다.

- AWS Cloud Formation
- AWS CloudHSM(하드웨어 보안 모듈)
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- AWS Elastic Beanstalk
- Amazon Elastic Block Store(EBS)
- Amazon Elastic Cloud Compute(EC2)
- Elastic Load Balancing(ELB)
- Amazon Elastic MapReduce(EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management(IAM)
- Amazon Redshift
- Amazon Relational Database Service(RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service(S3)
- AWS Storage Gateway
- Amazon Simple Workflow Service(SWF)
- Amazon Virtual Private Cloud(VPC)
- 기반이 되는 물리적 인프라 및 AWS 관리 환경

AWS의 ISO 9001 인증은 미국 동부(버지니아 북부), 미국 서부(오리건), 미국 서부(캘리포니아 북부), AWS GovCloud(미국), 남아메리카(상파울루), EU(아일랜드), 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

ISO 27001

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

- AWS CloudFormation
- AWS CloudTrail
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store(EBS)
- Amazon Elastic Cloud Compute(EC2)
- AWS Direct Connect
- Amazon EC2 VM Import/Export
- AWS CloudHSM(하드웨어 보안 모듈)
- Elastic Load Balancing(ELB)
- Amazon Elastic MapReduce(EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management(IAM)
- Amazon Redshift
- Amazon Relational Database Service(RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service(S3)
- Amazon Simple Workflow Service(SWF)
- AWS Storage Gateway
- Amazon Virtual Private Cloud(VPC)
- 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 인증에는 전 세계 모든 리전 내 모든 AWS 데이터 센터가 포함되며, AWS는 인증 유지를 위한 공식 프로그램을 구축했습니다. AWS는 웹 사이트에서 ISO 27001 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.

PCI DSS Level 1

AWS는 신용카드 업계(PCI)의 데이터 보안 표준(DSS) 하에서 레벨 1 정책을 준수합니다. 고객은 PCI 정책 준수 기술 인프라 상에서 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.

- AWS Auto Scaling
- AWS CloudFormation
- Amazon Cloudfront
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB(DDB)
- 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(SDB)
- Amazon Simple Storage Service(S3)
- Amazon SQS
- Amazon SWF
- Amazon Virtual Private Cloud(VPC)
- 기본 물리적 인프라(GovCloud 포함) 및 AWS 관리 환경

AWS PCI DSS 레벨 1 인증에 해당하는 최신 서비스 범위는 PCI DSS 레벨 1 FAQ에 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) 전문 표준에 따라 이루어집니다. 이러한 이중 표준 보고서는 미국 및 국제 감사 기관의 광범위한 재무 감사 요건을 모두 충족할 수 있도록 고안되었습니다. SOC 1 보고서는 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.

AWS SOC 1 제어 목표가 여기에 나와 있습니다. 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 리던던시	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)
- Amazon Redshift
- Amazon Relational Database Service(RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service(S3)
- Amazon Simple Workflow(SWF)
- Amazon Simple Queue Service(SQS)
- AWS Storage Gateway
- Amazon Virtual Private Cloud(VPC)

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 SOC 3(Service Organization Controls 3) 보고서를 발표합니다. 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. AWS SOC 3 보고서를 보려면 여기를 이용하십시오.

기타 규정 준수 모범 사례

AWS 플랫폼이 제공하는 유연성과 고객 관리 기능 덕분에 산업별 규정 준수 요건에 부합하는 솔루션 배포가 가능합니다.

- *CSA*: AWS는 CSA(Cloud Security Alliance) 공동 평가 이니셔티브 질문서를 작성했습니다. CSA가 발행한 이 질문서는 AWS의 서비스 지향 인프라에 어떤 보안 컨트롤이 있는지 참조하고 기록하는 데 이용할 수 있습니다. 이 질문서(CAIQ)에는 클라우드 소비자 및 클라우드 감사 기관에서 클라우드 공급자에게 물어야 할 140개 이상의 질문이 담겨 있습니다. AWS가 제작한 CSA 평가 이니셔티브 질문서는 이 문서의 부록 A를 참조하십시오.
- *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. 미국 영화 협회(MPAA) 콘텐츠 보안 모델에 부합하는 AWS는 이 문서의 부록 B를 참조하십시오.

준수 관련 주요 질문 및 AWS

이 섹션에서는 특히 AWS와 관련된 일반적인 클라우드 컴퓨팅 규정 준수 질문을 다룹니다. 이러한 일반적인 규정 준수 질문은 클라우드 컴퓨팅 환경에서 평가 및 운영할 경우에 도움이 될 수 있으며 AWS 고객의 컨트롤 관리 노력을 지원할 수 있습니다.

Ref	클라우드 컴퓨팅 질문	AWS 정보
1	컨트롤 소유권. 클라우드 배포 인프라에 대한 컨트롤의 소유자는 누구입니까?	AWS에 배포된 기술과 관련해서 AWS는 해당 기술의 물리적 구성 요소를 제어합니다. 고객이 연결점 및 전송에 대한 컨트롤을 포함해 기타 모든 컨트롤을 소유하고 제어합니다. AWS는 고객이 AWS가 제공하는 컨트롤과 그러한 컨트롤이 얼마나 효과적으로 작동하는지 더 잘 이해할 수 있도록 돕기 위해, 자세한 물리적 보안 및 환경 컨트롤뿐 아니라 EC2, S3 및 VPC에 대해 정의된 컨트롤도 포함하는 SOC 1 Type II 보고서를 발행합니다. 이러한 컨트롤은 대부분의 고객 요구를 충족해야 하는 높은 수준의 특정성으로 정의됩니다. AWS와 비밀 유지 계약을 체결한 AWS 고객은 SOC 1 Type II 보고서의 사본을 요청할 수 있습니다.
2	IT 감사. 클라우드 공급자 감사는 어떻게 수행할 수 있습니까?	물리적 컨트롤 위에 있는 대부분의 계층 및 컨트롤에 대한 감사는 고객의 책임입니다. AWS에서 정의한 논리적 및 물리적 컨트롤의 정의가 SOC 1 Type II 보고서(SSAE 16)에 문서화되어 있으며, 감사 및 규정 준수 팀이 검토를 진행할 때 이 보고서를 이용할 수 있습니다. AWS ISO 27001과 기타 인증도 감사자가 검토에 이용할 수 있습니다.
3	사베인-옥슬리 규정 준수. 클라우드 공급자 환경에 총체적인 시스템이 배포된 경우 SOX 규정을 어떻게 준수할 수 있습니까?	고객이 AWS 클라우드에 재무 정보를 소유한 경우 고객의 감사자가 사베인-옥슬리(SOX) 요건의 범위에 해당하는 일부 AWS 시스템을 파악할 수 있습니다. 고객의 감사자가 SOX 적용 가능성을 독자적으로 판단해야 합니다. 대부분의 논리적 액세스 제어는 고객이 관리하므로, 고객은 제어 활동이 관련 표준을 충족하는지 파악할 수 있는 가장 좋은 조건을 갖추고 있습니다. SOX 감사자가 해당 AWS 물리적 컨트롤을 요청할 경우 AWS가 제공하는 컨트롤을 자세히 설명하는 AWS SOC 1 Type II 보고서를 참조할 수 있습니다.
4	HIPAA 규정 준수. 클라우드 공급자 환경에 배포할 경우 HIPAA 규정 준수 요건을 충족할 수 있습니까?	HIPAA 요건이 적용되며 AWS 고객이 이를 관리합니다. AWS 플랫폼을 통해 HIPAA와 같은 산업 관련 인증 요건을 충족하는 솔루션을 배포할 수 있습니다. 고객은 AWS 서비스를 이용해 전자 건강 기록을 보호하는 데 필요한 수준과 동일하거나 그보다 높은 보안 수준을 유지할 수 있습니다. 고객은 AWS에서 HIPPA의 보안 및 개인 정보 보호 규정을 준수하는 건강 관리 애플리케이션을 구축해 왔습니다. AWS는 웹 사이트에서 HIPAA 규정 준수에 대한 백서를 포함해 이 주제에 대한 추가 정보를 제공합니다.
5	GLBA 규정 준수. 클라우드 공급자 환경에 배포할 경우 GLBA 규정 준수 요건을 충족할 수 있습니까?	대부분의 GLBA 요건은 AWS 고객이 관리합니다. AWS는 고객에게 데이터를 보호하고, 권한을 관리하며, AWS 인프라에 GLBA 준수 애플리케이션을 구축할 수 있는 수단을 제공합니다. 고객에게 물리적 보안 컨트롤이 효과적으로 작동한다는 특정 보증이 필요한 경우 AWS SOC 1 Type II 보고서에서 관련 내용을 참조할 수 있습니다.

Ref	클라우드 컴퓨팅 질문	AWS 정보
6	연방 규정 준수. 클라우드 공급자 환경에 배포할 경우 미국 정부 기관이 보안 및 개인 정보 보호 규정을 준수할 수 있습니까?	미연방 기관에는 2002년 FISMA(연방 정보 보안 관리법), FedRAMPsm(연방정부의 위험 및 인증 관리 프로그램), FIPS(연방 정보 처리 표준) 간행물 제140-2호, ITAR(국제 무기 거래 규정) 등 다양한 규정 준수 표준이 적용될 수 있습니다. 적용 가능한 법률에 명시된 요건에 따라 기타 법률 및 규정도 준수할 수 있습니다.
7	데이터 위치. 고객 데이터는 어디에 상주합니까?	AWS 고객은 데이터와 서버가 위치할 물리적 리전을 지정할 수 있습니다. 데이터가 저장되는 리전 클러스터 내에서 S3 데이터 객체에 대한 데이터 복제가 이루어지지만 다른 리전에 있는 다른 데이터 센터 클러스터에는 복제되지 않습니다. AWS 고객은 데이터와 서버가 위치할 물리적 리전을 지정할 수 있습니다. AWS는 법률 또는 정부기관의 요청을 준수해야 하는 경우가 아닌 이상, 통지 없이 고객이 선택한 리전에서 고객의 콘텐츠를 옮기지 않습니다. 이 문서의 작성일 현재, 미국 동부(버지니아 북부), 미국 서부(오리건), 미국 서부(캘리포니아 북부), AWS GovCloud(미국, 오리건), EU(아일랜드), EU(프랑크푸르트), 아시아 태평양(싱가포르), 아시아 태평양(도쿄), 아시아 태평양(시드니), 남아메리카(상파울루)의 10개 리전이 있습니다.
8	전자증거개시(E-Discovery). 클라우드 공급자가 전자증거개시 절차 및 요건 충족에 대한 고객의 요구를 충족합니까?	AWS는 인프라를 제공하고, 고객은 운영 체제, 네트워크 구성, 설치된 애플리케이션을 포함한 그 밖의 모든 구성 요소를 관리합니다. 고객은 AWS를 사용해 보관하거나 처리하는 전자 문서의 식별, 수집, 처리, 분석 및 작성을 포함하는 소송 절차에 적절하게 대응할 책임이 있습니다. 요청 시 AWS는 소송 절차에서 AWS의 지원이 필요한 고객과 협력할 수 있습니다.
9	데이터 센터 둘러보기. 클라우드 공급자가 고객이 데이터 센터를 둘러볼 수 있도록 허용합니까?	아닙니다. AWS 데이터 센터에서는 다양한 고객을 호스팅하기 때문에 고객의 데이터 센터 관람을 허용하지 않습니다. 불특정 다수의 고객이 타사 데이터에 물리적으로 접근할 우려가 있기 때문입니다. 이러한 고객의 요구를 충족하기 위해 독립적이고 역량 있는 감사자가 SOC 1 Type II 보고서의 일부로 규제 항목의 현재 상태와 운영을 검증합니다. 널리 사용되는 이 제3자 검증을 통해 고객은 배포된 컨트롤의 효과를 독립적인 관점으로 바라볼 수 있습니다. AWS와 비밀 유지 계약을 체결한 AWS 고객은 SOC 1 Type II 보고서의 사본을 요청할 수 있습니다. 데이터 센터의 물리적 보안에 대한 개별 평가는 ISO 27001 감사, PCI 평가, ITAR 감사 및 FedRAMPsm 테스트 프로그램에도 포함되어 있습니다.
10	타사 액세스. 제3자가 클라우드 공급자 데이터 센터에 액세스할 수 있습니까?	AWS는 내부 직원일지라도 데이터 센터에 대한 액세스를 엄격하게 관리합니다. AWS 액세스 정책에 따라 해당 AWS 데이터 센터 관리자가 명시적으로 승인한 경우를 제외하고는 제3자는 AWS 데이터 센터에 접근할 수 없습니다. 물리적 접근과 관련된 특정 통제 수단, 데이터 센터 접근 권한 부여 및 기타 관련 통제 수단에 대한 자세한 내용은 SOC 1 Type II 보고서를 참조하십시오.
11	권한 있는 작업. 권한 있는 작업이 모니터링 및 제어됩니까?	배포된 컨트롤이 시스템 및 데이터에 대한 액세스를 제한하고 시스템 또는 데이터에 대한 액세스를 제한 및 모니터링합니다. 또한 고객 데이터와 서버 인스턴스가 기본적으로 다른 고객과 논리적으로 격리됩니다. AWS SOC 1, ISO 27001, PCI, ITAR 및 FedRAMPsm 감사 중 독립적 감사 기관으로부터 권한 사용자 액세스 제어를 검토 받습니다.

Ref	클라우드 컴퓨팅 질문	AWS 정보
12	내부자 액세스. 클라우드 공급자가 고객 데이터 및 애플리케이션에 대한 부적절한 내부자 액세스 위협을 해결합니까?	AWS는 부적절한 내부자 액세스 위협을 해결하는 특정 SOC 1 컨트롤을 제공하며, 이 문서에 포함된 공개 인증 및 규정 준수 프로그램이 내부자 액세스를 해결합니다. 모든 인증 및 제3자 증명은 논리적 액세스와 관련한 사전적 및 사후적 컨트롤을 평가합니다. 또한 정기적인 위험 평가를 통해 내부자 액세스가 어떻게 제어 및 모니터링되고 있는지 집중적으로 검토합니다.
13	다중 테넌트. 고객 분리가 안전하게 구현되었습니까?	AWS 환경은 가상화된 다중 테넌트 환경입니다. AWS는 보안 관리 프로세스, PCI 컨트롤, 각 고객을 다른 고객과 격리할 수 있도록 고안된 기타 보안 컨트롤을 구현했습니다. AWS 시스템은 고객이 가상화 소프트웨어를 통한 필터링으로 자신에게 할당되지 않은 물리적 호스트 또는 인스턴스에 액세스하는 것을 차단할 수 있도록 설계되었습니다. 이 아키텍처는 독립적인 PCI QSA(Qualified Security Assessor)의 검증을 받았으며 2015년 4월에 발표된 PCI DSS 버전 3.1의 모든 요구 사항을 준수하는 것으로 확인되었습니다. AWS는 단일 테넌시 옵션도 제공합니다. 전용 인스턴스는 단일 고객에게 배정된 하드웨어를 실행하는 Amazon Virtual Private Cloud(Amazon VPC) 내에서 시작되는 Amazon EC2 인스턴스입니다. 전용 인스턴스를 통해 Amazon VPC와 AWS 클라우드의 이점을 최대한 활용하는 동시에 Amazon EC2 컴퓨터 인스턴스를 하드웨어 수준에서 격리할 수 있습니다.
14	하이퍼바이저 취약성. 클라우드 공급자가 알려진 하이퍼바이저 취약성을 해결했습니까?	Amazon EC2는 현재 고도로 맞춤화된 Xen 하이퍼바이저를 사용합니다. 하이퍼바이저는 내부 및 외부 침투 팀에서 정기적인 평가를 통해 새로운 취약성 및 기존 취약성이 있는지 확인하며, 게스트 가상 머신 사이에서 강력한 격리를 유지하는 데 매우 적합합니다. AWS Xen 하이퍼바이저 보안은 평가 및 감사 도중 독립 감사자가 정기적으로 평가합니다. Xen 하이퍼바이저와 인스턴스 격리에 대한 자세한 내용은 AWS 보안 백서를 참조하십시오.
15	취약성 관리. 시스템에 적절하게 패치가 적용되었습니까?	AWS는 하이퍼바이저 및 네트워크 서비스 등 고객에 대한 서비스 제공을 지원하는 시스템에 패치를 적용할 책임이 있습니다. 패치 적용은 AWS 정책과 ISO 27001, NIST, PCI 요건에 따라 수행됩니다. 고객은 게스트 운영 체제, 소프트웨어 및 애플리케이션을 관리하므로 자체 시스템에 패치를 적용할 책임이 있습니다.
16	암호화. 제공되는 서비스가 암호화를 지원합니까?	예. AWS는 고객이 S3, EBS, SimpleDB, EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있도록 지원합니다. VPC에 대한 IPSec 터널도 암호화됩니다. Amazon S3도 고객을 위한 옵션으로 Server Side Encryption을 제공합니다. 고객은 제3자 암호화 기술을 사용할 수도 있습니다. 자세한 내용은 AWS 보안 백서를 참조하십시오.
17	데이터 소유권. 클라우드 공급자는 고객 데이터에 대해 어떤 권한을 보유합니까?	AWS 고객은 데이터에 대한 관리 및 소유권을 보유합니다. AWS는 고객의 개인 정보를 보호하기 위해 만전을 기하며 준수해야 하는 법 집행 기관의 요청을 꼼꼼하게 파악합니다. AWS는 법 집행 기관의 명령이 확실한 근거가 없다고 판단할 경우 그러한 명령에 적극적으로 이의를 제기합니다.
18	데이터 격리. 클라우드 공급자가 고객 데이터를 적절하게 격리합니까?	고객을 대신해 AWS에 저장된 모든 데이터는 강력한 테넌트 격리 보안 및 제어 기능을 갖고 있습니다. Amazon S3는 고급 데이터 액세스 제어를 제공합니다. 특정 데이터 서비스 보안에 대한 자세한 내용은 AWS 보안 백서를 참조하십시오.

Ref	클라우드 컴퓨팅 질문	AWS 정보
19	조합 서비스. 클라우드 공급자가 자체 서비스와 다른 공급자의 클라우드 서비스를 함께 제공합니까?	AWS는 고객에게 AWS 서비스를 제공하기 위해 제3자 클라우드 공급자를 활용하지 않습니다.
20	물리적 및 환경 컨트롤. 이러한 컨트롤은 지정된 클라우드 공급자가 운영합니까?	예. SOC 1 Type II 보고서에 자세하게 설명되어 있습니다. 또한 ISO 27001 및 FedRAMPsm 등 AWS가 지원하는 그 밖의 인증에서도 물리적/환경적 제어의 모범 사례를 요구합니다.
21	클라이언트 측 보호. 클라우드 공급자가 고객이 PC 및 모바일 디바이스와 같은 클라이언트에서 액세스를 보호하고 관리할 수 있도록 허용합니까?	예. AWS는 고객이 자체 요건에 따라 클라이언트 및 모바일 애플리케이션을 관리할 수 있도록 허용합니다.
22	서버 보안. 클라우드 공급자가 고객이 가상 서버를 보호할 수 있도록 허용합니까?	예. AWS는 고객이 자체 보안 아키텍처를 구현할 수 있도록 허용합니다. 서버 및 네트워크 보안에 대한 자세한 내용은 AWS 보안 백서를 참조하십시오.
23	자격 증명 및 액세스 관리. 이 서비스에 IAM 기능이 포함되어 있습니까?	AWS는 고객이 사용자 ID를 관리하고, 보안 자격 증명을 할당하고, 사용자를 그룹화하며, 중앙 집중식으로 사용자 권한을 관리할 수 있는 ID 및 액세스 관리 제품군을 보유하고 있습니다. 자세한 내용은 AWS 웹 사이트를 참조하십시오.
24	예약 유지보수를 위한 중단. 공급자가 유지보수를 위해 시스템을 중단할 시기를 지정합니까?	AWS 고객은 정기 유지보수 및 시스템 패치 적용을 위해 시스템을 오프라인으로 전환하지 않아도 됩니다. AWS의 자체 유지보수 및 시스템 패치 적용은 일반적으로 고객에게 영향을 미치지 않습니다. 인스턴스 유지보수는 고객이 관리합니다.
25	확장 기능. 공급자가 고객이 원래 계약 이상으로 확장할 수 있도록 허용합니까?	AWS 클라우드는 매우 안전하고 복원력이 뛰어난 분산형 시스템으로, 고객에게 대규모 확장 역량을 제공합니다. 고객은 시스템을 수직 또는 수평으로 확장할 수 있으며 사용한 용량에 대해서만 비용을 지불합니다.
26	서비스 가용성. 공급자가 높은 수준의 가용성을 제공하기 위해 노력합니까?	AWS는 서비스 수준 협약(SLA)을 통해 높은 수준의 가용성을 제공하기 위해 노력합니다. 예를 들어, Amazon EC2는 서비스 기간 동안 연간 최소 99.95% 이상의 가동률을 제공합니다. Amazon S3는 매달 최소한 99.9% 이상의 가동률을 제공합니다. 이러한 가용성 측정치가 충족되지 않을 경우 서비스 크레딧이 제공됩니다.
27	DDoS(분산 서비스 거부) 공격. 공급자가 DDoS 공격으로부터 서비스를 어떻게 보호합니까?	AWS 네트워크는 기존의 네트워크 보안 문제와 관련하여 중요한 보호 방법을 제공합니다. 고객은 추가 보호 방법을 실행할 수도 있습니다. DDoS 공격 논의를 포함한 이 주제에 대한 자세한 내용은 AWS 보안 백서를 참조하십시오.
28	데이터 이동성. 고객이 요청할 경우 서비스 공급자가 저장한 데이터를 내보낼 수 있습니까?	AWS는 고객이 필요에 따라 AWS 스토리지에서 데이터를 가져오거나 내보낼 수 있도록 허용합니다. S3의 AWS Import/Export 서비스는 데이터 전송 시 이동식 스토리지 디바이스를 사용하여 AWS에서 많은 양의 데이터를 빠르게 송수신할 수 있습니다.

Ref	클라우드 컴퓨팅 질문	AWS 정보
29	서비스 공급자 비즈니스 연속성. 서비스 공급자가 비즈니스 연속성 프로그램을 운영합니까?	AWS는 비즈니스 연속성 프로그램을 운영합니다. 자세한 내용이 AWS 보안 백서에 나와 있습니다.
30	고객 비즈니스 연속성. 서비스 공급자가 고객이 비즈니스 연속성 계획을 구현할 수 있도록	AWS는 고객에게 빈번한 서버 인스턴스 백업 활용, 데이터 중복 복제, 다중 리전/가용 영역 배포 아키텍처를 포함한 강력한 연속성 계획을 구현할 수 있는 기능을 제공합니다.
31	데이터 내구성. 서비스 공급자가 데이터 내구성을 지정합니까?	Amazon S3는 내구성이 뛰어난 스토리지 인프라를 제공합니다. 객체는 Amazon S3 리전에서 여러 시설의 다양한 디바이스에 중복 저장됩니다. 데이터가 저장되면 Amazon S3가 손실된 중복성을 빠르게 검색 및 복원하여 객체의 내구성을 유지합니다. 또한 Amazon S3는 체크섬을 사용해 저장된 데이터의 무결성을 정기적으로 검사합니다. 손상이 감지된 경우 중복 데이터를 사용하여 복원합니다. S3에 저장된 데이터는 연간 99.999999999%의 내구성과 99.99%의 객체 가용성을 제공하도록 설계되었습니다.
32	백업. 서비스 공급자가 테이프에 백업합니까?	AWS는 고객이 자체 테이프 백업 서비스 공급자를 사용해 테이프에 백업할 수 있도록 허용합니다. 그러나 AWS에서는 테이프 백업 서비스를 제공하지 않습니다. Amazon S3 서비스는 데이터 스토리지 중복성을 통해 데이터 손실 가능성을 거의 0%로 낮추고 데이터 객체의 다중 사이트 사본과 동일한 내구성을 보장할 수 있도록 고안되었습니다. 데이터 내구성 및 중복성에 대한 정보는 AWS 웹 사이트를 참조하십시오.
33	가격 증가. 서비스 공급자가 예기치 않게 가격을 올립니까?	AWS는 시간이 지남에 따라 이러한 서비스를 제공하는 비용이 감소함에 따라 비용을 낮춘 사례가 자주 있습니다. AWS는 지난 몇 년간 지속적으로 가격을 낮춰 왔습니다.
34	지속가능성. 서비스 공급자가 장기적인 지속가능성 잠재력을 보유하고 있습니까?	AWS는 선도적인 클라우드 공급자로, Amazon.com의 장기적인 비즈니스 전략입니다. AWS는 매우 장기적인 지속가능성 잠재력을 보유하고 있습니다.

AWS 연락처

고객은 AWS 영업 및 비즈니스 개발 팀에 연락하여 외부 감사 기관에서 작성한 보고서 및 인증 내역을 요청하거나 AWS 규정 준수에 대한 자세한 정보를 요청할 수 있습니다. 담당자가 문의 유형에 따라 고객을 적절한 팀으로 연결해 줍니다. AWS 규정 준수에 대한 자세한 내용은 AWS 규정 준수 사이트를 참조하거나, awscompliance@amazon.com으로 직접 문의해 주십시오.

부록 A: CSA 공동 평가 이니셔티브 질문서 v1.1

CSA(Cloud Security Alliance)는 "클라우드 컴퓨팅의 보안 보장을 위한 모범 사례 적용을 장려하고, 다른 모든 컴퓨팅 방식에서 클라우드 컴퓨팅을 이용하여 보안을 강화하는 방법을 교육하는 비영리 조직"입니다(https://cloudsecurityalliance.org/about/ 참조). 광범위한 업계 보안 실무자, 기업 및 협회 등이 이 조직의 목표 달성을 위해 활동하고 있습니다.

CSA 평가 질문서는 CSA에서 클라우드 소비자 및/또는 클라우드 감사자가 클라우드 공급자에게 문의할 것이라고 예상하는 질문 세트를 제공합니다. 이 질문서는 클라우드 공급자 선정 및 보안 평가 등 다양한 용도에 사용할 수 있는 일련의 보안, 제어 및 프로세스 질문을 제공합니다. AWS는 아래 답변으로 이 질문서를 작성했습니다.

도메인	제어 그룹	CID	평가 질문	AWS 답변
규정 준수	감사 계획	CO-01.1	업계에서 인정하는 체계적인 형식(예: CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA의 Cloud Computing Management Audit/Assurance Program 등)을 사용하여 감사 보고서를 작성합니까?	AWS는 특정 산업 인증과 독립적인 외부 기관 인증을 획득하고, NDA에 의거해 AWS 고객에게 특정 인증, 보고서 및 기타 관련 문서를 직접 제공합니다.
규정 준수	독립 감사	CO-02.1	테넌트가 SAS70 Type II/ SOC2 16 ISAE3402/ISAE3402 또는 이와 유사한 제3자 감사 보고서를 볼 수 있도록 허용합니까?	AWS는 NDA에 의거하여 제3자 증명, 인증, Service Organization Controls 1(SOC 1) Type II 보고서 및 기타 관련 규정 준수 보고서를 고객에게 직접 제공합니다. AWS 보안 팀은 정기적으로 모든 인터넷 연결 서비스 endpoint IP 주소를 검사하여 취약성이 있는지 확인합니다(이러한 검사에는 고객 인스턴스가 포함되지 않음). AWS 보안 팀은 확인된 취약성을 해결하기 위해 해당 당사자에게 취약성을 알립니다. 또한 독립적인 보안 회사에서 정기적으로 외부 취약성 위협 평가를 수행합니다. 이러한 평가 결과 확인된 내용과 권장사항이 범주화되어 AWS 책임자에게 전달됩니다. 또한 AWS 제어 환경은 정기적인 내부 및 외부 위험 평가를 거칩니다. AWS는 외부 인증 기관 및 독립 감사자와 협력하여 AWS 전체 제어 환경을 검토하고 테스트합니다.
규정 준수		CO-02.2	산업 모범 사례 및 지침에 규정된 대로 정기적으로 클라우드 서비스 인프라에 대해 네트워크 침투 테스트를 수행합니까?	
규정 준수		CO-02.3	산업 모범 사례 및 지침에 규정된 대로 정기적으로 클라우드 인프라에 대해 애플리케이션 침투 테스트를 수행합니까?	
규정 준수		CO-02.4	산업 모범 사례 및 지침에 규정된 대로 정기적으로 내부 감사를 실시합니까?	
규정 준수		CO-02.5	산업 모범 사례 및 지침에 규정된 대로 정기적으로 외부 감사를 실시합니까?	
규정 준수		CO-02.6	테넌트가 요청할 경우 네트워크 침투 테스트 결과를 제공합니까?	
규정 준수		CO-02.7	테넌트가 요청할 경우 내부 및 외부 감사 결과를 제공합니까?	
규정 준수	외부 기관 감사	CO-03.1	테넌트가 독립적인 취약성 평가를 수행할 수 있도록 허용합니까?	고객은 검사가 고객의 인스턴스에 국한되고 AWS Acceptable Use Policy를 위반하지 않는범위에서 클라우드 인프라 검사를 수행할 수 있는 권한을 요청할 수 있습니다 AWS 취약성/침투 테스트 요청 양식을 통해 요청을 제출하여 이러한 유형의 검사에 대한 사전 승인을 얻을 수 있습니다.

도메인	제어 그룹	CID	평가 질문	AWS 답변
규정 준수		CO-03.2	외부의 제3자가 애플리케이션 및 네트워크에 대한 취약성 검사와 정기적인 침투 테스트를 수행합니까?	AWS 보안 팀은 정기적으로 독립적인 보안 회사와 협력하여 외부 취약성 위협 평가를 수행합니다. AWS SOC 1 Type II 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다.
규정 준수	연락처 /기관 관리	CO-04.1	계약 및 해당 규정에 따라 현지 당국과 연락 및 연락 지점을 유지하고 있습니까?	AWS는 ISO 27001 표준에서 요구하는 대로 산업 기관, 위험 및 규정 준수 조직, 현지 당국, 규제 기관과의 연락을 유지하고 있습니다.
규정 준수	정보 시스템 규제 매핑	CO-05.1	실수로 다른 테넌트의 데이터에 액세스하지 않고 단일 테넌트에 대해서만 데이터가 생성될 수 있도록 고객 데이터를 논리적으로 조각화 또는 암호화할 수 있습니까?	고객을 대신해 AWS에 저장된 모든 데이터는 강력한 테넌트 격리 보안 및 제어 기능을 갖고 있습니다. 고객은 데이터에 대한 관리 및 소유권을 보유하므로 데이터 암호화 선택은 고객의 책임입니다. AWS는 고객이 S3, EBS, SimpleDB, EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있도록 지원합니다. VPC에 대한 IPSec 터널도 암호화됩니다. Amazon S3도 고객을 위한 옵션으로 Server Side Encryption을 제공합니다. 자세한 내용은 AWS 위험 및 규정 준수 백서 http://aws.amazon.com/security를 참조하십시오.
		CO-05.2	장애 발생 또는 데이터 손실 시 특정 고객의 데이터를 논리적으로 조각화하고 복구할 수 있습니까?	
규정 준수	지적 재산	CO-06.1	테넌트의 지적 재산을 보호하기 위해 마련된 컨트롤을 설명하는 정책과 절차가 있습니까?	AWS 규정 준수 및 보안 팀은 COBIT(Control Objectives for Information and related Technology) 프레임워크를 기반으로 정보 보안 프레임워크 및 정책을 구축했습니다. AWS 보안 프레임워크는 ISO 27002 모범 사례와 PCI 데이터 보안 표준을 통합합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 위험 및 규정 준수 백서를 참조하십시오.
규정 준수	지적 재산	CO-07.1	클라우드 공급자의 이익을 위해 클라우드에 있는 테넌트 서비스의 사용률을 모니터링할 경우 테넌트 IP 권리가 보호됩니까?	AWS에서는 서비스의 가용성을 효과적으로 관리하기 위해 필요에 따라 리소스 사용률을 모니터링합니다. AWS는 리소스 사용률 모니터링 과정에서 고객의 지적 재산을 수집하지 않습니다.
규정 준수	지적 재산	CO-08.1	클라우드 공급자의 이익을 위해 클라우드에 있는 테넌트 서비스의 사용률을 모니터링할 경우 테넌트에게 옵트아웃 기능을 제공합니까?	클라우드에 있는 고객 서비스 사용률은 모니터링되지 않습니다.
데이터 거버넌스	소유권/관리 의무	DG-01.1	체계적인 데이터 레이블 지정 표준(예: ISO 15489, Oasis XML 카탈로그 사양, CSA 데이터 형식 지침)을 따릅니까?	AWS 고객은 데이터에 대한 관리 및 소유권을 보유하며 각자의 요건에 부합하는 체계적인 데이터 레이블 지정 표준을 구현할 수 있습니다.

도메인	제어 그룹	CID	평가 질문	AWS 답변
데이터 거버넌스	분류	DG-02.1	정책 태그/메타데이터(예: 태그는 잘못된 국가 등에서 게스트 운영 체제의 부팅/설치/데이터 전송을 제한하는 데 사용될 수 있음)를 통해 가상 머신을 식별할 수 있는 기능을 제공합니까?	가상 머신은 EC2 서비스의 일환으로 고객에게 할당됩니다. 고객은 사용되는 데이터와 리소스가 상주하는 위치를 제어할 수 있는 권한이 있습니다. 자세한 내용은 AWS 웹 사이트(http://aws.amazon.com)를 참조하십시오.
데이터 거버넌스		DG-02.2	정책 태그/메타데이터/하드웨어 태그(예: TXT/TPM, VN-Tag 등)를 통해 하드웨어를 식별할 수 있는 기능을 제공합니까?	AWS는 EC2 리소스에 태그를 지정할 수 있는 기능을 제공합니다. 메타데이터 형태의 EC2 태그를 사용해 사용자 친화적인 이름을 만들고, 검색 능력을 강화하며, 여러 사용자 간의 조정을 개선할 수 있습니다. AWS Management Console도 태그 지정을 지원합니다.
데이터 거버넌스		DG-02.3	시스템의 지리적 위치를 인증 요소로 사용할 수 있습니까?	AWS는 IP 주소를 기반으로 조건부 사용자 액세스 기능을 제공합니다. 고객이 시간, 원본 IP 주소 또는 SSL 사용 여부 등 사용자가 AWS를 사용할 수 있는 방식을 제어하는 조건을 추가할 수 있습니다.
데이터 거버넌스		DG-02.4	요청 시 테넌트의 데이터가 보관된 스토리지의 물리적 위치/지역을 제공할 수 있습니까?	AWS는 지리적으로 분산되어 있는 여러 리전에 인스턴스를 배치하고 데이터를 저장할 수 있는 유연성을 제공합니다. AWS 고객은 데이터와 서버가 위치할 물리적 리전을 지정할 수 있습니다. AWS는 법률 또는 정부기관의 요청을 준수해야 하는 경우가 아닌 이상, 통지 없이 고객이 선택한 리전에서 고객의 콘텐츠를 옮기지 않습니다. 이 문서의 작성일 현재, 미국 동부(버지니아 북부), 미국 서부(오리건), 미국 서부(캘리포니아 북부), AWS GovCloud(미국, 오리건), EU(아일랜드), EU(프랑크푸르트), 아시아 태평양(싱가포르), 아시아 태평양(도쿄), 아시아 태평양(시드니), 남아메리카(상파울루)의 10개 리전이 있습니다.
데이터 거버넌스		DG-02.5	테넌트가 데이터 라우팅 및 리소스 인스턴스화를 위해 허용 가능한 지리적 위치를 정의할 수 있습니까?	
데이터 거버넌스	취급/레이블 지정/보안 정책	DG-03.1	데이터와 데이터를 포함하는 객체의 레이블 지정, 취급 및 보안에 대한 정책 및 절차가 마련되어 있습니까?	AWS 고객은 데이터에 대한 관리 및 소유권을 보유하며 각자의 요건에 부합하는 레이블 지정 및 취급 정책과 절차를 구현할 수 있습니다.
데이터 거버넌스		DG-03.2	데이터 통합 컨테이너 역할을 하는 객체에 대한 레이블 상속 메커니즘이 구현되어 있습니까?	
데이터 거버넌스	보존 정책	DG-04.1	테넌트 데이터 보존 정책을 강화할 수 있는 기술적 제어 기능이 있습니까?	AWS는 고객에게 데이터를 삭제할 수 있는 기능을 제공합니다. 그러나 AWS 고객은 데이터에 대한 관리 및 소유권을 보유하므로 각자의 요건에 따라 데이터를 관리하는 것은고객의 책임입니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.

도메인	제어 그룹	CID	평가 질문	AWS 답변
데이터 거버넌스		DG-04.2	정부 또는 제3자의 테넌트 데이터 요청에 대응할 수 있는 문서화된 절차가 있습니까?	AWS는 고객의 개인 정보를 보호하기 위해 만전을 기하며 준수해야 하는 법 집행 기관의 요청을 꼼꼼하게 파악합니다. AWS는 법 집행 기관의 명령이 확실한 근거가 없다고 판단할 경우 그러한 명령에 적극적으로 이의를 제기합니다.
데이터 거버넌스	안전한 폐기	DG-05.1	테넌트가 원하는 경우, 보관된 데이터의 보안 삭제(예: 자기 소거/암호화 제거)를 지원합니까?	스토리지 디바이스의 수명이 다했을 경우 권한이 없는 개인에게 고객 데이터가 노출되는 것을 방지하기 위해 고안된 폐기 프로세스가 AWS 내에 마련되어 있습니다. AWS는 DoD 5220.22-M("국가 산업 보안 프로그램 운영 매뉴얼") 또는 NIST 800-88("미디어 삭제 가이드라인")에서 설명하는 기술을 사용해 폐기 프로세스에 따라 데이터를 제거합니다. 이 절차를 사용하여 하드웨어 디바이스를 폐기할 수 없는 경우 산업 표준 사례에 따라 디바이스의 저장을 제거하거나 디바이스를 물리적으로 파괴합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
데이터 거버넌스		DG-05.2	고객이 환경을 종료하거나 리소스를 사용하지 않을 경우 모든 컴퓨팅 리소스를 삭제하는 보증을 포함해 서비스 제공을 종료할 수 있는 게시된 절차를 제공할 수 있습니까?	
데이터 거버넌스	비 프로덕션 데이터	DG-06.1	비 프로덕션 환경에서 프로덕션 데이터가 복제되거나 사용되지 않도록 하는 절차가 마련되어 있습니까?	AWS 고객은 데이터에 대한 관리 및 소유권을 보유합니다. AWS는 고객에게 프로덕션 및 비 프로덕션 환경을 유지하고 개발할 수 있는 능력을 제공합니다. 프로덕션 데이터가 비 프로덕션 환경에 복제되지 않도록 해야 할 책임은 고객에게 있습니다.
데이터 거버넌스	정보 유출	DG-07.1	데이터 유출 또는 다중 테넌트 환경에서 테넌트 간의 의도적이거나 실수로 인한 손상을 방지할 수 있는 규제 항목이 마련되어 있습니까?	AWS 환경은 가상화된 다중 테넌트 환경입니다. AWS는 보안 관리 프로세스, PCI 컨트롤, 각 고객을 다른 고객과 격리할 수 있도록 고안된 기타 보안 컨트롤을 구현했습니다. AWS 시스템은 고객이 가상화 소프트웨어를 통한 필터링으로 자신에게 할당되지 않은물리적 호스트 또는 인스턴스에 액세스하는 것을 차단할 수 있도록 설계되었습니다. 이 아키텍처는 독립적인 PCI QSA(Qualified Security Assessor)의 검증을 받았으며 2015년 4월에 발표된 PCI DSS 버전 3.1의 모든 요구 사항을 준수하는 것으로 확인되었습니다.

도메인	제어 그룹	CID	평가 질문	AWS 답변
데이터 거버넌스		DG-07.2	클라우드 서비스 제품군과 연결되는 모든 시스템에 대해 데이터 손실 방지(DLP) 또는 압출 방지 솔루션이 마련되어 있습니까?	자세한 내용은 http://aws.amazon.com/security에서 AWS 위험 및 규정 준수 백서를 참조하십시오.
데이터 거버넌스	위험 평가	DG-08.1	테넌트가 산업 표준 연속 모니터링(테넌트가 물리적 및 논리적 제어 상태를 지속적으로 검증할 수 있음)을 구현할 수 있도록 보안 제어 상태 데이터를 제공합니까?	AWS는 고객에게 AWS에서 확립하고 운영하는 정책, 프로세스, 컨트롤에 대한 다양한 정보를 제공하기 위해 독립 감사자 보고서와 인증을 발행합니다. 관련 인증 및 보고서를 AWS 고객에게 제공할 수 있습니다. 고객이 시스템에서 논리적 컨트롤 연속 모니터링을 실행할 수 있습니다.
시설 보안	정책	FS-01.1	사무실, 방, 시설 및 보안 영역에서 안전하고 안정적인 업무 환경을 유지할 수 있는 정책과 절차가 마련되어 있음을 증명할 수 있습니까?	AWS는 외부 인증 기관 및 독립 감사자와 협력하여 규정 준수 프레임워크 준수를 검토하고 검증합니다. AWS SOC 1 Type II 보고서는 AWS에서 실행하는 특정 물리적 보안 제어 활동에 대한 자세한 정보를 제공합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 9.1항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
시설 보안	사용자 액세스	FS-02.1	현지 법률, 규정, 윤리 및 계약 제약조건에 의거하여 모든 입사지원자, 계약업체 및 제3자는 배경 조회를 받아야 합니까?	AWS는 준거법에서 허용하는 범위 내에서 채용 전 적격 심사 관행의 일환으로 직원의 직위와 AWS 시설에 대한 접근 권한에 따라 범죄 경력 조회를 실시합니다.
시설 보안	제어된 액세스 지점	FS-03.1	물리적 보안 경계(울타리, 벽, 장벽, 경비, 게이트, 전자 감시, 물리적 인증 메커니즘, 안내 데스크, 보안 순찰대)가 구현되어 있습니까?	물리적 보안 컨트롤에는 울타리, 벽, 보안 직원, 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단(단, 이에 제한되지 않음)과 같은 경계 컨트롤이 포함됩니다. AWS SOC 1 Type II 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 9.1항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.

도메인	제어 그룹	CID	평가 질문	AWS 답변
시설 보안	보안 영역 승인	FS-04.1	테넌트가 데이터가 저장되거나 액세스되는 위치를 기반으로 법정 관할 고려사항을 처리하기 위해 데이터를 가져오거나 내보낼 수 있는 지리적 위치를 지정할 수 있습니까?	AWS 고객은 데이터와 서버가 위치할 물리적 리전을 지정할 수 있습니다. AWS는 법률 또는 정부기관의 요청을 준수해야 하는 경우가 아닌 이상, 통지 없이 고객이 선택한 리전에서 고객의 콘텐츠를 옮기지 않습니다. 이 문서의 작성일 현재, 미국 동부(버지니아 북부), 미국 서부(오리건), 미국 서부(캘리포니아 북부), AWS GovCloud(미국, 오리건), EU(아일랜드), EU(프랑크푸르트), 아시아 태평양(싱가포르), 아시아 태평양(도쿄), 아시아 태평양(시드니), 남아메리카(상파울루)의 10개 리전이 있습니다. 자세한 내용은 AWS 웹 사이트(http://aws.amazon.com)를 참조하십시오.
시설 보안	권한 없는 개인의 진입	FS-05.1	서비스 영역과 같은 진입점 및 진출점과 권한 없는 개인이 구내에 진입할 수 있는 기타 지점이 모니터링되고 통제되고 데이터 스토리지 및 프로세스로부터 격리되어 있습니까?	건물 주위와 입구 지점에서 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단을 활용하여 전문 보안 직원에 의해 이들 건물에 대한 물리적인 접근을 엄격하게 통제하고 있습니다. 허가받은 직원이 데이터 센터에 접근하려면 2가지 요소를 이용한 신원확인과정을 최소 두 번 통과해야 합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오. 또한 AWS SOC 1 Type II 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다.
시설 보안	오프사이트 승인	FS-06.1	테넌트에게 하나의 물리적 위치에서 다른 위치로 데이터가 옮겨질 수 있는 시나리오를 설명하는 문서를 제공합니까? (예: 오프사이트 백업, 비즈니스 연속성 failover, 복제)	AWS 고객은 데이터가 위치할 물리적 리전을 지정할 수 있습니다. AWS는 법률 또는 정부기관의 요청을 준수해야 하는 경우가 아닌 이상, 통지 없이 고객이 선택한 리전에서 고객의 콘텐츠를 옮기지 않습니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.

도메인	제어 그룹	CID	평가 질문	AWS 답변
시설 보안	오프사이트 장비	FS-07.1	테넌트에게 자산 관리 및 장비 용도 변경을 관할하는 정책 및 절차를 설명하는 문서를 제공합니까?	ISO 27001 표준에 따라 스토리지 디바이스의 수명이 다했을 경우 권한이 없는 개인에게 고객 데이터가 노출되는 것을 방지할 수 있도록 고안된 폐기 프로세스가 AWS 절차 내에 마련되어 있습니다. AWS는 DoD 5220.22-M("국가 산업 보안 프로그램 운영 매뉴얼") 또는 NIST 800-88("미디어 삭제 가이드라인")에서 설명하는 기술을 사용해 폐기 프로세스에 따라 데이터를 제거합니다. 이 절차를 사용하여 하드웨어 디바이스를 폐기할 수 없는 경우 산업 표준 관행에 따라 디바이스의 저장을 제거하거나 디바이스를 물리적으로 파괴합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 도메인 9.2항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
시설 보안	자산 관리	FS-08.1	자산 소유권을 포함하여 모든 중요 자산의 재고를 빠짐없이 보유하고 있습니까?	ISO 27001 표준에 따라 AWS 하드웨어 자산이 소유자에게 할당되며 AWS 담당자가 AWS의 독점적인 재고 관리 도구를 사용해 자산을 추적 및 모니터링합니다. AWS 조달 및 공급망 팀은 모든 AWS 공급업체와의 관계를 유지합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 7.1항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
시설 보안		FS-08.2	모든 중요 공급업체의 재고를 빠짐없이 보유하고 있습니까?	
인사관리 보안	배경 조회	HR-01.1	현지 법률, 규정, 윤리 및 계약 제약조건에 의거하여 모든 입사지원자, 계약업체 및 제3자는 배경 조회를 받아야 합니까?	AWS는 준거법에서 허용하는 범위 내에서 채용 전 적격 심사 관행의 일환으로 직원의 직위와 AWS 시설에 대한 접근 권한에 따라 범죄 경력 조회를 실시합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
인사관리 보안	고용 계약	HR-02.1	직원에게 정보 보안 컨트롤을 제공하는 데 있어서 직원의 역할과 테넌트의 역할에 대해 분명하게 교육합니까?	모든 직원은 회사의 기업 행동강령 및 윤리강령을 제공받고 정기적으로 정보 보안 교육을 수료하고 수료증을 받아야 합니다. 준수성 감사는 직원들이 확립된 정책을 이해하고 따르는지 검증하기 위해 정기적으로 수행됩니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
		HR-02.2	직원이 수료한 교육의 수료증을 문서화합니까?	

도메인	제어 그룹	CID	평가 질문	AWS 답변
인사관리 보안	고용 종료	HR-03.1	고용 절차에서 다음 고용 종료 또는 변경을 수행할 역할 및 책임이 할당, 문서화 및 전달됩니까?	AWS 인사관리 팀은 직원 및 벤더의 종료 및 역할 변경 시 따라야 할 내부 관리 책임을 정의합니다. 조달/회수 직원 및 계약업체의 접근 권한 설정에 관한 책임은 인사관리부서(HR), 기업 경영 및 서비스 소유자가 분담합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
정보 보안	관리 프로그램	IS-01.1	테넌트에게 정보 보안 관리 프로그램(ISMP)을 설명하는 문서를 제공합니까?	AWS는 고객에게 AWS ISMS 프로그램을 설명하는 ISO 27001 인증 문서를 제공합니다.
정보 보안	관리 지원/개입	IS-02.1	경영진과 직속 관리자가 명확하게 문서화된 지침, 약속, 명시적인 과제, 과제 실행 확인을 통해 정보 보안을 지원하는 공식적인 조치를 취하도록 보장하는 정책이 마련되어 있습니까?	ISO 27001 표준에 따라 AWS 정보 보안 프레임워크를 통해 정책 및 절차가 확립되었습니다. Amazon의 규제 환경은 회사의 경영진에서부터 시작됩니다. 경영진과 선임 책임자는 회사의 우선 순위와 핵심 가치 형성에 중요한 역할을 합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 위험 및 규정 준수 백서를 참조하십시오.
정보 보안	정책	IS-03.1	정보 보안과 개인 정보 보호 정책이 특정 산업 표준(ISO-27001, ISO-22307, CoBIT 등)을 준수합니까?	COBIT 프레임워크, ISO 27001 표준 및 PCI DSS 요건을 기반으로 AWS 정보 보안을 통해 정책 및 절차가 확립되었습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. 또한 AWS는 SOC 1 Type II 보고서를 발행합니다. 자세한 내용은 SOC 1 보고서를 참조하십시오. 자세한 내용은 http://aws.amazon.com/security에서 AWS 위험 및 규정 준수 백서를 참조하십시오.
		IS-03.2	공급자가 정보 보안과 개인 정보 보호 정책을 준수하도록 보장하는 계약이 있습니까?	
		IS-03.3	컨트롤, 아키텍처, 규정 및/또는 표준 프로세스의 실사 매핑 증거를 제공할 수 있습니까?	
정보 보안	기준 요건	IS-04.1	인프라의 모든 구성 요소(예: 하이퍼바이저, 운영 체제, 라우터, DNS 서버 등)의 정보 보안 기준을 문서화했습니까?	ISO 27001 표준에 따라 AWS는 중요 구성 요소에 대한 시스템 기준을 유지합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 12.1 및 15.2항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. 고객이 자체 가상 머신 이미지를 제공할 수 있습니다. VM Import를 사용해 가상 머신 이미지를 기존 환경에서 Amazon EC2 인스턴스로 손쉽게 가져올 수 있습니다.
정보 보안		IS-04.2	정보 보안 기준에 따라 인프라의 규정 준수를 지속적으로 모니터링 및 보고할 수 있습니까?	
정보 보안		IS-04.3	고객이 내부 표준을 준수할 수 있도록 신뢰할 수 있는 가상 머신 이미지를 제공하도록 허용합니까?	

도메인	제어 그룹	CID	평가 질문	AWS 답변
정보 보안	정책 검토	IS-05.1	정보 보안 및/또는 개인 정보 보호 정책 자료를 변경한 경우 테넌트에게 알립니까?	http://aws.amazon.com/security 에서 AWS 보안 프로세스 개요 백서와 위험 및 규정 준수 백서는 AWS 정책 업데이트를 반영하기 위해 정기적으로 업데이트됩니다.
정보 보안	정책 시행	IS-06.1	보안 정책 및 절차를 위반한 직원에 대한 공식적인 징계 및 제재 정책이 마련되어 있습니까?	AWS는 직원에게 보안 정책을 전달하고 정보 보안과 관련한 역할 및 책임을 교육하기 위한 보안 교육을 제공합니다. Amazon 표준 또는 규약을 위반한 직원은 조사를 받고 적절한 징계 조치(예: 경고, 성과 계획, 정직 및/또는 해고)를 받게 됩니다. 자세한 내용은 http://aws.amazon.com/security의 AWS 보안 프로세스 개요 백서를 참조하십시오. 자세한 내용은 ISO 27001 표준, 부록 A, 8.2항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
정보 보안		IS-06.2	직원이 위반 발생 시 취할 수 있는 조치와 정책 및 절차에 명시된 조치를 인지하도록 돕고 있습니까?	
정보 보안	사용자 액세스 정책	IS-07.1	더 이상 비즈니스에 필요하지 않은 시스템 액세스를 적시에 제거할 수 있는 컨트롤이 마련되어 있습니까?	접근 권한은 직원의 기록이 Amazon의 인사관리 시스템에서 제거되면 자동으로 취소됩니다. 직원의 직무 기능이 변경된 경우, 자원에 대한 지속적인 접근 여부를 구체적으로 허가받아야 하며, 그렇지 않을 경우 접근이 자동으로 취소됩니다. AWS SOC 1 Type II 보고서는 사용자 액세스 취소에 대한 자세한 내용을 제공합니다. AWS 보안 백서의 "직원 수명 주기" 섹션에도 자세한 내용이 나와 있습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 11항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
정보 보안		IS-07.2	더 이상 비즈니스에 필요하지 않은 시스템 액세스를 제거할 수 있는 속도를 추적하는 측정치를 제공합니까?	
정보 보안	사용자 액세스 제한/승인	IS-08.1	테넌트 데이터에 대한 액세스를 허용하고 승인하는 방법을 문서화합니까?	AWS 고객은 데이터에 대한 관리 및 소유권을 보유합니다. 콘텐츠의 개발, 내용, 운영, 유지 및 사용에 대한 책임은 고객에게 있습니다.
정보 보안		IS-08.2	액세스 제어 목적으로 공급자 및 테넌트 데이터 분류 방법론을 조정할 수 있는 방법이 있습니까?	

도메인	제어 그룹	CID	평가 질문	AWS 답변
정보 보안	사용자 액세스 취소	IS-09.1	직원, 계약업체, 고객, 비즈니스 파트너 또는 제3자의 상태가 변경된 경우 구현된 조직 시스템, 정보 자산 및 데이터에 대한 사용자 액세스를 적시에 해지, 취소 또는 수정합니까?	접근 권한은 직원의 기록이 Amazon의 인사관리 시스템에서 제거되면 자동으로 취소됩니다. 직원의 직무 기능이 변경된 경우, 자원에 대한 지속적인 접근 여부를 구체적으로 허가받아야 하며, 그렇지 않을 경우 접근이 자동으로 취소됩니다. AWS SOC 1 Type II 보고서는 사용자 액세스 취소에 대한 자세한 내용을 제공합니다. AWS 보안 백서의 "직원 수명 주기" 섹션에도 자세한 내용이 나와 있습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 11항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
정보 보안		IS-09.2	상태 변경은 고용, 계약 또는 합의 종료, 고용 변경 또는 조직 내 인사 이동을 반영하기 위해 조치입니까?	
정보 보안	사용자 액세스 검토	IS-10.1	모든 시스템 사용자 및 관리자에게 최소한 1년에 한 번 자격 증명을 요구합니까(테넌트가 관리하는 사용자 제외)?	ISO 27001 표준에 따라 90일마다 모든 액세스 권한이 검토되며 명시적 재승인을 받지 않으면 리소스에 대한 액세스가 자동으로 취소됩니다. 사용자 액세스 검토와 관련한 컨트롤이 SOC 1 Type II 보고서에 개략적으로 설명되어 있습니다. 사용자 권한 컨트롤 예외가 SOC 1 Type II 보고서에 설명되어 있습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 11.2항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
정보 보안		IS-10.2	사용자의 권한이 부적절하다고 판명된 경우 모든 수정 및 인증 조치가 기록됩니까?	
정보 보안		IS-10.3	테넌트 데이터에 대한 무단 액세스가 허용될 수 있는 경우 테넌트와 권한 수정 및 인증 보고서를 공유합니까?	
정보 보안	교육/인식	IS-11.1	테넌트 데이터에 액세스할 수 있는 모든 사람이 클라우드 관련 액세스 및 데이터 관리 문제(다중 테넌트, 국적, 클라우드 제공 모델 업무 분담 개념, 이해충돌)를 해결할 수 있도록 공식 보안 인식 교육 프로그램을 제공합니까?	ISO 27001 표준에 따라 모든 AWS 직원들은 정기적으로 정보 보안 교육을 수료하고 수료증을 받아야 합니다. 준수성 감사는 직원들이 확립된 정책을 이해하고 따르는지 검증하기 위해 정기적으로 수행됩니다.
정보 보안		IS-11.2	관리자와 데이터 관리자가 보안 및 데이터 무결성과 관련한 각자의 법적 책임에 대해 적절한 교육을 받았습니까?	
정보 보안	산업 지식/벤치마킹	IS-12.1	정보 보안과 관련된 산업 그룹 및 전문가 협의회에 참여하고 있습니까?	AWS 규정 준수 및 보안 팀은 보안과 관련된 산업 그룹 및 전문가 서비스와 지속적으로 접촉하고 있습니다. AWS는 COBIT 프레임워크를 기반으로 정보 보안 프레임워크 및정책을 구성하고 ISO 27002 제어 및 PCI DSS를 기반으로 ISO 27001 인증 가능 프레임워크를 통합했습니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 위험 및 규정 준수 백서를 참조하십시오.

도메인	제어 그룹	CID	평가 질문	AWS 답변
		IS-12.2	업계 표준을 기준으로 보안 제어를 벤치마킹합니까?	
정보 보안	역할 / 책임	IS-13.1	테넌트에게 관리자 책임과 테넌트의 책임을 명료하게 설명하는 역할 정의 문서를 제공합니까?	AWS 보안 프로세스 개요 백서와 AWS 위험 및 규정 준수 백서는 AWS와 고객의 역할 및 책임에 대한 자세한 정보를 제공합니다. 백서는 http://aws.amazon.com/security에서 참조할 수 있습니다.
정보 보안	관리 감독	IS-14.1	관리자가 자신의 책임 영역과 관련된 보안 정책, 절차 및 표준을 인지하고 준수할 책임을 집니까?	Amazon의 규제 환경은 회사의 경영진에서부터 시작됩니다. 경영진과 선임 책임자는 회사의 우선 순위와 핵심 가치 형성에 중요한 역할을 합니다. 모든 직원은 회사의 기업 행동강령 및 윤리강령을 제공받고 정기적으로 교육을 수료합니다. 준수성 감사는 직원들이 확립된 정책을 이해하고 따르도록 하기 위해 수행됩니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 위험 및 규정 준수 백서를 참조하십시오.
정보 보안	업무 분담	IS-15.1	테넌트에게 클라우드 서비스 내에서 업무 분담을 유지하는 방법에 대한 문서를 제공합니까?	고객이 AWS 리소스의 업무 분담을 관리할 수 있습니다. 내부적으로 AWS는 업무 분담을 관리하는 데 있어서 ISO 27001 표준을 준수합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 10.1항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
정보 보안	사용자 책임	IS-16.1	사용자가 게시된 보안 정책, 절차, 표준, 적용 가능한 규제 요건을 인지하고 준수해야 할 책임을 이해하도록 돕고 있습니까?	AWS는 다양한 내부 커뮤니케이션 방법을 전사적으로 구현하여 직원들이 자신의 역할과 책임을 이해하고 중요한 사안을 적시에 의논할 수 있도록 돕습니다. 이러한 방법에는 Amazon 인트라넷을 통한 전자 메일 메시지와 정보 게시물뿐 아니라 신입 직원을 위한 오리엔테이션 및 교육 프로그램이 포함됩니다. 자세한 내용은 ISO 27001 표준, 부록 A, 도메인 8.2 및 11.3을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서에서도 자세한 내용을 확인하실 수 있습니다.
정보 보안		IS-16.2	사용자가 안전하고 안정적인 업무 환경을 유지할 책임을 인지하도록 돕고 있습니까?	
정보 보안		IS-16.3	사용자가 자리를 비울 때 장비를 안전하게 보관해야 할 책임을 인지하도록 돕고 있습니까?	

도메인	제어 그룹	CID	평가 질문	AWS 답변
정보 보안	작업 영역	IS-17.1	데이터 관리 정책과 절차에 테넌트 및 서비스 차원의 이해충돌이 설명되어 있습니까?	AWS 데이터 관리 정책은 ISO 27001 표준을 준수합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 도메인 8.2 및 11.3을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. AWS SOC 1 Type II 보고서는 AWS에서 AWS 리소스에 대한 무단 액세스를 방지하기 위해 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다.
정보 보안		IS-17.2	데이터 관리 정책 및 절차에 테넌트 데이터에 대한 무단 액세스를 방지할 수 있는 변조 감사 또는 소프트웨어 기능이 포함되어 있습니까?	
정보 보안		IS-17.3	가상 머신 관리 인프라에 가상 머신의 빌드/구성 변경을 탐지할 수 있는 변조 감사 또는 소프트웨어 무결성 기능이 포함되어 있습니까?	
정보 보안	암호화	IS-18.1	테넌트별로 고유한 암호화 키를 생성할 수 있습니까?	AWS 고객은 AWS 서버 측 암호화 서비스를 사용하는 경우를 제외하고 자체적으로 암호화를 관리합니다. 이 경우 AWS는 테넌트별로 고유한 암호화 키를 생성합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
정보 보안		IS-18.2	테넌트가 생성한 암호화 키를 지원하거나 테넌트가 공개 키 인증서에 액세스하지 않고도 ID 데이터를 암호화할 수 있도록 허용합니까(예: ID 기반 암호화)?	
정보 보안	암호화 키 관리	IS-19.1	환경 내에서 디스크 또는 스토리지에 저장된 테넌트 데이터를 암호화합니까?	AWS는 고객이 S3, EBS, SimpleDB, EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있도록 지원합니다. VPC에 대한 IPSec 터널도 암호화됩니다. Amazon S3도 고객을 위한 옵션으로 Server Side Encryption을 제공합니다. 고객은 타사의 암호화 기술을 사용할 수도 있습니다. AWS 키 관리 절차는 ISO 27001 표준을 준수합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 15.1항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
정보 보안		IS-19.2	네트워크와 하이퍼바이저 인스턴스 간에 데이터와 가상 머신 이미지를 전송할 때 암호화를 활용해 이러한 데이터를 보호합니까?	
정보 보안		IS-19.3	테넌트를 대신해 암호화 키를 관리할 수 있습니까?	
정보 보안		IS-19.4	키 관리 절차를 관리합니까?	
정보 보안	취약성/패치 관리	IS-20.1	산업 모범 사례에 규정된 대로 네트워크 계층 취약성 검사를 정기적으로 수행하고 있습니까?	고객은 게스트 운영 체제, 소프트웨어 및 애플리케이션에 대한 관리 및 소유권을 보유하고 있으므로 시스템에 취약성 검사를 수행하고 패치를 적용할 책임은 고객에게 있습니다. 고객은 검사가 고객의 인스턴스에 국한되고 AWS Acceptable Use Policy를 위반하지 않는 범위에서 클라우드 인프라 검사를 수행할 수 있는 권한을 요청할 수 있습니다. AWS 보안 팀은 모든 인터넷 연결 서비스 endpoint IP 주소를 정기적으로 검사하여 취약성이 있는지 확인합니다. AWS 보안 팀은 확인된 취약성을 해결하기 위해 해당 당사자에게 취약성을 알립니다. AWS의 자체 유지보수 및 시스템 패치 적용은 일반적으로 고객에게 영향을 미치지 않습니다. 자세한 내용은http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
정보 보안		IS-20.2	산업 모범 사례에 규정된 대로 애플리케이션 계층 취약성 검사를 정기적으로 수행하고 있습니까?	
정보 보안		IS-20.3	산업 모범 사례에 규정된 대로 로컬 운영 체제 계층 취약성 검사를 정기적으로 수행하고 있습니까?	
정보 보안		IS-20.4	테넌트가 요청할 경우 취약성 검사 결과를 제공합니까?	

도메인	제어 그룹	CID	평가 질문	AWS 답변
정보 보안		IS-20.5	모든 컴퓨팅 디바이스, 애플리케이션, 시스템 전반에서 신속하게 취약성에 패치를 적용할 수 있습니까?	자세한 내용은 ISO 27001 표준, 부록 A, 12.5항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
정보 보안		IS-20.6	테넌트가 요청할 경우 위험 기반 시스템 패치 적용 기간을 제공합니까?	
정보 보안	안티바이러스/악성 소프트웨어	IS-21.1	클라우드 서비스를 지원하는 모든 시스템에 맬웨어 방지 프로그램이 설치되어 있습니까?	안티바이러스/악성 소프트웨어를 관리하는 AWS의 프로그램, 프로세스 및 절차는 ISO 27001 표준을 준수합니다. 자세한 내용은 AWS SOC 1 Type II 보고서를 참조하십시오. ISO 27001 표준, 부록 A, 10.4항에서도 자세한 내용을 확인하실 수 있습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
정보 보안		IS-21.2	업계에서 허용하는 기간 내에 모든 인프라 구성 요소에서 서명, 목록 또는 행동 패턴을 사용하는 보안 침입 탐지 시스템을 업데이트합니까?	
정보 보안	인시던트 관리	IS-22.1	보안 인시던트 대응 계획을 문서화했습니까?	AWS의 인시던트 대응 프로그램, 계획 및 절차는 ISO 27001 표준에 따라 개발되었습니다. AWS SOC 1 Type II 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. AWS 보안 프로세스 개요 백서(http://aws.amazon.com/security 에서 제공)에도 자세한 내용이 나와 있습니다.
정보 보안		IS-22.2	맞춤화된 테넌트 요건을 보안 인시던트 대응 계획에 통합합니까?	
정보 보안		IS-22.3	보안 인시던트 도중 AWS와 테넌트가 책임져야 할 영역을 지정하는 역할 및 책임 문서를 게시합니까?	
정보 보안	인시던트 보고	IS-23.1	SIEM(보안 정보 및 이벤트 관리) 시스템에서 상세 분석 및 경고를 위해 데이터 소스(예: 앱 로그, 방화벽 로그, IDS 로그, 물리적 액세스 로그 등)를 병합합니까?	AWS의 인시던트 대응 프로그램, 계획 및 절차는 ISO 27001 표준에 따라 개발되었습니다. AWS SOC 1 Type II 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. 고객을 대신해 AWS에 저장된 모든 데이터는 강력한 테넌트 격리 보안 및 제어 기능을 갖고 있습니다. 자세한 내용은 AWS 보안 프로세스 개요 백서와 AWS 위험 및 규정 준수 백서(http://aws.amazon.com/security에서 제공)를 참조하십시오.
정보 보안		IS-23.2	인시던트를 특정 테넌트에서 격리할 수 있도록 프레임워크를 기록하고 모니터링합니까?	
정보 보안	인시던트 대응 법적 준비	IS-24.1	인시던트 대응 계획이 법적으로 허용되는 연계보관성(chain-of-custody) 관리 프로세스 및 컨트롤에 대한 산업 표준을 준수합니까?	AWS의 인시던트 대응 프로그램, 계획 및 절차는 ISO 27001 표준에 따라 개발되었습니다. AWS SOC 1 Type II 보고서는 AWS에서 실행하는 특정 규제항목에 대한 자세한 정보를 제공합니다. 고객을 대신해 AWS에 저장된 모든 데이터는 강력한 테넌트 격리 보안 및 제어 기능을 갖고 있습니다.

도메인	제어 그룹	CID	평가 질문	AWS 답변
정보 보안		IS-24.2	인시던트 대응 기능에 법적으로 허용되는 과학 수사 데이터 수집 및 분석 기법 사용이 포함되어 있습니까?	자세한 내용은 AWS 보안 프로세스 개요 백서와 AWS 위험 및 규정 준수 백서(http://aws.amazon.com/security에서 제공)를 참조하십시오.
정보 보안		IS-24.3	다른 테넌트 데이터를 동결시키지 않고 특정 테넌트의 증거 보존(일정 기간 동안 데이터 동결)을 지원할 수 있습니까?	
정보 보안		IS-24.4	법적 소환에 대응해 데이터를 생성할 때 테넌트 데이터 분리를 강화하고 증명합니까?	
정보 보안	인시던트 대응 측정치	IS-25.1	유형, 볼륨, 모든 정보 보안 인시던트에 대한 영향을 모니터링하고 정량화합니까?	ISO 27001 표준에 따라 AWS 보안 측정치를 모니터링 및 분석합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 13.2항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
정보 보안		IS-25.2	테넌트가 요청할 경우 통계 정보 보안 인시던트 데이터를 공유합니까?	
정보 보안	사용 제한	IS-26.1	테넌트 데이터 및/또는 메타데이터를 활용하거나 액세스할 수 있는 방법에 대한 문서를 제공합니까?	AWS 고객은 데이터에 대한 관리 및 소유권을 보유합니다.
정보 보안		IS-26.2	검사 기술(검색 엔진 등)을 사용해 테넌트 데이터 사용에 대한 메타데이터를 수집 또는 생성합니까?	
정보 보안		IS-26.3	테넌트가 검사 기술을 통한 데이터/메타데이터 액세스를 옵트아웃할 수 있습니까?	
정보 보안	자산 수익률	IS-27.1	개인 정보 보호 침해를 모니터링하고 개인 정보 보호 이벤트가 데이터에 영향을 미칠 수 있는 경우 테넌트에게 알릴 수 있는 시스템이 마련되어 있습니까?	AWS 고객은 자체 환경에서 개인 정보 보호 침해가 있는지 모니터링할 책임이 있습니다. AWS SOC 1 Type II 보고서는 AWS 관리 환경을 모니터링하기 위해 마련된 컨트롤에 대한 개요를 제공합니다.
정보 보안		IS-27.2	개인 정보 보호 정책이 산업 표준을 준수합니까?	
정보 보안	전자상거래	IS-28.1	퍼블릭 네트워크(예: 인터넷)를 통과하는 데 필요한 경우, 테넌트 데이터를 보호하기 위해 개방형 암호화 방법(3.4ES, AES 등)을 제공합니까?	모든 AWS API는 SSL을 보호하는 endpoint를 통해 서버 인증을 제공합니다. AWS는 고객이 S3, EBS, SimpleDB, EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있도록 지원합니다. VPC에 대한 IPSec 터널도 암호화됩니다. Amazon S3도 고객을 위한 옵션으로 Server Side Encryption을 제공합니다. 고객은 제3자 암호화 기술을 사용할 수도 있습니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
정보 보안		IS-28.2	인프라 구성 요소가 공용 네트워크(예: 하나의 환경에서 다른 환경으로의 인터넷 기반 데이터 복제)를 통해 서로 통신해야 할 경우 언제든지 개방형 암호화 방법론을 활용합니까?	

도메인	제어 그룹	CID	평가 질문	AWS 답변
정보 보안	감사 도구 액세스	IS-29.1	정보 보안 관리 시스템에 대한 액세스를 제한, 기록, 모니터링합니까? (예: 하이퍼바이저, 방화벽, 취약성 스캐너, 네트워크 스니퍼, API 등)	ISO 27001 표준에 따라 AWS는 AWS 리소스에 대한 논리적 액세스에 대한 최소 표준을 규정하는 공식적인 정책 및 절차를 확립했습니다. AWS SOC 1 Type II 보고서는 AWS 리소스에 대한 액세스 프로비저닝을 관리하기 위해 마련된 컨트롤을 개략적으로 설명합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
정보 보안	진단/포트 액세스 구성	IS-30.1	전용 보안 네트워크를 활용해 클라우드 서비스 인프라에 대한 관리 액세스를 제공합니까?	업무와 관련하여 관리 평면에 접근해야 하는 관리자는 멀티 팩터 인증을 사용하여 특정 관리 호스트에 접근하는 데 필요한 접근 권한을 얻어야 합니다. 이러한 관리 호스트는 클라우드의 관리 평면을 보호하기 위해 특별히 설계, 구축, 구성 및 강화된 시스템입니다. 이러한 접근은 모두 기록되고 감사됩니다. 어떤 직원이 업무와 관련하여 관리 평면을 더 이상 액세스할 필요가 없게 될 경우, 이러한 호스트 및 관련 시스템에 대한 권한과 액세스 권한은 해지됩니다.
정보 보안	네트워크/인프라 서비스	IS-31.1	클라우드 서비스의 모든 관련 구성 요소에 대한 용량 및 사용률 데이터를 수집합니까?	AWS는 ISO 27001 표준에 따라 용량 및 사용률 데이터를 관리합니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
정보 보안		IS-31.2	테넌트에게 용량 계획 및 사용률 보고서를 제공합니까?	
정보 보안	이동식/모바일 디바이스	IS-32.1	노트북, 휴대폰, 개인 정보 단말기(PDA) 등 일반적으로 비 이동식 디바이스(예: 공급자 조직의 시설에 설치된 데스크톱 컴퓨터)보다 위험이 더 높은 이동식 및 모바일 디바이스의 중요한 데이터에 대한 액세스를 엄격하게 제한하기 위한 정책과 절차를 확립하고 조치를 마련했습니까?	ISO 27001 표준에 따라 AWS는 AWS 리소스에 대한 논리적 액세스에 대한 최소 표준을 규정하는 공식적인 정책 및 절차를 확립했습니다. AWS SOC 1 Type II 보고서는 AWS 리소스에 대한 액세스 프로비저닝을 관리하기 위해 마련된 컨트롤을 개략적으로 설명합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
정보 보안	소스 코드 액세스 제한	IS-33.1	애플리케이션, 프로그램 또는 객체 소스 코드에 대한 무단 액세스를 방지하고 권한 있는 사람에게만 액세스를 허용하는 컨트롤이 마련되어 있습니까?	ISO 27001 표준에 따라 AWS는 AWS 리소스에 대한 논리적 액세스에 대한 최소 표준을 규정하는 공식적인 정책 및 절차를 확립했습니다. AWS SOC 1 Type II 보고서는 AWS 리소스에 대한 액세스 프로비저닝을 관리하기 위해 마련된 컨트롤을 개략적으로 설명합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.

도메인	제어 그룹	CID	평가 질문	AWS 답변
정보 보안		IS-33.2	테넌트 애플리케이션, 프로그램 또는 객체 소스 코드에 대한 무단 액세스를 방지하고 권한 있는 사람에게만 액세스를 허용하는 컨트롤이 마련되어 있습니까?	
정보 보안	유틸리티 프로그램 액세스	IS-34.1	가상 파티션에 중대한 영향을 미칠 수 있는 관리 유틸리티(예: 종료, 복제 등)를 적절히 제한 및 모니터링하고 있습니까?	ISO 27001 표준에 따라 시스템 유틸리티를 적절하게 제한하고 모니터링합니다. AWS SOC 1 Type II 보고서는 시스템 액세스를 제한하기 위해 마련된 규제 항목에대한 자세한 정보를 제공합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
정보 보안		IS-34.2	가상 인프라를 직접 대상으로 하는 공격(예: 시밍, Blue Pill, 하이퍼 점핑 등)을 감지하는 기능이 있습니까?	
정보 보안		IS-34.3	기술 컨트롤이 가상 인프라를 표적으로 하는 공격을 방지합니까?	
법적 고지	비밀 유지 계약	LG-01.1	데이터 및 운영 정보 보호에 대한 조직의 필요를 반영하는 비밀 유지 계약 또는 기밀 협약의 요건을 정기적으로 확인, 문서화 및 검토합니까?	Amazon 법률 자문 팀이 Amazon NDA를 관리하고 AWS 비즈니스 요구를 반영하기 위해 정기적으로 개정합니다.
법적 고지	제3자 계약	LG-02.1	데이터가 처리, 저장 및 전송되는 국가의 법률에 따라 아웃소싱 공급자를 선정하고 모니터링합니까?	AWS는 고객에게 AWS 서비스를 제공하기 위해 제3자 클라우드 공급자를 활용하지 않습니다. 제3자 계약은 Amazon 법률 자문 팀에서 적절히 검토합니다.
법적 고지		LG-02.2	데이터가 시작되는 국가의 법률에 따라 아웃소싱 공급자를 선정하고 모니터링합니까?	
법적 고지		LG-02.3	법률 자문 팀이 모든 제3자 계약을 검토합니까?	
운영 관리	정책	OP-01.1	서비스 운영 역할을 적절하게 지원할 수 있도록 정책과 절차가 확립되어 있고 모두에게 제공됩니까?	COBIT 프레임워크, ISO 27001 표준 및 PCI DSS 요건을 기반으로 AWS 정보 보안 프레임워크를 통해 정책 및 절차가 확립되었습니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 위험 및 규정 준수 백서를 참조하십시오.
운영 관리	설명서	OP-02.1	권한 있는 직원에게 정보 시스템 설명서(예: 관리자 안내서 및 사용 설명서, 아키텍처 다이어그램 등)를 제공하여 정보 시스템의 구성, 설치 및 운영을 지원하고 있습니까?	AWS 직원은 Amazon의 인트라넷 사이트를 통해 내부에서 정보 시스템 문서를 사용할 수 있습니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.

도메인	제어 그룹	CID	평가 질문	AWS 답변
운영 관리	용량/리소스 계획	OP-03.1	상황/시나리오에 따른 시스템 수준별(네트워크, 스토리지, 메모리, I/O 등) 초과 구독에 대해 안내하는 설명서를 제공하고 있습니까?	AWS는 용량 관리 관행을 공개하지 않습니다. AWS는 성능 수준 약정을 전달하기 위해 서비스에 대한 서비스 수준 협약을 발행합니다.
운영 관리		OP-03.2	하이퍼바이저에 있는 메모리 초과 가입 기능의 사용을 제한합니까?	
운영 관리	장비 관리	OP-04.1	가상 인프라를 사용할 경우 클라우드 솔루션에 하드웨어 독립적인 복원 및 복구 기능이 포함되어 있습니까?	고객은 EBS 스냅샷 기능을 이용해 언제든지 가상 머신 이미지를 캡처하고 복원할 수 있습니다. 고객은 AMI를 내보내 온프레미스 또는 다른 공급자에서 사용할 수있습니다(소프트웨어 라이선스 제한이 적용됨). 자세한 내용은 http://aws.amazon.com/security의 AWS 보안 프로세스 개요 백서를 참조하십시오.
운영 관리		OP-04.2	가상 인프라를 사용할 경우 테넌트에게 가상 머신을 제 때에 이전 상태로 복원할 수 있는 기능을 제공합니까?	
운영 관리		OP-04.3	가상 인프라를 사용할 경우 가상 머신 이미지를 다운로드하여 새 클라우드 공급자에 이식할 수 있습니까?	
운영 관리		OP-04.4	가상 인프라를 사용할 경우 고객이 그러한 이미지를 자체 오프사이트 스토리지 위치에 복제할 수 있도록 머신 이미지가 제공됩니까?	
운영 관리		OP-04.5	클라우드 솔루션에 소프트웨어/공급자에 의존하지 않는 복원 및 복구 기능이 포함되어 있습니까?	
위험 관리	프로그램	RI-01.1	제3자 보험을 통해 손실을 보증합니까?	AWS는 AWS의 서비스 수준 협약에 따라 중단으로 인해 발생할 수 있는 손실을 보상합니다.
위험 관리		RI-01.2	조직의 서비스 수준 협약이 인프라 내에서 발생한 중단 또는 손실로 인해 야기될 수 있는 손실에 대해 테넌트 보상을 제공합니까?	
위험 관리	평가	RI-02.1	공식적인 위험 평가가 전사적인 프레임워크에 맞게 조정되어 있으며, 정성적 및 정량적 방법을 사용해 최소한 1년에 한 번 또는 정기적으로 공식적인 위험 평가를 수행하여 식별된 모든 위험의 발생 가능성과 영향을 파악합니까?	ISO 27001에 따라 AWS는 위험을 완화하고 관리하는 위험 관리 프로그램을 개발했습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증을 준수함을 검증 및 인증받았습니다.
위험 관리		RI-02.2	모든 위험 범주(예: 감사 결과, 위협 및 취약성 분석, 규제 준수)를 고려하여 내재 및 잔존 위험과 관련된 발생 가능성과 영향을 독립적으로 판단합니까?	AWS 위험 관리 프레임워크에 대한 자세한 내용은 AWS 위험 및 규정 준수 백서(aws.amazon.com/security에서 제공)를 참조하십시오.

도메인	제어 그룹	CID	평가 질문	AWS 답변
위험 관리	완화/수용	RI-03.1	합리적인 해결 기간 내에 회사에서 확립한 기준에 따라 모든 위험이 수용 가능한 수준으로 완화됩니까?	ISO 27001 표준, 부록 A, 4.2항에 따라 AWS는 위험을 완화하고 관리하는 위험 관리 프로그램을 개발했습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증을 준수함을 검증 및 인증받았습니다. AWS 위험 관리 프레임워크에 대한 자세한 내용은 http://aws.amazon.com/security에서
		RI-03.2	합리적인 기간 내에 회사에서 확립한 기준에 따라 수정 조치가 수용 가능한 수준에서 수행됩니까?	AWS 위험 및 규정 준수 백서를 참조하십시오.
위험 관리	비즈니스/정책 변경의 영향	RI-04.1	보안 정책, 절차, 표준 및 컨트롤이 관련성 및 유효성을 유지할 수 있도록 위험 평가 결과에 이러한 항목에 대한 업데이트가 포함됩니까?	AWS 보안 정책, 절차, 표준 및 컨트롤 업데이트는 ISO 27001 표준에 따라 매년 진행됩니다. 자세한 내용은 ISO 27001 표준, 부록 A, 5.1항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증을 준수함을 검증 및 인증받았습니다.
위험 관리	타사 액세스	RI-05.1	다중 실패 재해 복구 기능을 제공합니까?	AWS는 각 리전 내의 여러 가용 영역뿐 아니라 여러 리전 내에 인스턴스를 배치하고 데이터를 저장하는 유연성을 고객들에게 제공합니다. 각 가용 영역은 독립된 장애 영역으로 설계되었습니다. 장애 시 자동화된 프로세스는 고객 데이터 트래픽을 장애 지역에서 먼 곳으로 이동합니다. AWS SOC 1 Type II 보고서에 자세한 정보가 나와 있습니다. 자세한 내용은 ISO 27001 표준 부록 A, 도메인 11.2를 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증을 준수함을 검증 및 인증받았습니다.
		RI-05.2	공급자 실패 시 업스트림 공급자를 통해 서비스 연속성을 모니터링합니까?	
		RI-05.3	각 서비스에 공급자가 둘 이상 있습니까?	
		RI-05.4	사용하는 서비스가 포함되어 있는 운영 중복성 및 연속성 요약에 대한 액세스 권한을 제공합니까?	
		RI-05.5	테넌트에게 재해를 선언할 수 있는 기능을 제공합니까?	
		RI-05.6	테넌트에게 트리거링된 failover 옵션을 제공합니까?	
		RI-05.7	비즈니스 연속성 및 중복성 계획을 테넌트와 공유합니까?	
릴리스 관리	새로운 개발/인수	RM-01.1	새로운 애플리케이션, 시스템, 데이터베이스, 인프라, 서비스, 운영 및 시설 개발 또는 인수를 위한 관리 권한 부여에 대한 정책과 절차가 확립되어 있습니까?	ISO 27001 표준에 따라 AWS는 새로운 리소스 개발을 관리하는 절차를 마련했습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증을 준수함을 검증 및 인증받았습니다. AWS SOC 1 Type II 보고서에서도 자세한 내용을 확인하실 수 있습니다.

도메인	제어 그룹	CID	평가 질문	AWS 답변
릴리스 관리	프로덕션 변경	RM-02.1	테넌트에게 프로덕션 변경 관리 절차와 이에 대한 테넌트의 역할/권한/책임을 설명하는 문서를 제공합니까?	AWS SOC 1 Type II 보고서는 AWS 환경에서 변경 관리를 관리하기 위해 마련된 컨트롤을 개괄적으로 설명합니다. ISO 27001 표준, 부록 A, 12.5항에서도 자세한 내용을 확인하실 수 있습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
릴리스 관리	품질 테스트	RM-03.1	테넌트에게 품질 보증 프로세스를 설명하는 문서를 제공합니까?	AWS는 ISO 27001 표준을 준수하는 시스템 개발 수명 주기(SDLC) 프로세스의 일환으로 품질 표준을 통합합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 10.1항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
릴리스 관리	아웃소싱 개발	RM-04.1	모든 소프트웨어 개발 시 품질 표준을 충족할 수 있도록 보장하는 컨트롤이 마련되어 있습니까?	AWS는 일반적으로 소프트웨어 개발을 아웃소싱하지 않습니다. AWS는 ISO 27001 표준을 준수하는 시스템 개발 수명 주기(SDLC) 프로세스의 일환으로 품질 표준을 통합합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 10.1항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
릴리스 관리		RM-04.2	아웃소싱 소프트웨어 개발 활동에서 소스 코드 보안 결함을 탐지할 수 있는 컨트롤이 마련되어 있습니까?	
릴리스 관리	권한 없는 소프트웨어 설치	RM-05.1	권한 없는 소프트웨어가 시스템에 설치되는 것을 제한하고 모니터링하는 컨트롤이 마련되어 있습니까?	악성 소프트웨어를 관리하는 AWS의 프로그램, 프로세스 및 절차는 ISO 27001 표준을 준수합니다. 자세한 내용은 AWS SOC 1 Type II 보고서를 참조하십시오. ISO 27001 표준, 부록 A, 10.4항에서도 자세한 내용을 확인하실 수 있습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
복원력	관리 프로그램	RS-01.1	실현된 위험 이벤트의 영향을 최소화하고 테넌트에게 적절하게 알릴 수 있도록 비즈니스 연속성 및 재해 복구를 정의하는 정책, 프로세스 및 절차가 마련되어 있습니까?	AWS 비즈니스 연속성 정책 및 계획은 ISO 27001 표준에 따라 개발 및 테스트되었습니다. AWS 및 비즈니스 연속성에 대한 자세한 내용은 ISO 27001 표준, 부록 A, 14.1항과 AWS SOC 1 보고서를 참조하십시오.
복원력	영향 분석	RS-02.1	테넌트가 운영 서비스 수준 협약(SLA) 성능을 지속적으로 파악하고 보고받을 수 있도록 지원합니까?	AWS Cloudwatch는 고객이 AWS에서 실행하는 AWS 클라우드 리소스와 애플리케이션을 모니터링합니다. 자세한 내용은 aws.amazon.com/cloudwatch를 참조하십시오. AWS는 서비스 상태 대시보드에 서비스 가용성에 대한 최신 정보도 게시합니다. status.aws.amazon.com을 참조하십시오.

도메인	제어 그룹	CID	평가 질문	AWS 답변
복원력		RS-02.2	테넌트에게 표준 기반 정보 보안 측정치(CSA, CAMM 등)를 제공합니까?	
복원력		RS-02.3	고객이 SLA 성능을 지속적으로 파악하고 보고받을 수 있도록 지원합니까?	
복원력	비즈니스 연속성 계획	RS-03.1	테넌트에게 지리적 위치에 크게 구애받지 않는 호스팅 옵션을 제공합니까?	데이터 센터는 전 세계 여러 리전에 클러스터 형태로 구축됩니다. AWS는 각 리전 내의 여러 가용 영역뿐 아니라 여러 리전 내에 인스턴스를 배치하고 데이터를 저장하는 유연성을 고객들에게 제공합니다. 고객은 다수의 리전 및 가용 영역의 이점을 활용하여 AWS 아키텍처를 구축해야 합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
복원력		RS-03.2	테넌트에게 다른 공급자에 대한 인프라 서비스 failover 기능을 제공합니까?	
복원력	비즈니스 연속성 테스트	RS-04.1	지속적인 효과를 보장하기 위해 정기적으로 또는 중요 조직 또는 환경이 변경될 경우 비즈니스 연속성 계획을 테스트합니까?	AWS 비즈니스 연속성 계획은 ISO 27001 표준에 따라 개발 및 테스트되었습니다. AWS 및 비즈니스 연속성에 대한 자세한 내용은 ISO 27001 표준, 부록 A, 14.1항과 AWS SOC 1 보고서를 참조하십시오.
복원력	환경 위험	RS-05.1	예상되는 정밀 공격뿐 아니라 자연적인 원인 및 재해로 인한 손상으로부터 보호하는 물리적인 조치가 고안되었고 대책이 적용되었습니까?	AWS 데이터 센터는 환경 위험에 대한 물리적인 보호 조치를 통합합니다. 환경 위험에 대한 AWS의 물리적 보호 조치는 독립적인 감사 기관으로부터 검증을 받았으며 ISO 27002 모범 사례를 준수함을 인증받았습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 9.1항과 AWS SOC 1 Type II 보고서를 참조하십시오.
복원력	장비 위치	RS-06.1	가혹한 환경적 위험(홍수, 토네이도, 지진, 허리케인 등)의 발생 가능성이 높은 지역에 데이터 센터가 있습니까?	AWS 데이터 센터는 환경 위험에 대한 물리적인 보호 조치를 통합합니다. AWS 서비스는 고객에게 여러 가용 영역뿐 아니라 여러 리전 내에 데이터를 저장할 수 있는 유연성을 제공합니다. 고객은 다수의 리전 및 가용 영역의 이점을 활용하여 AWS 아키텍처를 구축해야 합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 9.1항과 AWS SOC 1 Type II 보고서를 참조하십시오.

도메인	제어 그룹	CID	평가 질문	AWS 답변
복원력	장비 정전	RS-07.1	유틸리티 서비스 중단(예: 정전, 네트워크 장애 등)으로부터 장비를 보호할 수 있는 보안 메커니즘과 중복성이 구현되어 있습니까?	AWS 장비는 ISO 27001 표준에 따라 중단으로부터 보호됩니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. AWS SOC 1 Type II 보고서는 오작동 또는 물리적 재해가 컴퓨터 및 데이터 센터 시설에 미치는 영향을 최소화하기 위해 마련된 컨트롤에 대한 자세한 정보를 제공합니다. http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서도 참조하십시오.
복원력	전력/통신	RS-08.1	테넌트에게 시스템 간에 데이터를 전송할 수 있는 경로를 보여 주는 문서를 제공합니까?	AWS 고객은 데이터와 서버가 위치할 물리적 리전을 지정할 수 있습니다. AWS는 법률 또는 정부기관의 요청을 준수해야 하는 경우가 아닌 이상, 통지 없이 고객이 선택한 리전에서 고객의 콘텐츠를 옮기지 않습니다. AWS SOC 1 Type II 보고서에 자세한 정보가 나와 있습니다. 또한 고객은 고객이 트래픽 라우팅을 제어하는 전용, 개인 네트워크를 통해 액세스하는 등 AWS 시설에 액세스할 수 있는 네트워크 경로를 선택할 수 있습니다.
복원력		RS-08.2	테넌트가 데이터 전송 방식과 데이터가 통과하는 법정 관할 지역을 정의할 수 있습니까?	
보안 아키텍처	고객 액세스 요건	SA-01.1	고객에게 데이터, 자산, 정보 시스템에 대한 액세스 권한을 부여하기 전에 고객 액세스에 대해 식별된 모든 보안, 계약 및 규제 요건이 계약에 따라 해결 및 수정됩니까?	AWS 고객은 준거법과 규정을 준수하는 범위 내에서 AWS를 사용할 책임이 있습니다. AWS는 산업 인증, 제3자 증명, 백서(http://aws.amazon.com/security에서 제공)를 통해 고객에게 보안 및 제어 환경을 전달하고, AWS 고객에게 직접 인증, 보고서 및 기타 관련 문서를 제공합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 6.2항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
보안 아키텍처	사용자 ID 자격 증명	SA-02.1	기존 고객 기반 SSO(Single Sign On) 솔루션 사용을 지원하거나 이러한 솔루션을 서비스에 통합합니까?	AWS Identity and Access Management(IAM) 서비스는 AWS Management Console에 ID 페더레이션을 제공합니다. 다중 요소 인증은 고객이 선택적으로 활용할 수 있는 기능입니다. 자세한 내용은 AWS 웹 사이트(http://aws.amazon.com/mfa)를 참조하십시오.
보안 아키텍처		SA-02.2	개방형 표준을 사용해 테넌트에게 인증 기능을 위임합니까?	
보안 아키텍처		SA-02.3	사용자 인증/권한 부여의 수단으로 자격 증명 연동 표준(SAML, SPML, WS-Federation 등)을 지원합니까?	

도메인	제어 그룹	CID	평가 질문	AWS 답변
보안 아키텍처		SA-02.4	사용자 액세스에 대한 지역의 법적 및 정책 제한을 적용하는 Policy Enforcement Point 기능이 있습니까?	
보안 아키텍처		SA-02.5	데이터에 대한 역할 기반 및 컨텍스트 기반 권한 부여를 지원하는 ID 관리 시스템이 마련되어 있습니까(테넌트 데이터 분류 지원)?	
보안 아키텍처		SA-02.6	테넌트에게 강력한(멀티 팩터) 사용자 액세스 인증 옵션을 제공하고 있습니까?	
보안 아키텍처		SA-02.7	테넌트가 제3자 신원 확인 서비스를 사용하도록 허용합니까?	
보안 아키텍처	데이터 보안/무결성	SA-03.1	산업 표준을 사용해 데이터 보안 아키텍처를 설계했습니까? (예: CDSA, MULITSAFE, CSA 신뢰할 수 있는 클라우드 아키텍처 표준, FedRAMP[sm] CAESARS)	AWS 데이터 보안 아키텍처는 주요 산업 표준을 통합하도록 설계되었습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 10.8항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
보안 아키텍처	애플리케이션 보안	SA-04.1	SDLC(시스템/소프트웨어 개발 주기)의 기본 보안 기능을 업계 표준(BSIMM[성숙 모델의 빌드 보안] 벤치마크, 개방형 그룹 ACS 신뢰 기술 제공업체 프레임워크, NIST 등)에 따라 구현하고 있습니까?	AWS 시스템 개발 수명 주기는 AWS 보안 팀의 공식적인 디자인 검토, 위협 모델링 및 일체의 위험 평가 등 업계 모범 사례를 통합합니다. 자세한 내용은 AWS 보안 프로세스 개요 백서를 참조하십시오. ISO 27001 표준, 부록 A, 12.5항에서도 자세한 내용을 확인하실 수 있습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
보안 아키텍처		SA-04.2	프로덕션 전에 자동 소스 코드 분석 도구를 사용해 코드 보안 결함을 탐지합니까?	
보안 아키텍처		SA-04.3	모든 소프트웨어 공급업체가 시스템/소프트웨어 개발 수명 주기(SDLC) 보안에 대한 산업 표준을 준수하는지 확인합니까?	
보안 아키텍처	데이터 무결성	SA-05.1	수동 또는 시스템 처리 오류 또는 데이터 손상을 방지하기 위한 데이터 입력 및 출력 무결성 루틴(조정 및 수정 검사)이 구현되어 있습니까?	AWS SOC 1 Type II 보고서에 설명된 것처럼 AWS 데이터 무결성 컨트롤은 전송, 저장 및 처리를 포함한 모든 단계에서 데이터 무결성이 유지됨을 합리적으로 보증합니다. ISO 27001 표준, 부록 A, 12.2항에서도 자세한 내용을 확인하실 수 있습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.

도메인	제어 그룹	CID	평가 질문	AWS 답변
보안 아키텍처	프로덕션/비 프로덕션 환경	SA-06.1	SaaS 또는 PaaS 서비스의 경우 테넌트에게 프로덕션 및 테스트 프로세스를 위한 별도의 환경을 제공합니까?	AWS 고객은 프로덕션 및 테스트 환경을 구축하고 관리할 수 있는 역량과 책임이 있습니다. AWS 웹 사이트는 AWS 서비스를 활용하여 환경을 구축할 수 있는 지침을 제공합니다(http://aws.amazon.com/documentation/).
보안 아키텍처		SA-06.2	IaaS 서비스의 경우 테넌트에게 적합한 프로덕션 및 테스트 환경을 구축할 수 있는 방법에 대한 지침을 제공합니까?	
보안 아키텍처	원격 사용자 멀티 팩터 인증	SA-07.1	모든 원격 사용자에 다중 요소 인증이 필요합니까?	다중 요소 인증은 고객이 선택적으로 활용할 수 있는 기능입니다. 자세한 내용은 AWS 웹 사이트(http://aws.amazon.com/mfa)를 참조하십시오.
보안 아키텍처	네트워크 보안	SA-08.1	IaaS 서비스의 경우 고객에게 가상화된 솔루션을 사용하여 상응하는 계층형 보안 아키텍처를 구축할 수 있는 방법에 대한 지침을 제공합니까?	AWS 웹 사이트는 AWS 공용 웹 사이트(http://aws.amazon.com/documentation/)를 통해 게시되는 여러 백서에서 계층형 보안 아키텍처 구축에 대한 지침을 제공합니다.
보안 아키텍처	조각화	SA-09.1	비즈니스 및 고객 보안 요건을 충족할 수 있도록 시스템과 네트워크 환경이 논리적으로 분리됩니까?	AWS 고객은 정의된 요건에 따라 네트워크 조각화를 관리할 책임이 있습니다. 내부적으로 AWS 네트워크 조각화는 ISO 27001 표준을 따릅니다. 자세한 내용은 ISO 27001 표준, 부록 A, 11.4항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
보안 아키텍처		SA-09.2	법률, 규제 및 계약 요건을 준수할 수 있도록 시스템과 네트워크 환경이 논리적으로 분리됩니까?	
보안 아키텍처		SA-09.3	프로덕션 환경과 비 프로덕션 환경이 분리될 수 있도록 시스템과 네트워크 환경이 논리적으로 분리됩니까?	
보안 아키텍처		SA-09.4	중요한 데이터가 보호 및 격리될 수 있도록 시스템과 네트워크 환경이 논리적으로 분리됩니까?	
보안 아키텍처	무선 보안	SA-10.1	네트워크 환경 매개 변수를 보호하기 위한 정책, 절차, 메커니즘이 확립 및 구현되었으며 권한 없는 트래픽을 제한할 수 있도록 구성되어 있습니까?	AWS 네트워크 환경을 보호하기 위한 정책, 절차 및 메커니즘이 마련되어 있습니다. AWS SOC 1 Type II 보고서에 자세한 정보가 나와 있습니다. ISO 27001 표준, 부록 A, 10.6항에서도 자세한 내용을 확인하실 수 있습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
보안 아키텍처		SA-10.2	강력한 암호화로 적절한 보안 설정을 활성화하여 인증, 전송, 벤더 기본 설정 변경을 수행할 수 있는 정책, 절차 및 메커니즘이 확립 및 구현되었습니까? (예: 암호화 키, 암호, SNMP 커뮤니티 문자열 등)	

도메인	제어 그룹	CID	평가 질문	AWS 답변
보안 아키텍처		SA-10.3	네트워크 환경을 보호하고 권한 없는(불법) 네트워크 디바이스를 탐지하여 적시에 네트워크에서 분리할 수 있는 정책, 절차 및 메커니즘이 확립 및 구현되었습니까?	
보안 아키텍처	공유 네트워크	SA-11.1	공유 네트워크 인프라를 통한 시스템 액세스는 보안 정책, 절차 및 표준에 따라 권한 있는 사람에게만 제한됩니다. 외부 엔터티와 공유하는 네트워크에는 조직 간의 네트워크 트래픽을 분리하는 데 사용되는 보상 컨트롤을 자세히 설명하는 문서화된 계획이 있습니다.	액세스는 서비스, 호스트, 네트워크 디바이스로만 엄격하게 제한되며 Amazon의 독점적인 권한 관리 시스템에서 명시적인 승인을 받아야 합니다. AWS SOC 1 Type II 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. 또한 ISO 27001 표준, 부록 A, 도메인 11을 참조하십시오. AWS는 독립 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
보안 아키텍처	클록 동기화	SA-12.1	모든 시스템이 공통 시간 참조를 사용하도록 동기화된 시간 서비스 프로토콜(예: NTP)을 활용합니까?	ISO 27001 표준에 따라 AWS 정보 시스템은 NTP(Network Time Protocol)를 통해 동기화되는 내부 시스템 클록을 사용합니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
보안 아키텍처	장비 식별	SA-13.1	알려진 장비 위치를 기반으로 연결 인증 무결성을 검증하기 위한 연결 인증 방법으로 자동 장비 식별을 사용합니까?	AWS는 ISO 27001 표준에 따라 장비 식별을 관리합니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
보안 아키텍처	감사 로깅/침입 탐지	SA-14.1	적시에 탐지, 근본 원인 분석을 통한 조사, 인시던트에 대한 대응을 원활하게 수행할 수 있도록 지원하는 파일 무결성(호스트) 및 네트워크 침입 탐지(IDS) 도구가 구현되었습니까?	AWS 인시던트 대응 프로그램(탐지, 조사 및 인시던트 대응)은 ISO 27001 표준에 따라 개발되었습니다. AWS SOC 1 Type II 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. AWS 보안 프로세스 개요 백서(http://aws.amazon.com/security 에서 제공)에도 자세한 내용이 나와 있습니다.
보안 아키텍처		SA-14.2	감사 로그에 대한 물리적 및 논리적 사용자 액세스가 권한 있는 사람에게만 허용됩니까?	
보안 아키텍처		SA-14.3	컨트롤/아키텍처/프로세스에 대한 규정 및 표준 실사 매핑이 수행되었다는 증거를 제공할 수 있습니까?	
보안 아키텍처	모바일 코드	SA-15.1	권한 있는 모바일 코드가 명확하게 정의된 보안 정책에 따라 작동할 수 있도록 모바일 코드를 설치 및 사용하기 전에 권한을 부여하고 코드 구성을 확인합니까?	AWS는 고객이 자체 요건에 따라 클라이언트 및 모바일 애플리케이션을 관리할 수 있도록 허용합니다.

도메인	제어 그룹	CID	평가 질문	AWS 답변
보안 아키텍처		SA-15.2	모든 권한 있는 모바일 코드가 실행되지 않습니까?	

부록 B: AWS의 MPAA(미국 영화 협회) 콘텐츠 보안 모델 준수

MPAA(미국 영화 협회)에서는 보호 미디어 및 콘텐츠를 안전하게 저장, 처리 및 배달하기 위한 모범 사례를 제정했습니다. MPAA 콘텐츠 보안 모범 사례에 대한 추가 정보는 http://www.fightfilmtheft.org/best-practice.html을 참조하십시오. 미디어 회사에서는 이러한 모범 사례를 콘텐츠 관리의 위험 및 감사 보안을 평가하는 방법으로 이용할 수 있습니다.
아래 표에는 2013년 1월 1일 발표된 AWS의 MPAA(미국 영화 협회) 콘텐츠 보안 모델 준수 내역이 나와 있습니다. 자세한 내용을 참조할 수 있도록 AWS 외부 감사 인증 및 보고서도 제공됩니다.
* ISO 27002 및 NIST 800-53 매핑은 *"MPAA 콘텐츠 보안 모범 사례 일반 지침 2013년 1월 1일"*에 따라 캡처한 것입니다.

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-10	경영진의 보안 의식/관리	정보 보안 프로그램 및 위험 평가 결과를 정기적으로 검토하여 경영진/소유자의 정보 보안 기능 실수를 확인합니다.	Amazon의 규제 환경은 회사의 경영진에서부터 시작됩니다. 경영진과 선임 책임자는 회사의 우선 순위와 핵심 가치 형성에 중요한 역할을 합니다. AWS는 COBIT(Control Objectives for Information and related Technology) 체계에 따라 정보 보안 체계 및 정책을 수립했으며 ISO 27002 통제, AICPA(미국 공인 회계사 협회)의 신뢰 서비스 원칙(Trust Services Principles), PCI DSS v3.1 및 NIST(국립 표준 기술 연구소) 간행물 800-53 개정 3판(연방 정보 시스템 및 조직을 위한 보안 통제 권고)에 근거하여 ISO 27001 인증 가능한 체계를 효과적으로 통합했습니다. AWS 보안 교육을 포함하여 AWS 직원의 전체적인 정기 역할 기반 교육. 준수성 감사는 직원들이 확립된 정책을 이해하고 따르도록 하기 위해 수행됩니다.	MS-1	SOC1(1.1) SOC2(S.2.3)	4.1 6.11	12.4 12.5	PM-1 PM-2
MS.S-1.0	경영진의 보안 의식/관리	경영진 관리/소유자가 승인한 정보 보안에 대한 통제 체계(예: ISO 27001)를 구현하는 정보 보안 관리 시스템을 수립합니다.						
MS-1.1	경영진의 보안 의식/관리	경영진/소유자에게 콘텐츠 보호를 위한 기업의 책임을 교육하고 알립니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-2.0	위험 관리	시설과 관련된 콘텐츠 도용 및 유출 위험을 식별하고 우선순위를 지정하기 위해 콘텐츠 워크플로우와 중요한 자산에 초점을 맞춘 공식적인 보안 위험 평가 프로세스를 개발합니다.	AWS는 적어도 1년에 한 번씩 업데이트 및 검토되는 공식적인 문서화된 위험 평가 정책을 구현했습니다. 이 정책은 목적, 범위, 역할, 책임 및 경영진의 책임감을 규정합니다. 이 정책에 따라, 모든 AWS 리전 및 회사를 포함하는 연간 위험 평가가 AWS 규정 준수 팀과 AWS 고위 경영진에 의해 실시됩니다. 또한 독립적인 감사 기관에 의해 이에 대한 인증, 증명 및 보고도 실시됩니다. 위험 관리의 목적은 AWS의 위협과 취약성을 식별하고 위협과 취약성에 위험 등급을 배정하며, 평가를 공식적으로 문서화하고 문제 해결을 위한 위험 처리 계획을 작성하는 것입니다. 위험 평가 관리는 매년 또는 연간 위험 평가 전에 새 위험 평가가 필요한 중대한 변화가 발생할 때마다 AWS 고위 경영진에 의해 검토됩니다. 고객은 자신의 데이터(콘텐츠)에 대한 소유권을 보유하며 규정 준수 요건을 충족하도록 데이터의 워크플로우와 관련된 위험을 평가하고 관리할 책임이 있습니다. AWS의 지속적 SOC, PCI DSS, ISO 27001 및 FedRAMP^{sm} 규정 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 위험 관리 프레임워크를 검토합니다.	MS-2	SOC2(S3.31, S4.2, S4.3)	4.1 4.2 7.2	12.1 12.2	CA-1 CA-2 CA-5 RA-1 RA-2 RA-3
MS-2.1	위험 관리	클라이언트 지시에 따라 보안 수준이 높은 콘텐츠를 식별합니다.						
MS-2.2	위험 관리	최소한 MPAA 모범 사례 일반 지침과 해당되는 보조 지침 및 문서에 따라 매년 또는 주요 워크플로우 변화가 발생할 때마다 내부 위험 평가를 실시하고 식별된 위험에 대한 조치를 취합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-3.0	보안 조직	보안 키 연락 지점을 식별하고 콘텐츠 및 자산 보호에 대한 역할과 책임을 공식적으로 정의합니다.	AWS는 AWS 보안 팀에서 관리하고 AWS CISO(최고 정보 보안 책임자)가 이끄는 정보 보안 조직을 구성했습니다. AWS는 보안 인식 교육을 관리하고 AWS를 지원하는 모든 정보 시스템 사용자에게 제공합니다. 이 연간 보안 인식 교육에는 보안 및 인식 목적 교육, 모든 AWS 정책 위치, AWS 사고 대응 절차(내부 및 외부 보안 사고 보고 방법에 대한 지침 포함)가포함됩니다. AWS 내 시스템에는 주요 운영 및 보안 측정치를 모니터링하기 위한 계측 기능이 광범위하게 설치되어 있습니다. 주요 측정치가 초기 경고 임계값을 초과하는 경우 운영 관리 담당자에게 자동으로 알리도록 경보가 구성되어 있습니다. 임계값을 초과하면 AWS 사고 대응 프로세스가 시작됩니다. Amazon 사고 대응 팀은 비즈니스에 영향을 미치는 이벤트 발생 시 업계 표준 진단 절차를 이용하여 문제를 해결합니다. 직원이 연중무휴 24시간 근무하며 사고를 감지하고 해결책에 대한 영향을 관리합니다. SOC, PCI DSS, ISO 27001 및 FedRAMP^{sm} 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 역할 및 책임을 검토합니다.	MS-3	SOC1(1.1) SOC2(S.2.3)	6.1.3	12.4 12.5	PM-2
MS.S-3.0	보안 조직	사전 모니터링 정보 시스템 및 물리적 보안을 책임질 보안 팀을 구성하여 의심스러운 활동을 식별하고 이에 대응합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-4.0	정책 및 절차	자산 및 콘텐츠 보안에 대한 정책과 절차를 확립합니다. 정책은 최소한 다음 항목을 포함해야 합니다. • 인사관리 정책 • 사용 제한(예: 소셜 네트워킹, 인트라넷, 전화 등) • 자산 분류 • 자산 취급 정책 • 디지털 기록 디바이스(예: 스마트폰, 디지털 카메라, 캠코더) • 예외 정책(예: 정책 위반 기록 절차) • 암호 관리(예: 암호 최소 길이, 화면보호기) • 시설에서 고객 자산 제거 금지 • 시스템 변경 관리 • 내부고발자 정책 • 제재 정책(예: 징계 정책)	AWS는 COBIT(Control Objectives for Information and related Technology) 체계에 따라 정보 보안 체계 및 정책을 수립했으며 ISO 27002 통제, AICPA(미국 공인 회계사 협회)의 신뢰 서비스 원칙(Trust Services Principles), PCI DSS v3.1 및 NIST(국립 표준 기술 연구소) 간행물 800-53 개정 3판(연방 정보 시스템 및 조직을 위한 보안 통제 권고)에 근거하여 ISO 27001 인증 가능한 체계를 효과적으로 통합했습니다. AWS는 보안 인식 교육을 관리하고 AWS를 지원하는 모든 정보 시스템 사용자에게 제공합니다. 이 연간 보안 인식 교육에는 보안 및 인식 목적 교육, 모든 AWS 정책 위치, AWS 사고 대응 절차(내부 및 외부 보안 사고 보고 방법에 대한 지침 포함)가 포함됩니다. AWS의 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP^{sm} 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 정책, 절차 및 관련 교육 프로그램을 검토합니다.	MS-4	SOC1(1.2) SOC2(S1.1, S1.2, S1.3, S2.2, S2.3, S2.4, S3.7 S3.8, S3.9, S4.2, S4.3))	5.1.1 5.1.2 6.1.1 8.1.3 8.2.2	3.1 8.5 12.1 12.2 12.3 12.6	AT-1 AT-2 AT-3 AT-4 PL-1 PS-7

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS.S-4.0	정책 및 절차	시설에서 처리하는 콘텐츠와 관련된 심층 교육을 제공합니다.						
MS-4.1	정책 및 절차	최소한 일년에 한 번 이상 보안 정책과 절차를 검토하고 업데이트합니다.						
MS.S-4.1	정책 및 절차	암호화된 콘텐츠를 처리하는 모든 개인에 대해 암호화 및 키 관리와 관련된 애플리케이션 및 프로세스를 교육합니다.						
MS-4.2	정책 및 절차	모든 정책, 절차 및/또는 고객 요건 및 업데이트에 따라 모든 직원(예: 정직원, 계약직, 인턴)과 타사 작업자(예: 계약업체, 프리랜서, 임시 대리인)는 리소스 사용 후 로그아웃을 해야 합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-4.3	정책 및 절차	보안 인식 프로그램을 개발하고 정기적으로 업데이트하며 최소한 다음 내용을 포함하는 보안 정책 및 절차에 대해 고용 시 또는 매년(고용 후) 회사 직원 및 타사 작업자를 교육합니다. • IT 보안 정책 및 절차 • 콘텐츠/자산 보안 및 취급 • 보안 인시던트 보고 및 에스컬레이션 • 징계 조치						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-5.0	인시던트 대응	보안 인시던트가 탐지 및 보고된 경우 취해야 할 조치를 설명하는 공식적인 인시던트 대응 계획을 수립합니다.	AWS는 문서화된 공식적인 사고 대응 정책 및 프로그램을 구현했습니다. 이 정책은 목적, 범위, 역할, 책임 및 경영진의 책임감을 규정합니다. AWS에서는 3단계 접근 방식에 따라 인시던트를 관리합니다. 1. 활성화 및 알림 단계: AWS에 대한 인시던트는 이벤트 감지로 시작됩니다. 이벤트는 다음과 같은 여러 방법을 통해 감지될 수 있습니다. a. 측정치 및 경보 - AWS는 예외 상황 인식 기능을 관리하며 실시간 측정치 및 서비스 대시보드를 연중무휴 24시간 모니터링하고 경보를 울림으로써 대부분의 문제를 신속히 감지합니다. 사고의 대부분이 이러한 방식으로 감지됩니다. AWS에서는 조기 표시등 경보를 이용하여 고객에게 궁극적으로 영향을 미칠 수 있는 문제를 사전에 식별합니다. b. AWS 직원이 입력한 문제 티켓 c. 연중무휴 하루 24시간 기술 지원 핫라인으로의 전화. 이벤트가 사고 기준에 부합되면 관련 대기 지원 엔지니어가 AWS 이벤트 관리 도구 시스템을 이용하여 개입을 시작하고 관련 프로그램 해결자(예: 보안 팀)를 호출합니다. 해결자는 사고를 분석하여 추가 해결자 개입이 필요한지 여부와 해당 근본 원인을 파악합니다. 2. 복구 단계 - 해결 담당자가 고장 수리를 통해 사고를 해결합니다. 문제 해결 및 고장 수리를 거쳐 해당 구성 요소를 해결하고 나면, 통화 리더가 후속 조치 문서화와 후속 조치 행동의 다음 단계를 배정하고 통화 개입을 종료합니다.	MS-5	SOC 1(8.2) SOC 2(S2.4, S3.5, S3.7, S3.9)	13.1 13.1.1 13.2.2	12.9	IR-1 IR-2 IR-4 IR-5 IR-6 IR-7 IR-8
MS-5.1	인시던트 대응	보안 인시던트 탐지, 분석 및 해결을 담당하는 보안 인시던트 대응 팀을 식별합니다.						
MS-5.2	인시던트 대응	개인이 탐지된 인시던트를 보안 인시던트 대응 팀에 보고할 수 있는 보안 인시던트 보고 프로세스를 확립합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-5.3	인시던트 대응	콘텐츠가 누출, 도난 또는 손상되었을 수 있는 고객에게 사고 사실을 즉시 알리고 관리 팀과 고객 간의 사후 분석 회의가 개최됩니다.	3. 재구성 단계 – 관련된 수리 활동이 완료되면 통화 리더가 복구 단계의 완료를 선언합니다. 관련 팀에 사고에 대한 사후 분석과 근본 원인 심층 분석이 배정됩니다. 해당하는 고위 경영진이 사후 분석 결과를 검토하고, 설계 변경 등 관련된 조치를 COE(오류 수정) 문서에 기록한 다음 완료될 때까지 추적합니다. 위에 설명된 내부 통신 메커니즘 외에도, AWS는 고객 기반 및 커뮤니티를 지원하기 위한 다양한 통신 방법을 구현했습니다. 고객 지원 팀이 고객의 경험에 영향을 미치는 운영 문제를 전달받을 수 있도록 방법이 마련되어 있습니다. 고객 지원 팀에서 제공 및 관리하는 "서비스 상태 대시보드"는 고객에게 광범위하게 영향을 미칠 수 있는 모든 문제를 알려줍니다. AWS의 SOC, PCI DSS, ISO 27001 및 FedRAMP^{sm} 규정 준수에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 인시던트 관리 프로그램을 검토합니다.					

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-6.0	워크플로우	각 프로세스에서 콘텐츠 및 승인 체크포인트 추적과 다음과 같은 물리적 및 디지털 콘텐츠를 위한 프로세스를 포함하는 워크플로우를 문서화합니다. • 제공 • 입력 • 이동 • 보관 • 전송 위치로 다시 보내기 • 사이트에서 제거 • 폐기	고유의 게스트 운영 체제, 소프트웨어, 애플리케이션 및 데이터의 소유권과 관리 권한이 고객에게 있으므로 콘텐츠(데이터) 워크플로우 문서화는 AWS 고객의 책임입니다.	MS-6	AWS에 해당되지 않음	AWS에 해당되지 않음	AWS에 해당되지 않음	AWS에 해당되지 않음
MS-6.1	워크플로우	콘텐츠 워크플로와 관련된 위험을 예방, 탐지 및 수정하는 주요 컨트롤의 효과를 식별, 구현 및 평가합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-7.0	업무 분담	콘텐츠 워크플로우 내에서 임무를 분리하고 분리가 불가능한 경우 이를 상쇄하는 통제 수단을 구현하고 문서화합니다.	고유의 게스트 운영 체제, 소프트웨어, 애플리케이션 및 데이터의 소유권과 관리 권한이 고객에게 있으므로 콘텐츠(데이터) 워크플로우의 의무를 분리하는 일은 AWS 고객의 책임입니다. AWS에 디지털 자산 및 워크플로우를 호스팅하는 고객은 해당되는 경우 AWS Identity and Access Management를 활용하여 디지털 자산 및 콘텐츠 전송에 대한 의무 분리와 관련된 제어 요구 사항을 구현할 수 있습니다. 고객은 AWS CloudTrail을 활용하여 해당되는 경우 감사 로그를 보다 쉽게 검토 및 보존할 수 있습니다.	MS-7	AWS에 해당되지 않음	AWS에 해당되지 않음	AWS에 해당되지 않음	AWS에 해당되지 않음

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-8.0	배경 조회	모든 직원과 타사 작업자에 대해 배경 조회를 실시합니다.	AWS는 준거법에서 허용하는 범위 내에서 채용 전 적격 심사 관행의 일환으로 직원의 직위와 AWS 시설에 대한 접근 권한에 따라 범죄 경력 조회를 실시합니다. AWS의 지속적 SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 규정 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 배경 조회 프로그램을 검토합니다.	MS-8	SOC 2(S3.11)	8.1.2	12.7	PS-3
MS-9.0	기밀 협약	회사 직원과 타사 작업자는 모두 채용 시 그리고 그 이후로 매년 콘텐츠 취급 및 보호에 대한 요구 사항이 포함된 기밀 협약(예: 비밀 유지)에 서명해야 합니다.	Amazon 법률 자문 팀이 Amazon NDA(Non-Disclosure Agreement)를 관리하고 AWS 비즈니스 요구를 반영하기 위해 정기적으로 개정합니다. ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS의 NDA(비밀 유지 계약) 사용을 검토합니다.	MS-9		6.1.5 8.2.3 8.3.3		PL-4 PS-4 PS-6 PS-8 SA-9
MS-9.1	기밀 협약	회사 직원과 타사 작업자는 모두 고용 또는 계약 종료 시 소유하고 있던 콘텐츠 및 고객 정보를 모두 반납해야 합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-10.0	제3자 사용 및 조회	콘텐츠를 취급하는 모든 타사 작업자는 고용 시 기밀 협약(예: 비밀 유지)에 서명해야 합니다.	온보딩 프로세스의 일부로서 AWS 시스템 및 디바이스를 지원하는 모든 개인은 액세스 권한이 부여되기에 앞서 비밀 유지 계약서에 서명합니다. 추가로, 오리엔테이션 교육의 일부로서 개인은 Amazon 기업 행동강령 및 윤리강령(행동강령) 정책을 읽고 수락해야 합니다. AWS 시스템 및 디바이스를 지원하는 타사 공급자에 대한 개인 보안 요구 사항이 모회사인 AWS, Amzon.com 및 해당하는 타사 공급자 간의 상호 비밀 유지 계약서에 규정되어 있습니다. Amazon 법률 지문 및 AWS 조달 팀은 타사 공급자와의 계약서에 AWS 타사 공급자 개인 보안 요구 사항을 정의합니다. AWS 정보를 취급하는 모든 개인은 최소한 고용 전 배경 확인을 위한 선별 프로세스를 통과해야 하며, AWS NDA(비밀 유지 계약서)에 서명한 후 AWS 정보에 대한 액세스 권한을 받게 됩니다. 또한 PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 타사 요구 사항을 검토합니다.	MS-10		6.1.5 6.2 6.2.3 10.2 11.1 11.2	12.8	PL-4 PS-4 PS-6 PS-7 PS-8 SA-9
MS.S-10.0	제3자 사용 및 조회	물리적 자산에 대한 타사 스토리지 공급자 사용에 관한 정보를 고객에게 전달						
MS-10.1	제3자 사용 및 조회	제3자 계약의 보안 요구 사항을 포함하십시오.						
MS.S-10.1	제3자 사용 및 조회	국제(미국에서/미국으로) 운송 회사는 "테러리즘에 대한 세관-무역 동반자 관계(Customs-Trade Partnership Against Terrorism, CTPAT)" 인증을 받아야 합니다.						
MS-10.2	제3자 사용 및 조회	고용 종료 시 자산을 회수하고 제3자 작업자에게 기밀 협약과 계약 보안 요구 사항을 알리는 프로세스를 구현하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS.S-10.2	제3자 사용 및 조회	매년마다 그리고 해당 공급업체에서 위치를 변경하거나 추가 서비스를 제공할 때마다 운송 및 포장 공급업체를 재평가합니다.						
MS-10.3	제3자 사용 및 조회	해당하는 경우(예: 택배 서비스) 타사 작업자가 계약을 체결하고 보험에 가입해야 합니다.						
MS.S-10.3	제3자 사용 및 조회	타사 콘텐츠 전송 시스템 및 웹 사이트에 대한 액세스를 매년 검토합니다.						
MS-10.4	제3자 사용 및 조회	업무에 필요하지 않은 경우 콘텐츠/프로덕션 영역에 대한 제3자의 접근을 제한하십시오.						
MS.S-10.4	제3자 사용 및 조회	보안 실사 활동(예: 보안 평가, 자체 평가 설문지)을, 중요 콘텐츠를 처리하는 타사 작업자에 대한 선정 및 채용 프로세스의 일부로서 통합합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-10.5	제3자 사용 및 조회	또 다른 타사가 콘텐츠를 취급할 경우 타사는 이를 고객에게 알려야 합니다.						
PS-1.0	입구/출구	시설에 안내 데스크 너머로 분리된 접근 통제 구역이 없을 경우 항상 모든 입구/출구를 잠가야 합니다.	AWS에서는 데이터 센터 액세스 관련 멀티 팩터 인증 메커니즘과 권한이 부여된 개인만 AWS 데이터 센터에 출입할 수 있도록 하기 위해 설계된 추가 보안 메커니즘을 이용합니다. 권한이 부여된 개인은 카드 리더에 자신의 배지를 사용하고 고유 PIN을 입력해야만 권한이 부여된 해당 시설 및 작업실에 접근할 수 있습니다. 데이터 센터에 대한 물리적 접근에는 AWS의 전자 액세스 제어 시스템이 적용되는데, 이 시스템은 건물/작업실 입실용 카드 리더 및 PIN 패드와 건물/작업실 퇴실 전용 카드 리더로 구성됩니다. 건물/작업실 퇴실용 카드 리더 사용 적용은 부정 출입 방지 기능을 제공하여 권한이 없는 사람이 권한이 있는 사람과 함께 들어오거나 배지 없이 입실할 수 없도록 합니다. 이러한 액세스 제어 시스템 외에도, 주요 입구, 로딩 독, 천장 문/해치를 비롯한 AWS 데이터 센터의 모든 입구가 침입 탐지 디바이스로 보호되므로 문을 강제로 열거나 열림 상태로 유지되는 경우 경보음이 울립니다. AWS 데이터 센터는 전자 메커니즘 외에도 건물 내/외부에는 연중무휴 24시간 교육을 받은 보안 요원이 상주하고 있습니다. 시스템 경계 내에서 데이터 센터에 대한 접근은 알아야 할 필요를 기준으로만 허가되며 모든 물리적 접근 요청은 해당 AAM(영역 접근 관리자)의검토 및 승인을 받아야 합니다.	PS-1	SOC 1(5.5) SOC 2(S3.3, S3.4)	9.1.1 9.1.2	9.1	PE-3 PE-6
PS.S-1.0	입구/출구	모든 정규 입구/출구 지점에 보안 요원 상주						
PS-1.1	입구/출구	콘텐츠 영역을 다른 시설 영역(예: 관리 사무실)으로부터 분리하여 콘텐츠가 처리되는 영역에 대한 접근을 제어합니다.						
PS.S-1.1	입구/출구	모든 로딩 독 문을 잠그고 경보를 설치하며 사용 중 로딩 독 문을 모니터링합니다.						
PS.S-1.2	입구/출구	트럭 운전자가 시설의 다른 영역에서 들어올 수 없도록 트럭 운전자의 입구를 분리합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-1.3	입구/출구	임의 일정에 따라 일일 보안 순찰 프로세스를 구현하고 순찰 결과를 일지에 기록합니다.	SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 물리적 보안 메커니즘을 검토합니다.					
PS.S-1.4	입구/출구	보안 요원 교대 중에 감지된 모든 사고를 기록, 조사 및 해결합니다.						
PS-2.0	방문자 진입/진출	다음을 포함한 자세한 방문자 로그를 보관하십시오. • 이름 • 회사 • 들어온 시간/나간 시간 • 방문한 개인/단체 • 방문자의 서명 • 할당된 배지 번호	AWS 데이터 센터는 정체 불명의 시설에 상주하며 대중에게 공개되어 있지 않습니다. 물리적 접근은 주변과 건물 입구에서 모두 철저하게 제어됩니다. AWS는 긴급 수리 같은 합법적인 업무 목적으로 이러한 권한이 필요한 공급업체, 계약직원 및 방문자에게만 데이터 센터 접근 권한 및 정보를 제공합니다. 데이터 센터의 모든 방문자는 해당 AAM(영역 접근 관리자)로부터 사전 승인을 얻어야 하며 AWS 티켓 관리 시스템에 기록되어야 합니다. 방문자는 데이터 센터에 도착하면 신분증을 제출하고 서명해야 합니다. 그러고 나면 방문자 배치가 발급됩니다. 방문자는 데이터 센터에 있는 동안 계속적으로 정규 직원의 안내를 받습니다. SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 물리적 보안 메커니즘을 검토합니다.	PS-2	SOC 1(5.1) SOC 2(S3.3, S3.4)	9.1.2	9.2 9.4	PE-3 PE-7
PS-2.1	방문자 진입/진출	각 방문자에게 식별 배지 또는 스티커를 나눠 주고 항상 잘 보이게 부착하도록 하며 나갈 때 배지를 회수하십시오.						
PS-2.2	방문자 진입/진출	방문자에게 콘텐츠/프로덕션 영역에 대한 전자 접근권을 부여하지 마십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-2.3	방문자 진입/진출	현장 또는 콘텐츠/프로덕션 영역에 있는 동안 최소한 권한 있는 직원이 방문자와 동행해야 합니다.						
PS-3.0	식별	직원과 장기 근무하는 타사 작업자(예: 경비)에게 사진이 포함된 신분증을 발급하고 항상 신분증을 확인받고 잘 보이게 휴대하도록 하십시오.	AWS는 직원이 사진이 포함된 전자 액세스 카드를 이용해 장기간 데이터 센터에 접근할 수 있도록 승인합니다. SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 물리적 보안 메커니즘을 검토합니다.	PS-3	SOC 1(5.1) SOC 2(S3.3 , S3.4)	9.1.2	9.2 9.4	PE-3
PS-4.0	주변 보안	조직의 위험 평가에서 식별된 대로 시설이 노출될 수 있는 위험을 해결하는 주변 보안 컨트롤을 구현하십시오.	데이터 센터에 대한 물리적 접근에는 AWS의 전자 액세스 제어 시스템이 적용되는데, 이 시스템은 건물/작업실 입실용 카드 리더 및 PIN 패드와 건물/작업실 퇴실 전용 카드 리더로 구성됩니다. 건물/작업실 퇴실용 카드 리더 사용 적용은 부정 출입 방지 기능을 제공하여 권한이 없는 사람이 권한이 있는 사람과 함께 들어오거나 배지 없이 입실할 수 없도록 합니다. 이러한 액세스 제어 시스템 외에도, 주요 입구, 로딩 독, 천장 문/해치를 비롯한 AWS 데이터 센터의 모든 입구가 침입 탐지 디바이스로 보호되므로 문을 강제로 열거나 열림 상태로 유지되는 경우 경보음이 울립니다. AWS 데이터 센터는 전자 메커니즘 외에도 건물 내/외부에는 연중무휴 24시간 교육을 받은 보안 요원이 상주하고 있습니다.	PS-4	SOC 1(5.5) SOC 2(S3.3 , S3.4)	9.1.1	9.1	PE-3

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-4.0	주변 보안	추가 주변 안전 보호물(예: 펜스, 차량 바리케이드)을 설치하여 사내 환경으로의 무단 접근의 위험을 낮춥니다.	시스템 경계 내에서 데이터 센터에 대한 접근은 필지 방식으로만 허가되며 모든 물리적 접근 요청은 해당 AAM(영역 접근 관리자)의 검토 및 승인을 받아야 합니다. SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 물리적 보안 메커니즘을 검토합니다.					
PS.S-4.1	주변 보안	항상 주변 출입문을 잠그고 현장 직원에게 원격 잠금 해제 기능 처리를 전담시킵니다.						
PS.S-4.2	주변 보안	주변 입구에 보안 요원을 상주시키고 차량의 시설 캠퍼스 진입을 허용하는 프로세스(예: 전자 게이트 암, 주차증)를 구현합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-5.0	경보	모든 입구/출구(비상구 포함), 적재장, 비상계단, 제한 구역(예: 금고, 서버/기계실)에 적용되는 중앙 집중식 가청 경보 시스템을 설치하십시오.	주요 입구, 로딩 독, 천장 문/해치를 비롯한 AWS 데이터 센터의 모든 입구는 침입 탐지 디바이스로 보호되므로 문이 강제로 열리거나 열림 상태로 유지되는 경우 경보음이 울리고 AWS 중앙 물리 보안 모니터링에도 경보가 발생합니다. AWS 데이터 센터는 전자 메커니즘 외에도 건물 내/외부에는 연중무휴 24시간 교육을 받은 보안 요원이 상주하고 있습니다. 모든 경보는 보안 요원이 조사하며 모든 사고에 대한 근본 원인이 기록됩니다. 모든 경보는 대응이 SLA 시간 내에서 이루어지지 않을 경우 자동 에스컬레이션으로 설정됩니다. 시스템 경계 내에서 데이터 센터에 대한 접근은 필지 방식으로만 허가되며 모든 물리적 접근 요청은 해당 AAM(영역 접근 관리자)의 검토 및 승인을 받아야 합니다. SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 물리적 보안 메커니즘을 검토합니다.	PS-5	SOC 1(5.5) SOC 2(S3.3, S3.4)	9.1	9.1	PE-3 PE-6
PS-5.1	경보	에스컬레이션 알림이 보안 담당 직원에게 직접 전달되고 중앙 보안 그룹 또는 제3자가 모니터링할 수 있도록 경보를 구성하십시오.						
PS-5.2	경보	경보 시스템에 접근해야 하는 직원에게 고유한 경보 및 경보 해제 코드를 부여하고 그 외의 직원은 접근을 제한하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-5.3	경보	매년 경보 시스템을 실행하고 해제할 수 있는 사용자 목록을 검토하십시오.						
PS-5.4	경보	6개월마다 경보 시스템을 테스트하십시오.						
PS-5.5	경보	제한 구역(예: 금고, 서버/기계실)에 동작 감지기를 설치하고 효과적으로 배치하며 해당 보안 직원 및/또는 제3자에게 경보를 전달하도록 구성하십시오.						
PS-5.6	경보	중요 입구/출구가 미리 정해진 시간(예: 60초)보다 오랫동안 열려 있을 경우 알릴 수 있도록 콘텐츠/프로덕션 영역에 도어 비례제어 경보를 설치하십시오.						
PS-6.0	승인	시설 접근을 관리하고 접근 권한 변경 기록을 보관하는 프로세스를 구현하고 문서화하십시오.	데이터 센터에 대한 물리적 접근에는 AWS의 전자 액세스 제어 시스템이 적용되는데, 이 시스템은 건물/작업실 입실용 카드 리더 및 PIN 패드와 건물/작업실 퇴실 전용 카드 리더로 구성됩니다. 건물/작업실 퇴실용 카드 리더 사용 적용은 부정 출입 방지 기능을 제공하여 권한이 없는 사람이 권한이 있는 사람과 함께 들어오거나 배지 없이 입실할 수 없도록 합니다.	PS-4	SOC 1(5.3, 5.5) SOC 2(S3.3, S3.4, S5.3)	11.2 11.2.4	9.1	PE-1 PE-2 PE-3 PE-4 PE-5

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-6.0	승인	매월 그리고 회사 직원 및/또는 타사 작업자의 역할 또는 고용 상태가 변경될 때마다 제한된 영역(예: 볼트, 금고)에 대한 접근을 검토합니다.	이러한 액세스 제어 시스템 외에도, 주요 입구, 로딩 독, 천장 문/해치를 비롯한 AWS 데이터 센터의 모든 입구가 침입 탐지 디바이스로 보호되므로 문을 강제로 열거나 열림 상태로 유지되는 경우 경보음이 울립니다. AWS 데이터 센터는 전자 메커니즘 외에도 건물 내/외부에는 연중무휴 24시간 교육을 받은 보안 요원이 상주하고 있습니다. 시스템 경계 내에서 데이터 센터에 대한 접근은 필지 방식으로만 허가되며 모든 물리적 접근 요청은 해당 AAM(영역 접근 관리자)의 검토 및 승인을 받아야 합니다. SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 물리적 보안 메커니즘을 검토합니다.					
PS-6.1	승인	프로덕션 시스템에 대한 접근을 권한 있는 사람으로만 제한합니다.						
PS-6.2	승인	분기마다, 또한 직원 및/또는 타사 작업자의 역할 또는 고용 상태가 변경된 경우 제한 구역(예: 금고, 서버/기계실)에 대한 접근을 검토하십시오.						
PS-7.0	전자 액세스	시설 전체에 모든 입구/출구 및 콘텐츠가 보관, 전송 또는 처리되는 모든 영역에 대해 전자 액세스를 구현하십시오.	데이터 센터에 대한 물리적 접근에는 AWS의 전자 액세스 제어 시스템이 적용되는데, 이 시스템은 건물/작업실 입실용 카드 리더 및 PIN 패드와 건물/작업실 퇴실 전용 카드 리더로 구성됩니다. 건물/작업실 퇴실용 카드 리더 사용 적용은 부정 출입 방지 기능을 제공하여 권한이 없는 사람이 권한이 있는 사람과 함께 들어오거나 배지 없이 입실할 수 없도록 합니다. 배지 생성 및 인쇄 기능은 조직적으로 강제 적용되며 핵심 보안 요원으로 제한됩니다. 모든 배지는 일정 기간 동안만 활성화되며 배지 만료 날짜를 연장하려면 먼저 재승인을 받아야 합니다.	MS-9	SOC 1(5.3, 5.5) SOC 2(S3.3, S3.4, S5.3	9.1.2 9.1.3 11.2	9.1	PE-2 PE-3 PE-7
PS.S-7.0	전자 액세스	복제와 마스터링에 대해 각각 별도의 보관실을 설정합니다.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-7.1	전자 액세스	전자 액세스 시스템 관리는 담당자에게만 허용하십시오.	SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 물리적 보안 메커니즘을 검토합니다.					
PS-7.2	전자 액세스	빈 카드는 잠금장치가 있는 캐비닛에 보관하고, 직원에게 키 카드를 할당하기 전에 키 카드가 비활성화되어 있는지 확인하십시오.						
PS-7.3	전자 액세스	분실된 키 카드를 시스템에서 비활성화한 후에 새 키 카드를 발급하십시오.						
PS-7.4	전자 액세스	제3자에게 승인된 기간에 따라 만료 날짜(예: 90일)가 설정된 액세스 카드를 발급하십시오.						
PS-8.0	키	마스터 키는 권한 있는 사람(예: 소유자, 시설 관리자)에게만 배포하십시오.	시설 마스터 키 관리 절차를 포함한 물리적 보안 프로세스 및 절차는 AWS 물리적 보안 직원이 운영, 관리 및 실행합니다.	PS-8	SOC 1(5.5) SOC 2(S3.3, S3.4, S5.3	7.1.1 9.1.2 9.1.3	9.1	PE-2 PE-3 CM-8

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-8.1	키	마스터 키 배포를 추적 및 모니터링할 수 있는 체크인/체크아웃 프로세스를 구현하십시오.	SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 역할 및 책임을 검토합니다.					
PS-8.2	키	외부 입구/출구에 지정된 기술자만이 키를 복제할 수 있습니다.						
PS-8.3	키	분기마다 시설 입구/출구 키를 포함해 마스터 키와 제한 구역 키의 재고를 확인하십시오.						
PS-9.0	카메라	모든 시설 입구/출구와 제한 구역을 녹화하는 CCTV 시스템을 설치하십시오.	건물 주변과 진입점에서 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단을 활용하여 전문 보안 직원이 물리적인 액세스를 통제합니다. 서버 위치에 접근할 수 있는 물리적 액세스 지점은 AWS 데이터 센터 물리적 보안 정책에 정의된 대로 폐쇄 회로 TV 카메라(CCTV)로 촬영됩니다. 법률 또는 계약 의무 조항에서 30일로 제한하지 않은 경우 영상은 90일간 보관됩니다.	PS-9	SOC 1(5.4) SOC 2(S3.3)	9.1.2 9.1.3 10.10.6	9.1	PE-2 PE-3 PE-6
PS.S-9.0	카메라	매일 카메라 위치, 이미지 품질, 프레임 속도 및 보존 상태를 검토합니다.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-9.1	카메라	적어도 일주일에 한 번씩은 카메라 위치, 이미지 품질, 조명 상태, 프레임 속도 및 감시 화면의 적정 보존 상태를 검토합니다.	SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 물리적 보안 메커니즘을 검토합니다.					
PS.S-9.1	카메라	운영 시간 동안 감시 화면을 모니터링하고 감지된 보안 사고를 즉시 조사하는 직원 또는 직원 그룹을 배정합니다.						
PS-9.2	카메라	시스템 관리/모니터링 담당자에게만 CCTV 콘솔과 CCTV 장비(예: DVR)에 대한 물리적 및 논리적 접근을 허용하십시오.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-9.3	카메라	카메라 장면에 정확한 날짜 및 타임스탬프가 포함되어 있는지 확인하십시오.						
PS-10.0	로깅 및 모니터링	제한 구역에 대한 전자 액세스를 기록하고 검토하여 의심스러운 사건이 있는지 살피십시오.	건물 주변과 진입점에서 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단을 활용하여 전문 보안 직원이 물리적인 액세스를 통제합니다. 주요 입구, 로딩 독, 천장 문/해치를 비롯한 AWS 데이터 센터의 모든 입구는 침입 탐지 디바이스로 보호되므로 문이 강제로 열리거나 열림 상태로 유지되는 경우 경보음이 울리고 AWS 중앙 물리 보안 모니터링에도 경보가 발생합니다. AWS 데이터 센터는 전자 메커니즘 외에도 건물 내/외부에는 연중무휴 24시간 교육을 받은 보안 요원이 상주하고 있습니다. 모든 경보는 보안 요원이 조사하며 모든 사고에 대한 근본 원인이 기록됩니다. 모든 경보는 대응이 SLA 시간 내에서 이루어지지 않을 경우 자동 에스컬레이션으로 설정됩니다. 서버 위치에 접근할 수 있는 물리적 액세스 지점은 AWS 데이터 센터 물리적 보안 정책에 정의된 대로 폐쇄 회로 TV 카메라(CCTV)로 촬영됩니다. 법률 또는 계약 의무 조항에서 30일로 제한하지 않은 경우 영상은 90일간 보관됩니다. SOC, PCI DSS, ISO 27001 및 FedRAMP^{sm} 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 물리적 보안 메커니즘을 검토합니다.	PS-10	SOC 1(5.3, 5.5) SOC 2(S3.3, S3.4, S5.3)	10.10.2 10.10.3 13.1	9.1	AU-3 AU-6 AU-9 AU-11
PS.S-10.0	로깅 및 모니터링	해당되는 경우 다음 영역에 대한 전자 액세스 로그를 매주 한 번씩 검토합니다. • 마스터/스탬퍼 볼트 • 사전 마스터링 • 서버/기계실 • 스크랩실 • 보안 케이지						
PS-10.1	로깅 및 모니터링	탐지된 의심스러운 전자 액세스 활동을 조사하십시오.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-10.2	로깅 및 모니터링	확인된 모든 전자 액세스 사건을 지속적으로 기록하고 수행한 후속 조치 활동 문서를 함께 보관하십시오.						
PS-10.3	로깅 및 모니터링	CCTV 감시 장면과 전자 액세스 로그를 안전한 위치에 최소한 90일간, 또는 법에서 허용한 최대 기간 동안 보관하십시오.						
PS-11.0	검색	고용 시 직원과 제3자 작업자에게 가방과 짐을 무작위로 검색할 수 있으며 시설 정책에 검색을 규정한 조항이 있음을 알리십시오.	AWS 물리적 보안 정책에 따라, AWS에는 문제 발생 시 가방과 화물을 수색할 수 있는 권리가 있습니다. SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 물리적 보안 메커니즘을 검토합니다.	PS-11		8.1.3		

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-11.0	검색	다음을 포함하여 모든 시설 개인 및 방문자에 해당되는 퇴실 수색 프로세스를 구현합니다. • 검사를 위해 모든 외투, 모자 및 벨트 탈의 • 주머니의 모든 내용물 공개 • 보안 감독 하에서 자체 몸수색 실시 • 모든 가방에 대한 철저한 검사 • 랩톱의 CD/DVD 트레이 검사 • 검색 대상자로부터 반경 3인치 이내에서 휴대용 금속 탐지기로 개인 스캔						
PS.S-11.1	검색	개인이 디지털 레코딩 디바이스를 휴대한 채로 시설에 출입할 수 없도록 하고 이러한 디바이스에 대한 수색을 퇴실 수색 절차의 일부로서 포함합니다.						
PS.S-11.2	검색	프로덕션 영역으로 유입되는 모든 음식물에 대해 투명 비닐 봉지 및 음식 용기의 사용을 적용합니다.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-11.3	검색	너무 큰 의류(예: 배기 바지, 오버사이즈 후드 티셔츠)의 착용을 금지하는 복장 규정 정책을 구현합니다.						
PS.S-11.4	검색	번호, 훼손 방지 스티커/홀로그램을 사용하여 시설 반입/반출이 가능한 승인된 디바이스를 식별합니다.						
PS.S-11.5	검색	퇴실 수색 절차를 테스트하는 프로세스를 구현합니다.						
PS.S-11.6	검색	시설 주차장에서 나올 때 임의 차량 수색 프로세스를 실시합니다.						
PS.S-11.7	검색	매우 중요한 콘텐츠를 처리하는 복제 라인을 분리하고 분리된 영역에서 나올 때 수색을 실시합니다.						
PS.S-11.8	검색	보안 요원 활동을 모니터링하기 위한 추가 제어 수단을 구현합니다.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-12.0	재고 추적	물리적 자산(예: 고객 자산 및 새로 생성된 자산)을 상세하게 추적할 수 있는 콘텐츠 자산 관리 시스템을 구현하십시오.	콘텐츠 자산 관리는 AWS 고객이 소유, 구현 및 운영합니다. 물리적 사산의 재고 추적을 구현하는 일은 고객의 책임입니다. AWS 데이터 센터 환경의 경우, 데이터 센터로 배송되고 데이터 센터에서 수령하는 서버, 랙, 네트워크 디바이스, 하드 드라이브, 시스템 하드웨어 구성 요소 및 건축 자재를 포함하는(이에 제한되지 않음) 모든 새 정보 시스템 구성 요소는 사전에 데이터 센터 관리자에게 알려 승인을 받아야 합니다. 물품은 각 AWS 데이터 센터의 로딩 독으로 배달되며 화물의 손상 또는 훼손 여부에 대한 검사를 거쳐 24시간 상주하는 AWS 직원의 서명을 받습니다. 배송 도착 시, 물품은 AWS 자산 관리 시스템 및 디바이스 재고 추적 시스템 내에서 검사 및 수집됩니다. AWS 데이터 센터에서는 수령한 물품을 스와이프 배지와 PIN이 있어야 접근할 수 있는 데이터 센터 내 장비 보관실에 보관해 두었다가 데이터 센터 현장에 설치합니다. 물품은 데이터 센터에서 반출되기 전에 스캔, 추적 및 살균됩니다(데이터 센터 반출 허가 전). PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 자산 관리 프로세스와 절차를 검토합니다.	PS-12		7.1 7.1.1 10.10.3 10.10.6 15.1.3	9.6 9.7	AU-9 AU-11 CM-8 MP-3
PS.S-12.0	재고 추적	장기간 볼트 외부에 있는 자산에 대해 자동 알림을 사용합니다.						
PS-12.1	재고 추적	고객 자산과 생성된 미디어(예: 미디어, 하드 드라이브)를 수령할 때 바코드를 찍고, 자산을 사용하지 않을 경우 금고에 보관하십시오.						
PS.S-12.1	재고 추적	제시간에 배송할 수 없는 경우 지연되거나 반환되는 자산을 안전한 곳에 보관하고 일지에 기록합니다.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-12.2	재고 추적	자산 이동 거래 로그를 최소한 90일간 보관하십시오.						
PS-12.3	재고 추적	콘텐츠 자산 관리 시스템의 로그를 검토하고 이상이 있는지 조사하십시오.						
PS-12.4	재고 추적	해당하는 경우 자산 추적 시스템과 물리적 자산에 스튜디오 AKA("별칭")를 사용하십시오.						
PS-13.0	재고 파악	분기마다 자산 관리 기록과 대조하여 각 고객의 릴리스 전 시험 프로젝트의 재고 수를 파악하고 변동이 있을 경우 즉시 고객에게 알리십시오.	고객은 데이터와 관련 미디어 자산에 대한 관리 권한과 책임을 보유합니다. 물리적 자산의 재고 추적 및 모니터링을 구현할 책임은 고객에게 있습니다. AWS 자산 관리 시스템 및 디바이스 재고 추적 시스템은 AWS 데이터 센터 정보 시스템 구성 요소에 대한 재고를 체계적으로 관리합니다. 재고 감사는 정기적으로 실시되며, FedRAMP[sm] 준수 프로그램의 일환으로 독립적인 감사 기관의 검토를 받습니다.	PS-13		7.1.1 10.1.3		AU-6 AC-5 IR-4 IR-5

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-13.0	재고 파악	매주 자산 관리 기록과 대조하여 각 고객의 릴리스 전 시험 프로젝트의 재고 수를 파악하고 변동이 있을 경우 즉시 고객에게 알립니다.	PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 자산 관리 프로세스와 절차를 검토합니다.					
PS-13.1	재고 파악	금고 직원과 재고 파악 담당자 간에 업무를 분담하십시오.						
PS.S-13.1	재고 파악	워크플로우 프로세스 전체에 걸쳐 필름 엘리먼트(예: 원판, 처리되지 않은 필름)를 지속적으로 모니터링합니다.						
PS-13.2	재고 파악	일일 시효 보고서를 구현 및 검토하여 금고에서 반출된 후 회수되지 않은 중요 자산이 있는지 식별하십시오.						
PS-14.0	빈 미디어/원재료 재고 추적	빈 재고/원재료 재고를 받을 때 단위당 태그를 지정하십시오(예: 바코드, 고유 식별자 할당).	AWS 고객은 데이터와 미디어 자산에 대한 관리 및 소유권을 보유합니다. 미디어 스톡에 대한 보안 관리는 스튜디오/처리 시설의 책임입니다.	PS-14		7.1.1 10.7.1		MP-4 MP-2 PE-2 PE-3
PS.S-14.0	빈 미디어/원재료 재고 추적	매월 원자재(예: 폴리카보네이트)의 소비량을 추적하는 프로세스를 수립합니다.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-14.1	빈 미디어/원재료 재고 추적	빈 미디어/원재료 재고를 안전한 곳에 보관하십시오.						
PS-15.0	고객 자산	고객의 완제품 자산에 접근할 수 있는 권한은 자산 추적 및 관리 담당자에게만 허용하십시오.	적절한 물리적 보안이 구현되었는지 확인하는 일은 최종 자산의 물리적 사본을 선별/관리하는 인력의 책임입니다. MPAA PS-1 – PS-14에 명시된 바와 같이, AWS는 전체 데이터 센터를 대상으로 물리적 보안 프로그램 및 자산 관리 프로그램을 운영하고, 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 프로그램의 일환으로 외부 감사 기관으로부터 정기 감사 및 평가를 받고 있습니다.	PS-15	SOC 1(5.3, 5.5) SOC 2(S3.3, S3.4, S5.3)	7.1.1 9.1.2 10.7.1	9.1 9.6 9.7	MP-2 MP-4 PE-2 PE-3
PS.S-15.0	고객 자산	두 회사의 직원이 업무 시간 이후에 중요 영역(예: 금고, 보안 케이지)의 잠금을 해제하려면 별도의 출입 카드를 소지해야 합니다.						
PS-15.1	고객 자산	고객 자산을 안전한 제한 구역(예: 금고)에 보관하십시오.						
PS.S-15.1	고객 자산	스테이징 영역에 출입이 통제되는 케이지를 사용하고 감시 카메라가 설치된 영역을 모니터링합니다.						
PS.S-15.2	고객 자산	시설에서 밤새 보관되는 배달되지 않은 화물을 보관할 때는 잠금식 방화 금고를 사용합니다.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-15.3	고객 자산	배달되지 않은 스크리너를 보관할 수 있는 전용 보안 구역(예: 보안 케이지, 보안실)을 마련합니다. 이 보안 구역은 잠가 두고 출입을 통제하고, 감시 카메라 및/또는 보안 요원이 모니터링해야 합니다.						
PS-16.0	폐기	거부되거나, 손상되거나, 쓸모 없는 재고는 폐기(예: DVD 파쇄, 하드 드라이브 파괴)하기 전에 내용을 삭제하거나 자기를 소거하거나 파쇄하거나 물리적으로 파괴하고 자산 관리 기록을 업데이트하여 폐기를 반영하십시오.	AWS 절차에는 AWS 스토리지 디바이스의 수명이 다할 경우 권한이 없는 개인에게 고객 데이터가 노출되는 것을 방지하기 위해 고안된 폐기 프로세스가 포함되어 있습니다. AWS는 DoD 5220.22-M("국가 산업 보안 프로그램 운영 매뉴얼") 또는 NIST 800-88("미디어 삭제 가이드라인")에서 설명하는 기술을 사용해 폐기 프로세스에 따라 데이터를 제거합니다. 모든 폐기된 스토리지 디바이스는 업계 표준 관행에 따라 디가우징 후 물리적으로 파쇄됩니다. AWS는 지속적인 ISO 27001 및 FedRAMP[sm] 준수 프로그램의 일환으로, 외부의 독립적 감사 기관으로부터 AWS 스토리지 디바이스 폐기 프로세스를 정기적으로 검토 및 평가 받습니다.	PS-16		9.2.6 10.7.2	9.10	MP-6
PS.S-16.0	폐기	스크랩을 폐기하는 경우 보안 관계자가 스크래핑 프로세스를 모니터링하고 기록하도록 하는 프로세스를 구현합니다.						
PS-16.1	폐기	자산 복제 및 재사용을 방지하기 위해 폐기하기 전에 재활용/폐기 품목을 안전한 위치/용기에 보관하십시오.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-16.1	폐기	모든 회사 직원과 타사 작업자에게 자산 폐기 프로세스(예: 자산을 배정된 용기에 넣기)를 교육하는 정기적인 보안 교육을 실시합니다.						
PS-16.2	폐기	자산 폐기 로그를 최소한 12개월 동안 보관하십시오.						
PS.S-16.2	폐기	디스크를 스크랩 빈에 버리기 전에 디스크에 흠집을 냅니다.						
PS-16.3	폐기	콘텐츠 폐기를 담당하는 타사는 폐기를 완료할 때마다 폐기 인증서를 제출해야 합니다.						
PS.S-16.3	폐기	자동화를 통해 복제 시스템에서 거부된 디스크를 스크랩 빈으로 옮깁니다(기기 조작자 처리 없음).						
PS.S-16.4	폐기	DCDM 드라이브 또는 사전 릴리스된 콘텐츠 폐기 시 타사 이용을 금지합니다.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-17.0	배송	시설에서 시설 외부로 자산을 운송할 수 있는 권한을 부여하는 유효한 업무/선적 지시서를 발행해야 합니다.	AWS 데이터 센터 환경의 경우, 데이터 센터로 배송되고 데이터 센터에서 수령하는 서버, 랙, 네트워크 디바이스, 하드 드라이브, 시스템 하드웨어 구성 요소 및 건축 자재를 포함하는(이에 제한되지 않음) 모든 새 정보 시스템 구성 요소는 사전에 데이터 센터 관리자에게 알려 승인을 받아야 합니다. 물품은 각 AWS 데이터 센터의 로딩 독으로 배달되며 화물의 손상 또는 훼손 여부에 대한 검사를 거쳐 24시간 상주하는 AWS 직원의 서명을 받습니다. 배송 도착 시, 물품은 AWS 자산 관리 시스템 및 디바이스 재고 추적 시스템 내에서 검사 및 수집됩니다. PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 자산 관리 프로세스와 절차를 검토합니다.	PS-17		9.1.2 10.8.2 10.8.3	9.6 9.7	MP-5 AU-11 PE-16
PS.S-17.0	배송	트럭 운전자 정보에 대한 개별 일지에 기록하고 보관합니다.						
PS-17.1	배송	자산 선적 정보를 추적하고 기록하십시오. 이러한 기록에는 최소한 다음 정보가 포함되어야 합니다. • 선적 시간 • 발송인 이름 및 서명 • 수취인 이름 • 목적지 주소 • 배송업체의 운송장 번호 • 해당 업무 지시서 참조						
PS.S-17.1	배송	화물을 수령하는 개인은 운송 서류 수와 발송 지점의 서명을 반드시 확인해야 합니다.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-17.2	배송	유효한 업무/선적 지시서와 대조하여 시설에서 나가는 자산을 검증하십시오.						
PS.S-17.2	배송	운송이 현장에서 발생하는 경우 트레일러의 포장 및 밀봉 상태를 관찰하고 모니터링합니다.						
PS-17.3	배송	상차 대기 중인 자산을 안전하게 보관하십시오.						
PS.S-17.3	배송	시설 간 운송에 걸리는 이동 시간, 경로 및 배달 시간을 기록, 모니터링 및 검토하는 공식 프로세스를 구현합니다.						
PS-17.4	배송	배송업체와 배송 담당자가 시설의 콘텐츠/프로덕션 영역에 들어오지 못하도록 하십시오.						
PS.S-17.4	배송	필름 엘리먼트는 운송 이외의 방법으로 시설 외부로 반출할 수 없습니다(서명된 허가 통과서가 있는 경우 제외).						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-17.5	배송	공연 전 심사를 위한 인쇄물을 세그먼트(예: 홀수/짝수 릴)로 운송합니다.						
PS-18.0	인도	인도 시 배송된 콘텐츠를 검사하고 선적 서류(예: 포장 명세서, 적하 기록)와 대조하십시오.	AWS 데이터 센터에서는 수령한 새 정보 시스템 구성 요소를 스와이프 배지와 PIN이 있어야 접근할 수 있는 데이터 센터 내 장비 보관실에 보관해 두었다가 데이터 센터 현장에 설치합니다. 물품은 데이터 센터에서 반출되기 전에 스캔, 추적 및 살균됩니다(데이터 센터 반출 허가 전). PCI DSS, ISO 27001 및 FedRAMP[sm] 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 자산 관리 프로세스와 절차를 검토합니다.	PS-18		7.1 7.2 10.8.2 10.8.3	9.6 9.7	MP-3 MP-4 PE-16
PS-18.1	인도	배송 물품 인도 시 지정된 직원이 수령증을 작성하고 보관해야 합니다.						
PS-18.2	인도	즉시 다음 조치를 취하십시오. • 인도된 자산에 태그 지정(예: 바코드, 고유 식별자 할당) • 자산 관리 시스템에 자산 입력 • 제한 구역(예: 금고)으로 자산 이동						
PS-18.3	인도	야간 배송물을 인도할 수 있는 안전한 방법(예: 안전한 투입함)을 마련하십시오.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-19.0	라벨 부착	포장 외부에 AKA("별칭")와 같은 제목 정보를 사용하지 마십시오.	AWS 자산 레이블은 고객을 구분하지 않으며 AWS Asset Management Tool 내에서 하드웨어 인벤토리를 유지하는 데 이용됩니다. AWS 데이터 센터 내에서는 하드웨어가 고객이나 하드웨어에 저장된 데이터와 물리적으로 연결되어 있지 않습니다. 원본과 관계 없이 모든 고객 데이터는 중요 정보로 간주되며, 모든 미디어 역시 중요 자료로 처리됩니다. PCI DSS, ISO 27001 및 FedRAMP^{sm} 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 자산 관리 프로세스와 절차를 검토합니다.	PS-19		7.2	9.6 9.7	MP-3
PS-20.0	포장	모든 자산을 폐쇄되거나 밀봉된 컨테이너에 선적하고 자산의 가치에 따라 잠금장치가 있는 컨테이너를 사용하십시오.	물리적 최종 미디어 자산의 포장은 관련 배포 주체(예: 배포, DVD 제작, 사후 생산 등과 관련된 회사)의 책임입니다.	PS-20		10.8.3		MP-5
PS.S-20.0	포장	모든 운송에는 수축 포장을 적용하며 최종 운송 전에 포장을 검사하여 적절히 포장되었는지 확인합니다.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-20.1	포장	다음 컨트롤 중 최소한 하나 이상을 구현하십시오. • 부정 개봉 방지 테이프 • 부정 개봉 방지 포장 • 홀로그램 형태의 부정 개봉 방지 씰 • 보안 컨테이너(예: 번호 자물쇠가 달린 펠리칸 케이스)						
PS-21.0	운송 차량	자동차와 트럭을 항상 잠가 두고 자동차/트럭 내부의 잘 보이는 위치에 물품을 두지 마십시오.	물리적 최종 미디어 자산(예: DVD)의 운송은 관련 배포 주체(예: 배포, DVD 제작, 사후 생산 등과 관련된 회사)의 책임입니다.	PS-21				MP-5
PS.S-21.0	운송 차량	운송 차량(예: 트레일러)에는 다음 보안 기능이 포함되어야 합니다. • 운전자 캐빈과의 분리 • 화물칸 도어 잠금 및 밀폐 기능 • 보안 강화 운송을 위한 GPS						
PS.S-21.1	운송 차량	매우 중요한 타이틀을 운송하는 경우 화물칸 도어에 번호가 지정된 씰을 부착합니다.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-21.2	운송 차량	고위험 지역에 매우 중요한 콘텐츠를 배달할 때는 보안 에스코트를 사용해야 합니다.						
DS-1.0	WAN	내부 네트워크에 대한 무단 액세스를 방지하는 액세스 제어 요건이 있는 상태 추적 방화벽을 사용해 WAN을 분리하십시오.	규칙 세트, ACL(액세스 제어 목록) 및 구성이 사용되는 경계 보호 디바이스는 네트워크 패브릭 간의 정보 흐름을 적용합니다. 여러 네트워크 패브릭이 Amazon에서 나오며, 각 패브릭은 패브릭 간의 정보 흐름을 제어하는 디바이스에 의해 분리됩니다. 패브릭 간의 정보 흐름은 승인 기관에서 설정하며, 이러한 기관은 해당 디바이스의 ACL(액세스 제어 목록)에 명시되어 있습니다. 이러한 디바이스는 이 ACL에 규정된 대로 패브릭 간의 정보 흐름을 제어합니다. 적절한 담당자가 ACL을 정의 및 승인하고, AWS ACL 관리 도구를 사용하여 관리 및 배포합니다.	DS-1	SOC 1(3.2, 3.3, 3.4, 3.7, 3.9, 3.10, 3.14, 3.15, 3.16) SOC 2(S.3.2, S3.4, S.3.5, S4.1, S.4.2, S4.3, S3.12)	11.1 11.4	1.1 1.2 1.3 1.4 2.2 6.6 8.5 11.2	AC-2 AC-3 CM-7
DS-1.1	WAN	비즈니스 요구에 따라 6개월마다 ACL(액세스 제어 요건)을 검토해 구성 설정이 올바른지 확인하는 프로세스를 개발하십시오.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-1.2	WAN	기본적으로 모든 프로토콜을 거부하고 WAN에서 허용하는 안전한 프로토콜만 활성화합니다.	Amazon의 정보 보안 팀은 이러한 ACL을 승인합니다. 네트워크 패브릭 간에 승인된 방화벽 규칙 세트 및 액세스 제어 목록에 따라 정보 흐름을 특정 정보 시스템 서비스로 제한합니다. 액세스 제어 목록과 규칙 세트는 검토 및 승인을 거친 뒤 정기적으로(최소한 24시간마다) 경계 보호 디바이스에 자동으로 푸시되어 항상 최신 상태를 유지합니다. AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수의 일환으로, 정기적으로 외부의 독립적 감사 기관으로부터 AWS 네트워크 관리를 검토 받습니다. AWS는 인프라 구성 요소 전체에 걸쳐 최소 권한을 구현합니다. AWS는 특정 비즈니스 목적이 없는 모든 포트와 프로토콜을 금지합니다. AWS는 디바이스 사용에 필수적인 특징과 기능만 최소한 구현하는 엄격한 접근 방식을 따릅니다. 네트워크 검사를 수행하여 사용 중인 불필요한 포트 또는 프로토콜을 모두 수정합니다. 다양한 도구를 사용하여 AWS 환경의 호스트 운영 체제, 웹 애플리케이션, 데이터베이스에 대해 정기적으로 내부 및 외부 취약성 검사를 수행합니다. AWS의 지속적인 PCI DSS 및 FedRAMP[sm] 준수의 일환으로, 취약성 검사 및 수정 관행을 정기적으로 검토 받습니다.					
DS-1.3	WAN	DMZ 내에 외부에서 액세스할 수 있는 서버(예: 보안 FTP 서버, 웹 서버)를 배치하십시오.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-1.4	WAN	네트워크 인프라 디바이스(예: 방화벽, 라우터, 스위치 등)에 대한 패치를 정기적으로 적용하십시오.						
DS-1.5	WAN	보안 구성 표준에 따라 네트워크 인프라 디바이스를 강화하십시오.						
DS-1.6	WAN	콘텐츠 액세스를 제어하는 WAN 네트워크 인프라 디바이스(예: 방화벽, 라우터)에 대한 원격 액세스를 허용하지 마십시오.						
DS-1.7	WAN	네트워크 인프라 디바이스를 내부 네트워크의 중앙 집중식 보안 서버에 백업하십시오.						
DS-1.8	WAN	외부에서 액세스할 수 있는 호스트에 대해 매년 취약성 검사를 실시하고 문제를 해결하십시오.						
DS-1.9	WAN	권한 있는 사람에게만 통신 서비스 공급자를 통한 연결을 구성할 수 있는 권한을 부여하십시오.						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-2.0	인터넷	디지털 콘텐츠를 처리하거나 보관하는 시스템(데스크톱/서버)에 대한 인터넷 액세스를 금지하십시오.	경계 보호 디바이스는 규칙 세트, 액세스 제어 목록(ACL) 및 구성을 네트워크 패브릭 간의 정보 흐름에 적용하는 경계 보호 디바이스를 거부하는 모두 거부 모드로 구성됩니다. 이러한 디바이스는 모두 거부 모드로 구성되므로 승인된 방화벽에서 연결을 허용하도록 설정해야 합니다. AWS 네트워크 방화벽 관리에 대한 자세한 내용은 DS-2.0을 참조하십시오. AWS 자산에는 고유한 이메일 기능이 없으며 포트 25가 사용되지 않습니다. 고객(예: 스튜디오, 처리 시설 등)은 이메일 호스트 시스템을 운영할 수 있습니다. 그러나 그 경우 고객은 이메일 수신 및 발신 지점에서 적절한 수준의 스팸 및 맬웨어 방지 조치를 취하고, 스팸 및 맬웨어 정의가 새로 발표될 때마다 업데이트할 책임이 있습니다. Amazon 자산(예: 랩톱)은 이메일 필터링 및 맬웨어 탐지를 포함하는 안티바이러스 소프트웨어로 구성됩니다. AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP^{sm} 준수의 일환으로, 외부의 독립적 감사 기관으로부터 AWS 네트워크 방화벽 관리 및 Amazon의 안티바이러스 프로그램을 검토 받습니다.	DS-2	SOC 1(3.2, 3.3, 3.4, 3.7, 3.9, 3.10, 3.14, 3.15, 3.16) SOC 2(S.3.2, S3.4, S.3.5, S4.1, S.4.2, S4.3, S3.12)	7.1.3 11.2.2	1.1 1.2 1.3 1.4 2.2 5.1 6.6 8.5 11.2	CA-3 PL-4
DS-2.1	인터넷	비 프로덕션 네트워크로부터 다음을 차단하는 이메일 필터링 소프트웨어 또는 어플라이언스를 구현합니다. • 잠재적인 피싱 이메일 • 금지된 첨부 파일(예: Visual Basic 스크립트, 실행파일 등) • 10MB로 제한된 파일 크기 제한						

번호.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-2.2	인터넷	P2P 파일 거래, 바이러스, 해킹 또는 기타 악성 사이트로 알려진 웹 사이트에 대한 액세스를 제한하는 웹 필터링 소프트웨어 또는 애플리케이션을 구현하십시오.						
DS-3.0	LAN	물리적/논리적 네트워크 분리를 이용하여 콘텐츠/프로덕션 네트워크와 기타 네트워크(예: 사무실 네트워크, DMZ 등)를 구분하십시오.	AWS는 네트워크를 분리 및 관리할 수 있는 기능을 제공하지만 이러한 분리된 환경의 구현 및 운영에 대해서는 책임을 지지 않습니다.	DS-3		11.2 11.4.2 11.4.4 10.6.2 10.10		AC-6 AC-17 CM-7 SI-4
DS-3.1	LAN	권한 있는 사람에게만 콘텐츠/프로덕션 시스템 액세스를 허용하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-3.2	LAN	업무상 액세스가 필요한 승인된 사람에게만 콘텐츠/프로덕션 네트워크에 대한 원격 액세스를 허용하십시오.						
DS-3.3	LAN	권한 없는 디바이스의 패킷 스니핑을 방지하기 위해 콘텐츠/프로덕션 네트워크에서 사용하지 않는 모든 스위치 포트를 비활성화하십시오.						
DS-3.4	LAN	콘텐츠/프로덕션 네트워크의 허브 및 리피터와 같은 비교환 디바이스의 사용을 제한하십시오.						
DS-3.5	LAN	콘텐츠/프로덕션 네트워크 내의 컴퓨터 시스템에서 이중 홈 네트워킹(네트워크 브리징)을 금지하십시오.						
DS-3.6	LAN	콘텐츠/프로덕션 네트워크에 네트워크 기반 침입 탐지 또는 방지 시스템을 구현하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-4.0	무선	콘텐츠/프로덕션 네트워크에서 무선 네트워킹과 무선 디바이스 사용을 금지하십시오.	AWS 자산에는 고유한 무선 기능이 없습니다. Amazon 자산(예: 랩톱) 무선 기능은 산업 표준 보안 무선 구성 표준에 따라 구현 및 작동됩니다. Amazon은 무선 네트워크를 지속적으로 모니터링하여 악의적인 디바이스를 감지합니다.	DS-4		10.6.1 12.6	11.1	AC-18 SI-4
DS-4.1	무선	다음 보안 제어 수단을 이용하여 비 프로덕션 무선 네트워크(예: 관리 및 게스트)를 구성합니다. • WEP 비활성화 • AES 암호화 활성화 • "게스트" 네트워크를 회사의 다른 네트워크와 분리합니다.	AWS는 지속적인 PCI DSS, ISO 27001 및 FedRAMP[sm] 준수의 일환으로, 외부의 독립적 감사 기관으로부터 AWS 무선 네트워크 관리를 검토 받습니다.					
DS-4.2	무선	매년 불법 무선 액세스 지점을 검사하는 프로세스를 구현하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-5.0	I/O 디바이스 보안	콘텐츠 입력/출력(I/O)에 사용할 특정 시스템을 지정하십시오.	AWS는 시스템 출력 디바이스에 대한 액세스 권한을 권한 있는 사람으로만 제한합니다. 액세스 권한을 얻으려면 전자 요청서를 제출하여 액세스에 대한 비즈니스 사례를 제공하고 공인 승인자로부터 해당 권한 부여에 대한 문서화된 승인을 얻어야 합니다. AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수의 일환으로, 외부의 독립적 감사 기관으로부터 AWS 액세스 관리 절차를 검토 받습니다. 개인 전자 디바이스 및 이동식 미디어는 AWS 정보 시스템에 연결할 수 없습니다.	DS-5	SOC 1(2.1, 5.1) SOC 2(S.3.2, S3.3, S.3.4)	10.7.1 10.10.2	7.1 8.2	MP-2 AC-19 PE-5
DS-5.1	I/O 디바이스 보안	콘텐츠 I/O에 사용되는 시스템을 제외하고, 콘텐츠를 취급하거나 저장하는 모든 시스템에서 I/O(입력/출력) 디바이스(예: USB, FireWire, e-SATA, SCSI 등)를 차단하십시오.						
DS-5.2	I/O 디바이스 보안	콘텐츠를 물리적 미디어로 출력하는 데 사용되는 특정 I/O 시스템에서만 미디어 버너(예: DVD, Blu-ray, CD 버너)와 출력 기능이 있는 기타 디바이스를 설치하거나 사용하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-6.0	시스템 보안	모든 워크스테이션과 서버에 안티바이러스 소프트웨어를 설치하십시오.	AWS 환경 내에서는 패키지, 패키지 그룹 및 환경에서 배포 가능한 소프트웨어를 관리하는 데 구성 관리 도구가 사용됩니다. 패키지란 긴밀하게 결합된 소프트웨어, 콘텐츠 등 관련 파일의 모음입니다. 패키지 그룹이란 흔히 함께 표시되는 패키지 세트를 말합니다. 환경이란 호스트 클래스 세트(동일한 기능을 제공하는 호스트 또는 서버)에 배포되는 패키지 및 패키지 그룹의 세트 조합을 말합니다. 환경은 서버에서 특정 기능을 수행하는 데 필요한 전체 패키지 세트를 나타내기도 합니다. AWS는 호스트에 사용되는 기준 OS 배포를 유지합니다. 불필요한 모든 포트, 프로토콜 및 서비스는 기본 빌드에서 비활성화됩니다. 서비스 팀에서는 빌드 도구를 사용하여 도구에서 유지되는 구성 기준에 따라 서버 기능에 필요한 승인된 소프트웨어 패키지만 추가합니다. 서버는 정기적으로 검사되며 사용 중인 불필요한 포트 또는 프로토콜은 결함 수정 프로세스를 사용하여 모두 수정됩니다. 배포된 소프트웨어는 엄선된 산업 전문가에 의해 실시되는 반복적 침투 테스트를 거치게 됩니다. 침투 테스트 검사에 따른 수정도 결함 수정 프로세스를 통해 기준에 통합됩니다. Amazon 정보 보안 및 AWS 보안 팀은 Secunia 및 TELUS 보안 연구소의 해당 공급업체 결함을 알려주는 뉴스피드에 가입되어 있습니다. Amazon 정보 보안 팀은 공급업체의 웹 사이트와 기타 관련 유출구를 모니터링하며 새 패치가 있는지 확인합니다. 구현하기 전에 패치는 보안 및 운영 상의 영향 여부에 대해 평가되고 평가에 따라 적시에 적용됩니다.	DS-4		10.4.1 10.1.3 10.8.2 11.3.2 11.4.3 11.4.4		SI-3 SI-2 RA-5 AC-5 SC-2 PE-3 MA-4 PE-5 SA-7 SA-6
DS-6.1	시스템 보안	안티바이러스 정의를 매일 업데이트하십시오.						
DS-6.2	시스템 보안	파일 기반 콘텐츠를 콘텐츠/프로덕션 네트워크에 입력하기 전에 바이러스 검사를 실시하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-6.3	시스템 보안	다음과 같이 바이러스 검사를 수행합니다. • 모든 워크스테이션에 대해 정기적인 전체 시스템 바이러스 검사 활성화 • 서버에 대해 전체 시스템 바이러스 검사 활성화(예: 비 SAN 시스템)	Amazon 자산(예: 랩톱)은 이메일 필터링 및 맬웨어 탐지를 포함하는 안티바이러스 소프트웨어로 구성됩니다. AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수를 위해 외부의 독립적 감사 기관으로부터 모든 AWS 구성 관리 및 결함 수정 프로세스를 검토 받습니다.					
DS-6.4	시스템 보안	보안 취약성을 수정하는 패치/업데이트를 사용하여 시스템(예: 파일 전송 시스템, 운영 체제, 데이터베이스, 애플리케이션, 네트워크 디바이스)을 정기적으로 업데이트 프로세스를 구현합니다.						
DS-6.5	시스템 보안	사용자가 자체 워크스테이션의 관리자가 되는 것을 금지하십시오.						
DS-6.6	시스템 보안	콘텐츠를 다루는 이동식 컴퓨팅 디바이스(예: 노트북, 태블릿, 타워)를 두고 자리를 비울 경우 케이블 잠금장치를 사용하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-6.7	시스템 보안	하드웨어 및 기타 스토리지 디바이스의 데이터를 원격으로 지울 수 있도록 콘텐츠를 다루는 모든 이동식 컴퓨팅 디바이스에 원격 제거 소프트웨어를 설치하십시오.						
DS-6.8	시스템 보안	소프트웨어 설치 권한을 승인된 사용자로 제한합니다.						
DS-6.9	시스템 보안	내부에서 설정되는 시스템(예: 노트북, 워크스테이션, 서버)을 구성하는 보안 기준 및 표준을 구현하십시오.						
DS-6.10	시스템 보안	불필요한 서비스와 애플리케이션은 콘텐츠 전송 서버에서 제거해야 합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-7.0	계정 관리	콘텐츠를 다루는 모든 정보 시스템 및 애플리케이션의 관리자, 사용자 및 서비스 계정을 위한 계정 관리 프로세스를 확립하고 구현하십시오.	AWS에는 공식적인 액세스 제어 정책이 마련되어 있으며, 이 정책은 매년(또는 시스템에 정책에 영향을 주는 대규모 변화가 발생할 때마다) 검토 및 업데이트됩니다. 이 정책은 목적, 범위, 역할, 책임 및 경영진의 책임감을 규정합니다. AWS는 최소 권한의 개념을 채택하여 사용자가 직능을 수행하는 데 필요한 액세스만 허용합니다. 사용자 계정이 생성하는 경우 사용자 계정이 최소한의 액세스 권한이 부여되도록 생성됩니다. 이러한 최소 권한을 초과하는 액세스 권한에는 적절한 권한 부여가 필요합니다. AWS 시스템 및 디바이스의 권한 있는 사용자에게는 권한 있는 개인 직능 및 역할과 관련하여 그룹 멤버십을 통해 액세스 권한이 제공됩니다. 그룹 멤버십 조건은 그룹 소유자에 의해 설정 및 확인됩니다. 사용자, 그룹 및 시스템 계정에는 모두 고유한 식별자가 있으며 재사용되지 않습니다. 게스트/익명 및 임시 계정은 사용되지 않으며 디바이스에서 허용되지 않습니다.	DS-7	SOC 1(2.1, 2.2) SOC 2(S.3.2, S.3.4)	10.1.3 10.10.4 11.2 11.2.1 11.2.2 11.2.4	7.1 8.1 8.2	AC-2 AC-5 AC-6 AU-2 AU-12 IA-4 PS-4 PS-5 PE-2
DS-7.1	계정 관리	추적 가능한 계정 관리 활동 증거(예: 승인 이메일, 변경 요청 양식)를 보관하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-7.2	계정 관리	알아야 하는 사람에게 최소 권한의 원칙에 따라 고유한 자격 증명을 할당하십시오.	사용자 계정은 적어도 분기마다 한 번씩 검토를 받습니다. 모든 그룹 소유자는 분기마다 사용자를 검토하고 필요할 경우 더 이상 그룹 멤버십이 필요하지 않은 사용자를 모두 제거합니다. 이 검토는 AWS Account Management Tool에 의해 그룹 소유자로 전송되는 시스템 알림으로 시작됩니다. 이 도구는 그룹 소유자에게 그룹의 기준을 수행하라고 알립니다. 기준은 그룹 소유자에 의한 완전한 권한 재평가를 말합니다. 기한까지 기준이 완료되지 않으면 모든 그룹 구성원이 제거됩니다. 사용자 계정이 90일간 비활성 상태를 유지하면 시스템에 의해 자동으로 비활성화됩니다. AWS는 AWS 시스템 내에서 시스템 및 디바이스 전반에 걸쳐 감사 가능한 이벤트 범주를 식별했습니다. 여러 팀이 요구 사항에 따라 보안 관련 이벤트를 지속적으로 기록하도록 감사 기능을 구성합니다. 로그 스토리지 시스템은 로그 스토리지 요구가 증가함에 따라 용량을 자동으로 증가시키는 확장성과 가용성이 우수한 서비스를 제공하도록 설계되었습니다. AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수를 위해 외부의 독립적 감사 기관으로부터 AWS 액세스 관리 절차를 검토 받습니다.					
DS-7.3	계정 관리	기본 관리자 계정의 이름을 변경하고, 해당 자격 증명이 필요한 특수한 상황(예: 운영 체제 업데이트, 패치 설치, 소프트웨어 업데이트)에만 이러한 계정을 사용하십시오.						
DS-7.4	계정 관리	정보 시스템에 대한 액세스를 할당하는 담당자가 해당 시스템의 최종 사용자가 되지 않도록(즉, 담당자가 자신에게 액세스를 할당할 수 없어야 함) 업무를 분담하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-7.5	계정 관리	관리자 및 서비스 계정 활동을 모니터링하고 감사하십시오.						
DS-7.6	계정 관리	분기마다 콘텐츠를 다루는 모든 정보 시스템에 대한 사용자 액세스를 검토하고 더 이상 액세스가 필요하지 않은 사용자 계정을 제거하는 프로세스를 구현하십시오.						
DS-7.7	계정 관리	프로젝트마다 콘텐츠에 대한 사용자 액세스를 검토하십시오.						
DS-7.8	계정 관리	기술적으로 실현 가능한 경우 콘텐츠를 처리하는 시스템에서 로컬 계정 비활성화 또는 제거						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-8.0	인증	고유한 사용자 이름과 암호를 사용해 정보 시스템에 액세스하십시오.	AWS 인사 관리 시스템에서 온보딩 워크플로우 프로세스의 일부로서 고유한 사용자 식별자가 생성됩니다. 디바이스 프로비저닝 프로세스를 통해 디바이스에 대한 고유한 식별자를 확인할 수 있습니다. 두 프로세스에는 사용자 계정 또는 디바이스 설정에 대한 관리자 승인이 포함되어 있습니다. 프로비저닝 프로세스의 일부로서 사용자에게 직접 또는 디바이스로 초기 인증값이 제공됩니다. 내부 사용자는 SSH 퍼블릭 키를 자신의 계정과 연결할 수 있습니다. 시스템 계정 인증값은 요청자의 ID가 확인된 후 계정 생성 프로세스의 일부로서 요청자에게 제공됩니다. 인증값의 최소 강도는 암호 길이를 포함하여 AWS에 의해 정의되며 SSH 키 최소 비트 길이와 함께 복잡한 암호와 암호 수명 요구 사항 및 콘텐츠가 필요합니다. AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수를 위해 외부의 독립적 감사 기관으로부터 AWS 암호 정책 및 구현을 검토 받습니다.	DS-8	SOC 1(2.5) SOC 2(S.3.2, S.3.4)	11.2.1 11.2.3 11.4.2 11.5.2	8.4 8.5	IA-2 IA-4 IA-5 AC-7 AC-11 AC-17
DS-8.1	인증	정보 시스템에 대한 액세스 권한을 얻을 수 있는 강력한 암호 정책을 사용하십시오.						
DS-8.2	인증	네트워크에 대한 원격 액세스(예: VPN)에 대해 이중 인증(예: 사용자 이름/암호와 하드 토큰)을 구현합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-8.3	인증	서버 및 워크스테이션에 대해 암호로 보호되는 화면 보호기나 화면 잠금 소프트웨어를 구현합니다.						
DS-9.0	로깅 및 모니터링	최소한 다음과 같은 정보를 수집하여 보안 이벤트를 기록 및 보고하는 실시간 기록 및 보고 시스템을 구현하십시오. • 시기(타임스탬프) • 위치(출처) • 대상(사용자 이름) • 내용(콘텐츠)	AWS는 AWS 시스템 내에서 시스템 및 디바이스 전반에 걸쳐 감사 가능한 이벤트 범주를 식별했습니다. 여러 팀이 요구 사항에 따라 보안 관련 이벤트를 지속적으로 기록하도록 감사 기능을 구성합니다. 로그 스토리지 시스템은 로그 스토리지 요구가 증가함에 따라 용량을 자동으로 증가시키는 확장성과 가용성이 우수한 서비스를 제공하도록 설계되었습니다. 감사 레코드에는 필요한 분석 요구 사항을 지원하기 위한 데이터 요소 세트가 포함되어 있습니다. 또한, 감사 레코드는 AWS 보안 팀이나 기타 해당 팀에서 요구 시 검사 또는 분석을 수행하고 보안 관련 또는 비즈니스에 영향을 미치는 이벤트에 대응하는 데 사용할 수도 있습니다. AWS 팀에 배정된 인력은 감사 처리 실패 시 자동화된 경고를 받습니다. 감사 처리 실패에는 소프트웨어/하드웨어 오류 등이 포함됩니다. 경고가 발생하면 대기 중인 인력이 문제 티켓을 발급하고 해당 문제가 해결될 때까지 이벤트를 추적합니다.	DS-9	SOC 1(3.6)	10.1 10.10.2 10.10.5	10.1 10.2 10.3	AU-1 AU-2 AU-3 AU-6 SI-4
DS.S-9.0	로깅 및 모니터링	다음 용도로 사용되는 모든 시스템에서 로깅 메커니즘을 구현합니다. • 키 생성 • 키 관리 • 공급업체 인증서 관리						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-9.1	로깅 및 모니터링	능동적인 인시던트 대응을 용이하게 하기 위해 보안 이벤트가 탐지될 경우 자동 알림을 전송하도록 로깅 시스템을 구성하십시오.	AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수를 위해 외부의 독립적 감사 기관으로부터 AWS 로깅 및 모니터링 프로세스를 검토 받습니다.					
DS-9.2	로깅 및 모니터링	로깅 및 보고 시스템에서 보고한 비정상적인 활동을 조사하십시오.						
DS-9.3	로깅 및 모니터링	매주 로그를 검토하십시오.						
DS-9.4	로깅 및 모니터링	내부 및 외부 콘텐츠 이동 및 전송 로깅을 활성화하고 최소한 다음 정보를 포함합니다. • 사용자 이름 • 타임스탬프 • 파일 이름 • 소스 IP 주소 • 대상 IP 주소 • 이벤트(예: 다운로드, 보기)						
DS-9.5	로깅 및 모니터링	최소한 6개월간 로그를 보관하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-9.6	로깅 및 모니터링	로그 액세스를 담당자에게만 허용하십시오.						
DS-9.7	로깅 및 모니터링	외부 발신 콘텐츠 전송 시 프로덕션 조정자에게 자동 알림을 전송합니다.						
DS-10.0	보안 기법	지시를 받은 경우 보안 기법(예: 스포일링, 보이지 않는/보이는 워터마크)을 사용할 수 있도록 지원하고 적용하십시오.	AWS는 고객에게 S3, EBS 및 EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있는 기능을 제공합니다. VPC 세션도 암호화됩니다. 내부적으로 AWS는 AWS 인프라 내에서 사용되는 필수 암호화용 암호화 키를 설정하고 관리합니다. AWS는 AWS 정보 시스템에서 NIST 승인 키 관리 기술 및 프로세스를 사용하여 대칭적 암호화 키를 생성, 제어 및 배포합니다. AWS에서 개발한 보안 키 및 자격 증명 관리자를 사용하여 대칭적 키를 생성, 보호, 배포하는 한편, 호스트에서 필요한 AWS 자격 증명, RSA 프라이빗/퍼블릭 키 및 X.509 자격 증명을 보호하고 배포합니다. AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP^{sm} 준수를 위해 외부의 독립적 감사 기관으로부터 AWS 암호화 프로세스를 검토 받습니다.	DS-10		7.2.2 12.3.1 12.3.2	3.4.1	IA-5 SC-9 SC-12 SC-13
DS.S-10.0	어드밴스 보안 기술	다음을 충족하는 키 관리 프로세스를 구현합니다. • 신뢰할 수 있는 디바이스의 승인 및 취소 • 콘텐츠 키 생성, 갱신 및 취소 • 내부 및 외부에 콘텐츠 키 배포						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-10.1	보안 기법	다음 중 한 가지 방법으로 최소한 AES 128비트 암호화를 사용하여 하드 드라이브의 콘텐츠를 암호화합니다. • 파일 기반 암호화(콘텐츠 자체를 암호화함) • 드라이브 기반 암호화(하드 드라이브를 암호화함)						
DS.S-10.1	어드밴스 보안 기술	TDL(신뢰할 수 있는 디바이스 목록)의 디바이스가 권리 소유자 승인에 근거하여 적절한지 확인합니다.						
DS-10.2	보안 기법	대역외 통신 프로토콜(콘텐츠와 동일한 스토리지 미디어에 있지 않음)을 사용해 암호화 키 또는 암호를 전송합니다.						
DS.S-10.2	어드밴스 보안 기술	콘텐츠 키의 유효성을 확인하고 만료 날짜가 고객 지침을 준수하는지 확인합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-11.0	전송 도구	액세스 제어, 최소 AES 128비트 암호화 및 강력한 콘텐츠 전송 세션 인증을 사용하는 전송 도구를 구현하십시오.	AWS는 고객에게 S3, EBS 및 EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있는 기능을 제공합니다. VPC 세션도 암호화됩니다. AWS 연결의 경우 FIPS에 승인한 해시를 사용할 수 있습니다. AWS에서는 API 엔드포인트, VPC IPSEC VPN, IAM, MFA 하드웨어 토큰, SSH 같은 액세스 방법을 통해 사용자 인증 시 암호화 모듈을 이용합니다.	DS-11	SOC 1(4.1, 4.2, 4.3) SOC 2(S.3.6)	12.3.1	3.4.1	IA-5 SC-13
DS-11.1	전송 도구	암호화된 전송 도구를 사용할 수 없는 경우에 대비해 고객에게 서면으로 사전 승인을 받아야 하는 예외 프로세스를 구현하십시오.						
DS-12.0	전송 디바이스 방법론	콘텐츠 전송을 위한 전용 시스템을 구현하고 사용하십시오.	AWS는 네트워크를 분리 및 관리할 수 있는 기능을 제공하지만 이러한 분리된 환경의 구현 및 운영에 대해서는 책임을 지지 않습니다.	DS-12		10.7.1 10.8 11.4.5		AC-4 AC-20 SC-7
DS-12.1	전송 디바이스 방법론	파일 전송을 전담하는 시스템을 콘텐츠를 보관하거나 처리하는 시스템과 비 프로덕션 네트워크에서 분리하십시오.						
DS-12.2	전송 디바이스 방법론	콘텐츠/프로덕션 네트워크가 아니라 완충 영역(Demilitarized Zone, DMZ)에 콘텐츠 전송 시스템을 배치합니다.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-12.3	전송 디바이스 방법론	전송/수신이 성공하면 즉시 콘텐츠 전송 디바이스에서 콘텐츠를 제거하십시오.						
DS-13.0	클라이언트 포털	권한 있는 사용자에게만 콘텐츠 전송, 콘텐츠 스트리밍, 키 배포에 사용되는 웹 포털에 대한 액세스를 허용하십시오.	AWS는 클라이언트 포털을 생성 및 관리하는 기능을 고객에게 제공합니다. AWS는 고객을 대신하여 이 포털을 구현하거나 관리하지 않습니다.	DS-13		11.2.2 11.2.4 11.3.2 11.4.5 11.4.7 12.6.1		AC-2 AC-3 AC-4 AC-6 AC-20 IA-5 RA-3 RA-5 SC-10
DS-13.1	클라이언트 포털	포털 사용자에게 고유한 자격 증명(예: 사용자 이름 및 암호)을 할당하고 자격 증명을 클라이언트에 안전하게 배포하십시오.						
DS-13.2	클라이언트 포털	사용자가 본인의 디지털 자산에만 액세스할 수 있는지 확인하십시오(고객 A가 고객 B의 콘텐츠에 액세스해서는 안 됨).						
DS-13.3	클라이언트 포털	웹 포털을 DMZ의 전용 서버에 배치하고 특정 IP와 프로토콜의 액세스를 제한하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-13.4	클라이언트 포털	고객이 승인한 경우가 아니면 인터넷 웹 서버에 호스팅된 타사 프로덕션 추적 소프트웨어의 사용을 금지합니다.						
DS-13.5	클라이언트 포털	내부/외부 웹 포털에 HTTPS와 강력한 암호화 제품군(예: SSLv3 또는 TLS v1)을 사용하십시오.						
DS-13.6	클라이언트 포털	영구 쿠키 또는 일반 텍스트로 자격 증명을 저장하는 쿠키를 사용하지 마십시오.						
DS-13.7	클라이언트 포털	내부 또는 외부 포털의 콘텐츠에 대한 액세스가 지정된 기간 후에 자동으로 종료되도록 설정하십시오(구성 가능한 경우).						
DS-13.8	클라이언트 포털	매년 웹 애플리케이션 취약성을 테스트하십시오.						
DS-13.9	클라이언트 포털	권한 있는 사람에게만 통신 서비스 공급자를 통한 연결을 구성할 수 있는 권한을 부여하십시오.						

아니요.	보안 항목	모범 사례	AWS 구현	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-13.10	클라이언트 포털	비 프로덕션 네트워크에서 이메일(웹 메일 포함)을 사용해 콘텐츠를 전송하지 못하게 하고 예외 정책을 사용해 예외를 관리하십시오.						
DS-13.11	클라이언트 포털	최소한 분기마다 클라이언트 웹 포털에 대한 액세스를 검토하십시오.						

부록 C: AWS의 ASD(호주 신호 관리 위원회) 클라우드 컴퓨팅 보안 규정 준수

클라우드 컴퓨팅 보안 고려 사항은 클라우드 서비스 공급자가 제공하는 서비스에 대한 기관의 위험 평가 수행을 지원하기 위해 개발되었습니다. 다음은 2012년 9월 발표된 AWS의 신호 고려 사항 준수 내역입니다. 자세한 내용은 http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf를 참조하십시오.

주요 영역	질문	AWS 답변
가용성 및 비즈니스 기능 유지	a. 비즈니스에 중요한 데이터 또는 기능. 비즈니스에 중요한 데이터 또는 기능을 클라우드로 이동해도 되겠습니까?	AWS 고객은 자신의 콘텐츠에 대한 관리 권한과 소유권을 보유합니다. 콘텐츠의 분류 및 사용에 대한 책임은 고객에게 있습니다.
	b. 공급업체의 비즈니스 연속성 및 재해 복구 계획. 고객이 사용하는 공급업체 서비스와 고객 데이터 모두에 대한 가용성 및 복원을 포함하는 공급업체의 비즈니스 연속성과 재해 복구 계획의 사본을 고객이 철저히 검토해 볼 수 있습니까? 재해 후 고객이 사용하는 데이터와 서비스를 복구하는 데 얼마의 시간이 걸리며 이 때 공급업체의 규모 큰 다른 고객이나 더 많은 비용을 지불하는 고객을 우선으로 합니까?	AWS 고객은 데이터에 대한 관리 및 소유권을 보유합니다. AWS는 각 리전 내의 여러 가용 영역뿐 아니라 여러 리전 내에 인스턴스를 배치하고 데이터를 저장하는 유연성을 고객들에게 제공합니다. 각 가용 영역은 독립된 장애 영역으로 설계되었습니다. 장애 시 자동화된 프로세스는 고객 데이터 트래픽을 장애 지역에서 먼 곳으로 이동합니다. AWS SOC 1 Type 2 보고서에 자세한 정보가 나와 있습니다. 자세한 내용은 ISO 27001 표준 부록 A, 도메인 11.2를 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증을 준수함을 검증 및 인증받았습니다. 고객은 AWS를 통해 두 번째 물리적 장소에 대한 반복된 인프라 비용 지불 없이 주요 IT 시스템에 대한 신속한 재해 복구가 가능합니다. AWS 클라우드는 즉각적인 확장이 가능한 "파일럿 라이트" 환경부터 신속한 장애 조치가 가능한 "상시 대기" 환경까지, 다양한 주요 재해 복구(DR) 아키텍처를 지원합니다. AWS의 재해 복구에 대해 자세히 알아보려면 http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf를 참조하십시오. AWS는 고객에게 빈번한 서버 인스턴스 백업 활용, 데이터 중복 복제, 다중 리전/가용 영역 배포 아키텍처를 포함한 강력한 연속성 계획을 구현할 수 있는 기능을 제공합니다. AWS는 각 리전 내의 여러 가용 영역뿐 아니라 여러 리전 내에 인스턴스를 배치하고 데이터를 저장하는 유연성을 고객들에게 제공합니다. 각 가용 영역은 독립된 장애 영역으로 설계되었습니다. 장애 시 자동화된 프로세스는 고객 데이터 트래픽을 장애 지역에서 먼 곳으로 이동합니다. AWS 데이터 센터는 환경 위험에 대한 물리적인 보호 조치를 통합합니다. 환경 위험에 대한 AWS의 물리적 보호 조치는 독립적인 감사 기관으로부터 검증을 받았으며 ISO 27002 모범 사례를 준수함을 인증받았습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 9.1항과 AWS SOC 1 Type II 보고서를 참조하십시오.

주요 영역	질문	AWS 답변
	c. 데이터 백업 계획. 기관의 자체 환경에 위치하는 데이터 또는 최초 공급업체에서 발생했던 일반적인 실패 지점이 없는 두 번째 공급업체를 통해 저장된 데이터의 최신 백업 복사본을 유지하는 데 추가 비용이 소요됩니까?	콘텐츠의 관리 권한과 소유권은 AWS 고객에게 있으며 데이터 백업 계획을 관리해야 할 책임 역시 고객에게 있습니다. AWS는 고객이 필요에 따라 AWS 스토리지에서 데이터를 가져오거나 내보낼 수 있도록 허용합니다. S3의 AWS Import/Export 서비스는 데이터 전송 시 이동식 스토리지 디바이스를 사용하여 AWS에서 많은 양의 데이터를 빠르게 송수신할 수 있습니다. AWS는 고객이 자체 테이프 백업 서비스 공급자를 사용해 테이프에 백업할 수 있도록 허용합니다. 그러나 AWS에서는 테이프 백업 서비스를 제공하지 않습니다. Amazon S3 서비스는 데이터 스토리지 중복성을 통해 데이터 손실 가능성을 거의 0%로 낮추고 데이터 객체의 다중 사이트 사본과 동일한 내구성을 보장할 수 있도록 고안되었습니다. 데이터 내구성 및 중복성에 대한 정보는 AWS 웹 사이트를 참조하십시오. AWS는 재해 복구를 지원하기 위한 다양한 클라우드 컴퓨팅 서비스를 제공합니다. AWS의 재해 복구에 대해 자세히 알아보려면 http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf를 참조하십시오.
	d. 비즈니스 연속성과 재해 복구 계획. 첫 번째 공급업체에게 있었던 일반적인 실패 지점이 없으며 다른 데이터 센터를 사용하는 두 번째 공급업체를 통해 데이터나 비즈니스 기능을 복제하려면 추가 비용이 듭니까? 가급적이면 이 복제는 자동으로 "장애 조치"되도록 구성하는 것이 좋습니다. 이렇게 하면 한 공급업체의 서비스를 사용할 수 없는 경우 제어권이 다른 공급업체가 원활하게 자동으로 전환됩니다.	고객은 데이터에 대한 관리 권한과 소유권을 보유합니다. 고객은 AMI를 내보내 온프레미스 또는 다른 공급자에서 사용할 수 있습니다(소프트웨어 라이선스 제한이 적용됨). 자세한 내용은 http://aws.amazon.com/security의 AWS 보안 프로세스 개요 백서를 참조하십시오. AWS는 고객이 필요에 따라 AWS 스토리지에서 데이터를 가져오거나 내보낼 수 있도록 허용합니다. S3의 AWS Import/Export 서비스는 데이터 전송 시 이동식 스토리지 디바이스를 사용하여 AWS에서 많은 양의 데이터를 빠르게 송수신할 수 있습니다. AWS는 고객이 자체 테이프 백업 서비스 공급자를 사용해 테이프에 백업할 수 있도록 허용합니다. 그러나 AWS에서는 테이프 백업 서비스를 제공하지 않습니다. AWS 데이터 센터는 전 세계 여러 리전에 클러스터 형태로 구축됩니다. 모든 데이터 센터는 온라인으로 고객 서비스를 제공하며 "콜드" 상태인 데이터 센터는 없습니다. 가동이 중단되는 경우, 자동화된 프로세스에 따라 고객 데이터 트래픽을 해당 영역에서 운반합니다. 핵심 애플리케이션이 N+1 구성으로 구현되어, 데이터 센터 장애가 발생할 경우에도 나머지 사이트로 트래픽을 균형 있게 분산시킬 수 있는 충분한 용량을 갖추고 있습니다. AWS는 각 리전 내의 여러 가용 영역뿐 아니라 여러 리전 내에 인스턴스를 배치하고 데이터를 저장하는 유연성을 고객들에게 제공합니다. 각 가용 영역은 독립된 장애 영역으로 설계되었습니다. 즉 가용 영역 일반적인 대도시 지역 내에 물리적으로 고립되어 있으며 홍수 위험성이 낮은 지대에 위치합니다(자세한 홍수 지대 분류는 지역에 따라 차이가 있음). 또한, 무정전 전원 공급 장치(UPS)와 현장 백업 발전 시설을 분리하여 독립적인 유틸리티의 서로 다른 그리드를 통해 전력을 공급받음으로써 단일장애점(Single-point-of-Failure)을 더욱 줄여줍니다. 가용 영역은 모두 여러 1계층(tier-1) 전송서비스 공급자들에게 이중으로 연결됩니다. 고객은 다수의 지역 및 가용 영역의 이점을 활용하여 AWS 아키텍처를 구축해야 합니다. 여러 개의 가용 영역에 애플리케이션을 분산함으로써 자연 재해나 시스템 장애 등 대부분의 장애 모드에 직면한 경우에도 시스템을 유지할 수 있게 합니다. AWS SOC 1 Type 2 보고서에 자세한 정보가 나와 있습니다. 자세한 내용은 ISO 27001 표준 부록 A, 도메인 11.2를 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증을 준수함을 검증 및 인증받았습니다.

주요 영역	질문	AWS 답변
	e. 클라우드와의 네트워크 연결. 기관 사용자와 공급업체 네트워크 간의 네트워크 연결은 가용성, 트래픽 처리량(대역폭), 지연 시간 및 패킷 손실 면에서 적절합니까?	고객은 각 AWS 리전의 여러 VPN 엔드포인트를 포함하여 AWS 시설에 연결되는 네트워크 경로를 선택할 수도 있습니다. 또한, AWS Direct Connect를 사용하면 고객 자체 환경에서 AWS로 전용 네트워크 연결을 쉽게 설정할 수 있습니다. AWS Direct Connect를 사용하면 AWS와 사용자의 데이터 센터, 사무실, 또는 콜로케이션 환경 사이에 프라이빗 연결을 설정할 수 있습니다. 따라서 많은 경우 네트워크 비용이 줄고, 대역폭 처리량이 늘어나고, 인터넷 기반 연결보다 좀 더 일관된 네트워크 환경이 제공됩니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
	f. 공급업체의 가용성 보장. SLA(서비스 수준 계약)에서 공급업체가 견고한 자체 시스템 아키텍처와 비즈니스 프로세스를 사용하여 적정 시스템 가용성과 서비스 품질을 제공할 것을 보장합니까?	AWS는 SLA(서비스 수준 계약)를 통해 높은 수준의 가용성을 제공하기 위해 노력합니다. 예를 들어, Amazon EC2는 서비스 기간 동안 연간 최소 99.95% 이상의 가동률을 제공합니다. Amazon S3는 매달 최소한 99.99% 이상의 가동률을 제공합니다. 이러한 가용성 측정치가 충족되지 않을 경우 서비스 크레딧을 제공합니다. 고객은 다수의 지역 및 가용 영역의 이점을 활용하여 AWS 아키텍처를 구축해야 합니다. 여러 개의 가용 영역에 애플리케이션을 분산함으로써 자연 재해나 시스템 장애 등 대부분의 장애 모드에 직면한 경우에도 시스템을 유지할 수 있게 합니다. AWS는 높은 수준의 서비스 성능 및 가용성을 제공하기 위해 자동화된 모니터링 시스템을 활용합니다. 내외부용의 다양한 온라인 도구를 통해 사전 모니터링이 가능합니다. AWS 내 시스템은 주요 운영 측정치를 모니터링하기 위해 광범위하게 활용됩니다. 주요 운영 메트릭에서 초기 경고 임계값을 초과하는 경우 운영관리 담당자에게 통보하도록 경보가 구성됩니다. 전화 상담 일정을 구성해 담당자가 항상 운영 문제에 대응할 수 있게 합니다. 무선 호출 시스템을 통해 경보가 신속하고 안정적으로 운영 담당자에게 전달되도록 합니다. AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP^{sm} 준수의 일환으로, 정기적으로 외부의 독립적 감사 기관으로부터 AWS 네트워크 관리를 검토 받습니다.
	g. 중단의 영향. SLA의 최대 중단 시간은 얼마나 됩니까? 예약된 중단 시간이 기간과 시간 면에서 모두 허용 가능합니까? 아니면 예약된 중단으로 인해 나의 주요 비즈니스 프로세스가 방해를 받습니까?	AWS 고객은 정기 유지보수 및 시스템 패치 적용을 위해 시스템을 오프라인으로 전환하지 않아도 됩니다. AWS의 자체 유지보수 및 시스템 패치 적용은 일반적으로 고객에게 영향을 미치지 않습니다. 인스턴스 유지보수는 고객이 관리합니다.
	h. SLA에 예약 중단 포함 여부. SLA 보증 가용성 백분율에 예정된 정기 중단이 포함됩니까?	AWS에서는 고객에게 여러 가용 영역과 리전을 활용할 수 있도록 환경을 구성할 수 있는 기능을 제공하므로 중단이 예약된 환경을 운영하지 않습니다.

주요 영역	질문	AWS 답변
	i. SLA 보상. SLA에는 갑작스런 중단 시간이나 데이터 손실 등 SLA 위반으로 인한 실제 손해가 적절히 반영됩니까?	AWS는 AWS의 서비스 수준 협약에 따라 중단으로 인해 발생할 수 있는 손실을 보상합니다.
	j. 데이터 무결성 및 가용성. 공급업체에서는 손상이나 데이터 손실을 방지하기 위한 중복성 및 오프사이트 백업 등의 메커니즘을 어떻게 구현하며 내 데이터의 무결성 및 가용성을 어떻게 보장합니까?	AWS SOC 1 Type II 보고서에 설명된 것처럼 AWS 데이터 무결성 컨트롤은 전송, 저장 및 처리를 포함한 모든 단계에서 데이터 무결성이 유지됨을 합리적으로 보증합니다. ISO 27001 표준, 부록 A, 12.2항에서도 자세한 내용을 확인하실 수 있습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. 데이터 센터는 전 세계 여러 리전에 클러스터 형태로 구축됩니다. AWS는 각 리전 내의 여러 가용 영역뿐 아니라 여러 리전 내에 인스턴스를 배치하고 데이터를 저장하는 유연성을 고객들에게 제공합니다. 고객은 다수의 리전 및 가용 영역의 이점을 활용하여 AWS 아키텍처를 구축해야 합니다. 리전(Amazon S3용)이나 리전 내 가용 영역(EBS용)을 지정하여 데이터를 저장할 위치를 선택할 수 있습니다. Amazon EBS에 저장된 데이터는 정규 서비스 작업의 일부로 추가 비용 없이 여러 물리적 위치에 중복 저장됩니다. 그러나 Amazon EBS 복제본은 여러 영역이 아닌 동일한 가용 영역 안에 저장됩니다. Amazon S3는 내구성이 뛰어난 스토리지 인프라를 제공합니다. 객체는 Amazon S3 리전에서 여러 시설의 다양한 디바이스에 중복 저장됩니다. 데이터가 저장되면 Amazon S3가 손실된 중복성을 빠르게 검색 및 복원하여 객체의 내구성을 유지합니다. 또한 Amazon S3는 체크섬을 사용해 저장된 데이터의 무결성을 정기적으로 검사합니다. 손상이 감지된 경우 중복 데이터를 사용하여 복원합니다. S3에 저장된 데이터는 연간 99.999999999%의 내구성과 99.99%의 객체 가용성을 제공하도록 설계되었습니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
	k. 데이터 복원. 사용자가 실수로 파일, 이메일 또는 기타 데이터를 삭제하는 경우, 이러한 데이터를 백업에서 부분적으로 또는 완전히 복원하는 데 걸리는 시간은 얼마이며, SLA에 규정된 최대 허용 시간은 얼마입니까?	AWS 고객은 데이터에 대한 관리 및 소유권을 보유합니다. AWS는 각 리전 내의 여러 가용 영역뿐 아니라 여러 리전 내에 인스턴스를 배치하고 데이터를 저장하는 유연성을 고객들에게 제공합니다.

주요 영역	질문	AWS 답변
	l. 확장성. 사용자가 공급업체 서비스 사용량을 예고 없이 확장할 수 있도록 하기 위해 공급업체에서 제공하는 예비 컴퓨팅 리소스의 양을 얼마나 됩니까?	AWS 클라우드는 매우 안전하고 복원력이 뛰어난 분산형 시스템으로, 고객에게 대규모 확장 역량을 제공합니다. 고객은 시스템을 수직 또는 수평으로 확장할 수 있으며 사용한 용량에 대해서만 비용을 지불합니다.
	m. 공급업체 변경. 기관이나 다른 공급업체로 데이터를 이동하려는 경우 또는 공급업체가 갑자기 파산하거나 클라우드 사업을 그만두는 경우, 공급업체에 대한 고착화를 방지하기 위해 공급업체와 무관한 형식으로 데이터에 액세스하려면 어떻게 해야 합니까? 공급업체는 얼마나 적극적으로 협조할 것 같습니까? 공급업체의 스토리지 미디어에서 데이터가 영구적으로 삭제된 것을 어떻게 확인합니까? PaaS(Platform as a Service)의 경우, 애플리케이션을 다른 공급업체나 기관으로 쉽게 이동할 수 있도록 공급업체에서 사용하는 이식성 및 상호 운용성 지원 표준은 무엇입니까?	고객은 데이터에 대한 관리 권한과 소유권을 보유합니다. 고객은 AMI를 내보내 온프레미스 또는 다른 공급자에서 사용할 수 있습니다(소프트웨어 라이선스 제한이 적용됨). 자세한 내용은 http://aws.amazon.com/security의 AWS 보안 프로세스 개요 백서를 참조하십시오. AWS는 고객이 필요에 따라 AWS 스토리지에서 데이터를 가져오거나 내보낼 수 있도록 허용합니다. S3의 AWS Import/Export 서비스는 데이터 전송 시 이동식 스토리지 디바이스를 사용하여 AWS에서 많은 양의 데이터를 빠르게 송수신할 수 있습니다. AWS는 고객이 자체 테이프 백업 서비스 공급자를 사용해 테이프에 백업할 수 있도록 허용합니다. 그러나 AWS에서는 테이프 백업 서비스를 제공하지 않습니다.

주요 영역	질문	AWS 답변
타사의 무단 액세스로부터 데이터 보호	a. 클라우드 배포 모델 선택권. 보안성이 다소 떨어질 수 있는 퍼블릭 클라우드, 보안성이 좀 더 높은 하이브리드 클라우드 또는 커뮤니티 클라우드 또는 보안성이 매우 뛰어난 프라이빗 클라우드 중 어느 것을 고려해 보아야 합니까?	AWS 규정 준수 및 보안 팀은 COBIT(Control Objectives for Information and related Technology) 프레임워크를 기반으로 정보 보안 프레임워크 및 정책을 구축했습니다. AWS 보안 프레임워크는 ISO 27002 모범 사례와 PCI 데이터 보안 표준을 통합합니다. 자세한 내용은 http://aws.amazon.com/security 에서 AWS 위험 및 규정 준수 백서를 참조하십시오.AWS는 NDA에 의거하여 제3자 증명, 인증, Service Organization Controls 1(SOC 1) Type II 보고서 및 기타 관련 규정 준수 보고서를 고객에게 직접 제공합니다. Amazon Virtual Private Cloud(VPC)는 고객이 정의하는 가상 네트워크에서 AWS 리소스를 시작할 수 있도록 Amazon Web Services(AWS) 클라우드에서 논리적이고도 격리된 공간을 프로비저닝합니다. IP 주소 범위, 서브넷 생성, 라우팅 테이블 및 네트워크 게이트웨이 구성 선택 등 가상 네트워킹 환경을 완벽하게 제어할 수 있습니다. Amazon VPC에 대한 네트워크 구성을 손쉽게 사용자 지정할 수 있습니다. 예를 들어, 인터넷에 액세스하는 웹 서버에 대해 공용 페이싱 서브넷을 생성하고 인터넷 액세스가 없는 개인 페이싱 서브넷의 애플리케이션 서버나 데이터베이스 등의 백엔드 시스템을 배치할 수 있습니다. 보안 그룹 및 네트워크 액세스 제어 목록을 포함한 다중 보안 계층을 활용하여 각 서브넷에서 Amazon EC2 인스턴스에 대한 액세스를 제어하도록 지원할 수 있습니다. 또한, 고객의 회사 데이터 센터와 VPC 사이에 하드웨어 VPN(가상 프라이빗 네트워크) 연결을 생성하여 AWS 클라우드를 사내 데이터 센터의 확장으로 활용할 수 있습니다.
	b. 데이터의 중요성. 클라우드에서 저장되거나 처리될 데이터가 중요 데이터, 프라이빗 데이터 또는 퍼블릭 웹 사이트의 정보 등 공개적으로 이용할 수 있는 데이터로 분류됩니까? 집계된 데이터가 개별 데이터보다 더 중요합니까? 예를 들어 많은 양의 데이터를 저장하거나 손상된 경우 자격 증명 도용에 이용되기 쉬운 다양한 데이터를 저장하는 경우 중요도가 높아질 수 있습니다. 데이터가 손상될 경우 고위 경영진, 정부 공무원 또는 대중에게 자신이 상당한 주의를 기울였다는 사실을 입증할 수 있습니까?	AWS 고객은 데이터에 대한 관리 권한과 소유권을 보유하며 각자의 요건에 부합하는 구조화된 데이터 분류 프로그램을 구현할 수 있습니다.

주요 영역	질문	AWS 답변
	c. 법적 의무. 다양한 법률, 즉 개인 정보 보호법, 보관법, 데이터 유형별 기타 법률 등 다양한 법률에 따라 데이터를 보호하고 관리해야 하는 경우 어떤 의무가 부과됩니까? 공급업체에서는 고객의 이러한 의무가 오스트레일리아 정부의 요구를 충족할 수 있도록 이러한 의무의 준수를 계약적으로 수용합니까?	AWS 고객은 준거법과 규정을 준수하는 범위 내에서 AWS를 사용할 책임이 있습니다. AWS는 산업 인증, 제3자 증명, 백서(http://aws.amazon.com/security에서 제공)를 통해 고객에게 보안 및 제어 환경을 전달하고, AWS 고객에게 직접 인증, 보고서 및 기타 관련 문서를 제공합니다. AWS는 오스트레일리아 개인 정보 고려 사항과 관련하여 AWS 사용에 대한 백서를 발표했습니다. 이 백서는 http://d0.awsstatic.com/whitepapersp/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf에서 다운로드할 수 있습니다.
	d. 내 데이터에 액세스할 수 있는 국가. 내 데이터는 어느 국가에서 저장, 백업 및 처리됩니까? 데이터가 일시적으로 전달되는 해외 국가는 어디입니까? 장애 조치나 중복 데이터 센터는 어느 국가에 있습니까? 공급업체에서 이러한 질문에 대한 답변이 변경되는 경우 고객에게 알려 줍니까?	AWS 고객은 콘텐츠 및 서버가 위치하는 리전이나 AWS 리전을 선택합니다. 이렇게 하면 지리적 특정 요구 사항을 가진 고객이 선택한 위치에서 환경을 설정할 수 있습니다. 오스트레일리아의 AWS 고객은 아시아 태평양(시드니) 리전에만 AWS 서비스를 전적으로 배포하고 오스트레일리아 내륙에 콘텐츠를 저장할 수 있습니다. 고객이 이와 같인 선택하는 경우 고객이 데이터를 이동하기로 한 경우가 아니면 고객의 콘텐츠는 오스트레일리아에 위치합니다. 고객은 두 개 이상의 리전에 콘텐츠를 복제 및 백업할 수 있지만, AWS에서는 고객이 선택한 리전 외부로 고객의 콘텐츠를 이동하거나 복제하지 않습니다. AWS는 고객의 보안 유지를 위해 최선을 다하며, 소환장이나 법원 명령서 등 법적으로 유효하고 구속력이 있는 명령서나 해당 법률에서 요구를 준수하기 위해 법적으로 해당 조치가 필요한 경우가 아니면 오스트레일리아, 미국 또는 기타 정부의 요청에 응하여 데이터를 공개하거나 이동하지 않습니다. 미국 이외의 정부 또는 규제 기관은 일반적으로 미국 정부와의 사법 공조 조약(Mutual Legal Assistance Treaties) 등 인정된 국제 프로세스를 통해 유효하고 구속력 있는 명령서를 취득합니다. 또한, 당사에서는 법적으로 금지된 경우가 아니면 공개로부터 보호를 받을 수 있도록 콘텐츠를 공개하기 전에 가능하면 고객에게 알리는 것을 업무 방침으로 하고 있습니다.

주요 영역	질문	AWS 답변
	e. 데이터 암호화 기술. 네트워크에서 데이터가 전송 중일 때 데이터를 보호하는 데 DSD ISM에 의해 적절한 것으로 간주되는 해시 알고리즘, 암호화 알고리즘 및 키 길이가 사용되며, 공급업체의 컴퓨터와 백업 미디어에 모두 저장됩니까? 컴퓨터에서 처리되는 동안 데이터를 암호화할 수 있는 기능은 아직까지는 최신 기술이며 업계 및 학계에서 현재 연구 중인 분야입니다. 데이터가 중요시 되는 기간 동안 데이터를 보호할 수 있을 만큼 암호화가 충분히 강력합니까?	AWS는 고객이 S3, EBS, SimpleDB, EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있도록 지원합니다. VPC 세션도 암호화됩니다. Amazon S3도 고객을 위한 옵션으로 Server Side Encryption을 제공합니다. 고객은 제3자 암호화 기술을 사용할 수도 있습니다. 내부적으로 AWS는 AWS 인프라 내에서 사용되는 필수 암호화용 암호화 키를 설정하고 관리합니다. AWS는 AWS 정보 시스템에서 NIST 승인 키 관리 기술 및 프로세스를 사용하여 대칭적 암호화 키를 생성, 제어 및 배포합니다. AWS에서 개발한 보안 키 및 자격 증명 관리자를 사용하여 대칭적 키를 생성, 보호, 배포하는 한편, 호스트에서 필요한 AWS 자격 증명, RSA 프라이빗/퍼블릭 키 및 X.509 자격 증명을 보호하고 배포합니다. AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수를 위해 외부의 독립적 감사 기관으로부터 AWS 암호화 프로세스를 검토 받습니다. AWS CloudHSM 서비스로 사용자는 안전한 키 관리를 위한 정부 표준에 따라 설계되고 검증된 HSM 내의 암호화 키를 보호할 수 있습니다. 데이터 암호화에 사용한 암호화 키를 안전하게 생성, 저장 및 관리할 수 있으며 이 경우, 사용자만 자신의 암호화 키를 사용할 수 있습니다. AWS CloudHSM은 애플리케이션 성능에 지장을 주지 않고 엄격한 키 관리 요건을 준수하는데 도움이 됩니다. AWS CloudHSM 서비스는 Amazon Virtual Private Cloud(VPC)와 작동합니다. CloudHSM은 사용자가 지정하는 IP 주소를 사용하여 VPC에 프로비저닝되어 사용자의 Amazon Elastic Compute Cloud(EC2) 인스턴스에 대한 간단하고 개별적인 네트워크 연결을 제공합니다. EC2 인스턴스 근처에 CloudHSM을 배치하면 네트워크 지연이 감소하여 애플리케이션 성능을 개선할 수 있습니다. AWS는 다른 AWS 고객과 분리된 CloudHSM에 대한 독점적인 액세스를 제공합니다. 여러 리전 및 가용 지역(AZ)에서 사용 가능한 AWS CloudHSM으로 안전하고 내구성 있는 키 스토리지를 Amazon EC2 애플리케이션에 추가할 수 있습니다.
	f. 미디어 폐기. 수명이 다 되었을 때 데이터가 저장되어 있는 스토리지 미디어를 폐기하는 데 사용되는 프로세스는 무엇이며 해당 프로세스가 DSD ISM에 의해 적절한 것으로 간주되는 프로세스입니까?	스토리지 디바이스의 수명이 다했을 경우 권한이 없는 개인에게 고객 데이터가 노출되는 것을 방지하기 위해 고안된 폐기 프로세스가 AWS 내에 마련되어 있습니다. AWS는 DoD 5220.22-M("국가 산업 보안 프로그램 운영 매뉴얼") 또는 NIST 800-88("미디어 삭제 가이드라인")에서 설명하는 기술을 사용해 폐기 프로세스에 따라 데이터를 제거합니다. 이 절차를 사용하여 하드웨어 디바이스를 폐기할 수 없는 경우 산업 표준 관행에 따라 디바이스의 저장을 제거하거나 디바이스를 물리적으로 파괴합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.

주요 영역	질문	AWS 답변
	g. 공급업체의 원격 모니터링 및 관리. 공급업체에서 데이터를 저장하거나 처리하는 컴퓨터를 모니터링하거나 관리합니까? 그렇다면 이러한 작업이 오스트레일리아나 해외에서 원격으로 수행됩니까? 공급업체에서 이 작업을 수행하는 데 사용되는 워크스테이션의 보안에 대한 패치 규정 준수 보고서 및 기타 세부 정보를 제공할 수 있습니까? 그리고 공급업체 직원의 신뢰할 수 없는 개인 소유 랩톱 사용을 금지하는 제어 수단은 무엇입니까?	IT 인프라를 AWS 서비스로 이전할 경우 고객과 AWS 간에 책임 공유 모델이 만들어집니다. 이 공유 모델을 통해 고객사는 운영 부담을 덜 수 있습니다. 그 이유는 AWS에서 호스트 운영 체제 및 가상화 계층부터 서비스 운영 시설의 물리적 보안에 이르기까지 구성 요소를 운영, 관리, 규제하기 때문입니다. 고객의 책임 및 관리 범위에는 AWS가 제공하는 보안 그룹 방화벽의 구성과 게스트 운영 체제(업데이트 및 보안 패치 포함) 및 기타 관련 애플리케이션 소프트웨어가 포함됩니다.
	h. 고객의 자체적 모니터링 및 관리. 고객은 이러한 시스템이 로컬에 있든 아니면 클라우드에 있든 관계 없이 모든 시스템을 파악하기 위해 무결성 확인, 규정 준수 확인, 보안 모니터링 및 네트워크 관리용 기존 도구를 사용할 수 있습니까? 공급업체에서 제공하는 추가 도구를 사용하는 방법을 배워야 합니까? 공급업체에서 제가 자체적으로 모니터링하는 데 사용할 수 있는 메커니즘 등을 제공할 수 있습니까?	AWS Cloudwatch는 고객이 AWS에서 실행하는 AWS 클라우드 리소스와 애플리케이션을 모니터링합니다. 자세한 내용은 aws.amazon.com/cloudwatch를 참조하십시오. AWS는 서비스 상태 대시보드에 서비스 가용성에 대한 최신 정보도 게시합니다. status.aws.amazon.com을 참조하십시오 AWS Trusted Advisor는 고객의 AWS 환경을 검사하고 비용 절감, 시스템 성능 및 신뢰성 개선 또는 보안 격차를 해결할 기회가 생기면 이를 권장합니다.
	i. 데이터 소유권. 공급업체가 파산하는 경우 데이터의 소유권은 고객에게 있습니까? 아니면 공급업체에 귀속되어 청산인에 의해 매각될 자산으로 간주될 수 있습니까?	AWS 고객은 데이터에 대한 소유권과 관리 권한을 보유합니다. AWS에서는 각 고객이 선택한 AWS 서비스를 해당 고객에게 제공하는 데만 각 고객의 콘텐츠를 사용할 뿐 부수적 목적을 위해 고객의 콘텐츠를 사용하지 않습니다. AWS는 모든 고객의 콘텐츠를 동일하게 취급하며 AWS에서 저장하기로 선택한 콘텐츠의 유형을 파악하지 않습니다. AWS에서는 고객이 선택한 컴퓨팅, 스토리지, 데이터베이스 및 네트워킹 서비스를 단순히 가용화할 뿐이므로, 서비스를 제공하기 위해 고객에 콘텐츠에 액세스할 필요가 없습니다.

주요 영역	질문	AWS 답변
	j. 게이트웨이 기술. 공급업체에서는 보안 게이트웨이 환경을 구축하는 데 어떤 기술을 사용합니까? 예를 들어 방화벽, 트래픽 흐름 필터, 콘텐츠 필터 및 안티바이러스 소프트웨어 및 데이터 다이오드 등이 있습니다.	AWS 네트워크는 기존의 네트워크 보안 문제와 관련하여 중요한 보호 방법을 제공합니다. 고객은 추가 보호 방법을 실행할 수도 있습니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 개요 백서를 참조하십시오. Amazon 자산(예: 랩톱)은 이메일 필터링 및 맬웨어 탐지를 포함하는 안티바이러스 소프트웨어로 구성됩니다. AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP[sm] 준수의 일환으로, 외부의 독립적 감사 기관으로부터 AWS 네트워크 방화벽 관리 및 Amazon의 안티바이러스 프로그램을 검토 받습니다.
	k. 게이트웨이 인증. 공급업체의 게이트웨이 환경이 정부 보안 표준 및 규정에 대해 인증을 받았습니까?	AWS는 AWS 게이트웨이 환경을 포함하는 특정 산업 인증 및 독립적인 타사 인증을 획득했습니다.
	l. 이메일 콘텐츠 필터링. 이메일 SaaS(Software as a Service)의 경우 공급업체에서 우리 기관의 이메일 콘텐츠 정책을 적용할 수 있는 사용자 지정 가능한 이메일 콘텐츠 필터링을 제공합니까?	고객은 시스템을 사용하여 이메일 기능을 호스팅할 수 있지만, 이 경우 이메일 진입 및 진출 지점에서의 적절한 스팸 및 맬웨어 보호 수준을 사용하고 새 릴리스를 사용할 수 있을 때 스팸 및 맬웨어 정의를 업데이트하는 일은 고객의 책임입니다.

주요 영역	질문	AWS 답변
	m. 공급업체의 IT 보안 태세를 지원하는 정책 및 프로세스. 컴퓨터와 네트워크 보안 태세가 위협 및 위험 평가, 지속적인 취약성 관리, 변경 관리 프로세스(보안, 침투 테스트, 로깅 및 정규 로그 분석이 통합됨), 오스트레일리아 정부가 보증하는 보안 제품의 사용, 오스트레일리아 정부 보안 표준 및 규정 준수를 포함하여 정책 및 프로세스에 의해 어떻게 지원되는지에 대한 자세한 정보를 얻을 수 있습니까?	COBIT 프레임워크, ISO 27001 표준 및 PCI DSS 요건을 기반으로 AWS 정보 보안을 통해 정책 및 절차가 확립되었습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. 또한 AWS는 SOC 1 Type II 보고서를 발행합니다. 자세한 내용은 SOC 1 보고서를 참조하십시오. 자세한 내용은 http://aws.amazon.com/security에서 AWS 위험 및 규정 준수 백서를 참조하십시오. AWS 고객은 AWS에서 관리하는 주요 컨트롤을 식별할 수 있습니다. 주요 컨트롤은 고객의 제어 환경에 매우 중요하며, 연례 재무 감사와 같은 규정 준수 요건을 준수하기 위해 이러한 주요 컨트롤의 외부 운영 효과 증명이 필요합니다. 이러한 목적으로 AWS는 서비스 조직 규제 1(SOC 1) 유형 II 보고서에 다양하고 구체적인 IT 컨트롤을 게재합니다. 구 SAS(Statement on Auditing Standards) 제70호인 SOC 1 보고서는 SSAE 16(Statement on Standards for Attestation Engagements No. 16)이라는 이름으로 알려져 있으며, 미국 공인회계사 협회(AICPA)가 개발한 감사 표준으로 널리 통용되고 있습니다. SOC 1 감사는 AWS에서 정의한 제어 목표 및 제어 활동(인프라 AWS 관리의 일부에 대한 제어 목표 및 제어 활동 포함)의 설계 및 운영 효과 모두를 심층적으로 감사합니다. “Type II”란 보고서에 설명된 각 컨트롤에 대해 외부 감사자가 설계 정확도 평가를 수행할 뿐 아니라 운영 효과 테스트도 실시한다는 사실을 나타냅니다. AWS에서 지정한 외부 감사자는 독립성과 역량을 갖추고 있으므로 보고서에서 식별된 컨트롤이 AWS의 제어 환경에서 높은 수준의 신뢰성을 제공해야 합니다.
	n. 공급업체의 IT 보안 태세 지원 기술. 공급업체의 컴퓨터 및 네트워크 보안 태세가 보안 패치 적용, 정기적인 안티바이러스 업데이트, 알 수 없는 취약성을 보호하는 심층 방어 메커니즘, 가장 강력한 보안 설정으로 구성된 강화된 운영 체제 및 소프트웨어 애플리케이션, 침입 탐지/방지 시스템 및 데이터 손실 방지 메커니즘 등 직접적인 기술 통제 수단에 의해 어떻게 지원되는지에 대한 자세한 정보를 얻을 수 있습니까?	AWS는 NDA에 의거하여 제3자 증명, 인증, Service Organization Controls 1(SOC 1) Type II 보고서 및 기타 관련 규정 준수 보고서를 고객에게 직접 제공합니다. AWS 보안 팀은 정기적으로 모든 인터넷 연결 서비스 endpoint IP 주소를 검사하여 취약성이 있는지 확인합니다(이러한 검사에는 고객 인스턴스가 포함되지 않음). AWS 보안 팀은 확인된 취약성을 해결하기 위해 해당 당사자에게 취약성을 알립니다. 또한 독립적인 보안 회사에서 정기적으로 외부 취약성 위협 평가를 수행합니다. 이러한 평가 결과 확인된 내용과 권장사항이 범주화되어 AWS 책임자에게 전달됩니다. 또한 AWS 제어 환경은 정기적인 내부 및 외부 위험 평가를 거칩니다. AWS는 외부 인증 기관 및 독립 감사자와 협력하여 AWS 전체 제어 환경을 검토하고 테스트합니다.

주요 영역	질문	AWS 답변
	o. 공급업체의 IT 보안 태세 감사. 고객에게 제공되는 환경에 대한 검사 및 기타 침투 테스트 수행 등 공급업체의 보안 대책 구현 상태를 고객이 감사할 수 있습니까? 감사가 불가능한 타당한 이유가 있는 경우 감사 및 기타 취약성 평가를 실시하는 유명 타사 감사 기관은 어디입니까? 공급업체에서 실시하는 내부 감사에는 어떤 것이 있으며 이러한 평가에 사용되는 규정 표준과 조직의 기타 권장 관행(Cloud Security Alliance 등)은 무엇입니까? 최근 결과 보고서의 사본을 고객이 자세히 검토해 볼 수 있습니까?	AWS는 NDA에 의거하여 제3자 증명, 인증, Service Organization Controls 1(SOC 1) Type II 보고서 및 기타 관련 규정 준수 보고서를 고객에게 직접 제공합니다. 고객은 검사가 고객의 인스턴스에 국한되고 AWS Acceptable Use Policy를 위반하지 않는 범위에서 클라우드 인프라 검사를 수행할 수 있는 권한을 요청할 수 있습니다. AWS 취약성/침투 테스트 요청 양식을 통해 요청을 제출하여 이러한 유형의 검사에 대한 사전 승인을 얻을 수 있습니다. AWS 보안 팀은 정기적으로 독립적인 보안 회사와 협력하여 외부 취약성 위협 평가를 수행합니다. AWS SOC 1 Type 2 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다.
	p. 사용자 인증. 공급업체에서는 SaaS(Software as a Service)를 사용하기 위해 로그인하는 사용자를 위해 어떤 자격 증명 및 액세스 관리 시스템을 지원합니까?	AWS Identity and Access Management(IAM)를 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. AWS는 자격 증명을 단일 위치에서 관리하여 사용자를 보다 쉽게 관리할 수 있는 자격 증명 연동을 지원합니다. AWS IAM에는 SAML(Security Assertion Markup Language) 2.0이라는 여러 자격 증명 공급자가 사용하는 개방형 표준에 대한 지원이 포함합니다. 이 새로운 기능을 사용하면 사용자에게 권한을 부여하는 연동된 Single Sign-On 또는 SSO를 통해 AWS Management Console에 로그인하거나 Shibboleth 및 Windows Active Directory 연동 서비스와 같은 SAML 호환 자격 증명 공급자의 어설션을 사용하여 AWS API에 대한 프로그래밍 호출을 작성할 수 있습니다.
	q. 중앙 집중식 데이터 제어. SaaS(Software as a Service)를 사용하여 액세스되는 중요 데이터를 저장하거나 처리할 때 기관의 사용자가 신뢰할 수 있는 운영 체제를 사용하지 않는 비승인 또는 비보안 컴퓨팅 디바이스를 사용할 수 없도록 제한하는 사용자 교육, 정책 및 기술 통제 수단은 무엇입니까?	해당 사항 없음

주요 영역	질문	AWS 답변
	r. 공급업체의 물리적 보안 태세. 공급업체는 오스트레일리아 정부에서 보증하는 물리적 보안 제품 및 디바이스를 사용합니까? 공급업체의 물리적 데이터 센터는 서버, 인프라 및 위의 제품 및 디바이스에 저장된 데이터 훼손이나 도난을 방지하기 위해 어떻게 설계되었습니까? 권위 있는 타사에서 인증하는 공급업체의 물리적 데이터 센터입니까?	AWS에서 정의한 논리적 및 물리적 컨트롤의 정의가 SOC 1 Type II 보고서(SSAE 16)에 문서화되어 있으며, 감사 및 규정 준수 팀이 검토를 진행할 때 이 보고서를 이용할 수 있습니다. AWS ISO 27001과 기타 인증도 감사자가 검토에 이용할 수 있습니다. 물리적 보안 컨트롤에는 울타리, 벽, 보안 직원, 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단(단, 이에 제한되지 않음)과 같은 경계 컨트롤이 포함됩니다. 건물 주변과 진입점에서 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단(단, 이에 제한되지 않음)을 활용하여 전문 보안 직원이 물리적인 접근을 엄격하게 통제하십시오. 허가받은 직원이 데이터 센터에 접근하려면 2가지 요소를 이용한 신원확인과정을 최소 두 번 통과해야 합니다. 서버 위치에 접근할 수 있는 물리적 액세스 지점은 AWS 데이터 센터 물리적 보안 정책에 정의된 대로 폐쇄 회로 TV 카메라(CCTV)로 촬영됩니다. 법률 또는 계약 의무 조항에서 30일로 제한하지 않은 경우 영상은 90일간 보관됩니다 AWS는 합법적인 사업 목적으로 이러한 권한이 필요한 계약업체와 직원에게만 데이터 센터 접근 권한 및 정보를 제공합니다. 모든 방문자는 신분증을 제시해야 하며, 통과한 후에는 승인된 직원의 안내를 받습니다. 물리적 접근과 관련된 특정 통제 수단, 데이터 센터 접근 권한 부여 및 기타 관련 통제 수단에 대한 자세한 내용은 SOC 1 Type II 보고서를 참조하십시오. 자세한 내용은 ISO 27001 표준, 부록 A, 9.1항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	s. 소프트웨어 및 하드웨어 조달. 클라우드 인프라 소프트웨어 및 하드웨어가 적법한 출처에 의해 공급되었으며 운송 중에 악의적으로 수정되지 않도록 하는 데 어떠한 조달 프로세스가 사용됩니까?	ISO 27001 표준에 따라 AWS 하드웨어 자산이 소유자에게 할당되며 AWS 담당자가 AWS의 독점적인 재고 관리 도구를 사용해 자산을 추적 및 모니터링합니다. AWS 조달 및 공급망 팀은 모든 AWS 공급업체와의 관계를 유지합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 7.1항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.

주요 영역	질문	AWS 답변
공급업체의 고객에 의한 무단 액세스로부터 데이터 보호	a. 고객 분리. 가상화 및 "다중 테넌트" 메커니즘을 통해 여러 테넌트 간에 논리적 분리 및 네트워크 분리가 적절히 이루어지므로 나와 동일한 물리적 컴퓨터를 사용하는 악의적인 고객이 내 데이터에 액세스할 수 없음을 어떻게 보장합니까	Amazon EC2는 현재 고도로 맞춤화된 Xen 하이퍼바이저를 사용합니다. 하이퍼바이저는 내부 및 외부 침투 팀에서 정기적인 평가를 통해 새로운 취약성 및 기존 취약성이 있는지 확인하며, 게스트 가상 머신 사이에서 강력한 격리를 유지하는 데 매우 적합합니다. AWS Xen 하이퍼바이저 보안은 평가 및 감사 도중 독립 감사자가 정기적으로 평가합니다. 고객을 대신해 AWS에 저장된 모든 데이터는 강력한 테넌트 격리 보안 및 제어 기능을 갖고 있습니다. 고객은 데이터에 대한 관리 및 소유권을 보유하므로 데이터 암호화 선택은 고객의 책임입니다. AWS는 고객이 S3, EBS 및 EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있도록 지원합니다. VPC 세션도 암호화됩니다. Amazon S3도 고객을 위한 옵션으로 Server Side Encryption을 제공합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 위험 및 규정 준수 백서를 참조하십시오.
	b. 보안 태세 약화. 공급업체의 클라우드 인프라 사용이 기관의 기존 네트워크 보안 태세를 어떻게 약화시킵니까? 공급업체가 고객의 명시적 승인 없이 특정 고객을 공개하여 특별히 해당 고객을 대상으로 하는 상대방을 도와줄 수도 있습니까?	AWS 고객은 기밀 사항으로 간주되므로 명시적 승인 없이는 고객 정보가 공개되지 않습니다. Amazon Virtual Private Cloud(VPC)는 고객이 정의하는 가상 네트워크에서 AWS 리소스를 시작할 수 있도록 Amazon Web Services(AWS) 클라우드에서 논리적이고도 격리된 공간을 프로비저닝합니다. IP 주소 범위, 서브넷 생성, 라우팅 테이블 및 네트워크 게이트웨이 구성 선택 등 가상 네트워킹 환경을 완벽하게 제어할 수 있습니다.
	c. 전용 서버. 가상 머신이 실행되는 물리적 컴퓨터를 고객이 제어할 수 있습니까? 별도의 비용을 지불하여 전용 서버나 가상 프라이빗 클라우드 등 다른 고객이 동일한 물리적 컴퓨터를 사용할 수 없도록 할 수 있습니까?	VPC에서는 고객이 호스트 하드웨어 수준에서 물리적으로 분리된 Amazon EC2 인스턴스를 시작할 수 있습니다. 이러한 인스턴스는 단일 테넌트 하드웨어에서 실행됩니다. VPC를 '전용' 테넌시로 지정하는 경우, VPC에서 시작되는 모든 인스턴스가 이 기능을 활용합니다. 또는 VPC를 '기본' 테넌시로 생성할 수 있습니다. 하지만 고객은 VPC에서 시작되는 특정 인스턴스를 '전용' 테넌시로 지정할 수도 있습니다.
	d. 미디어 폐기. 내가 데이터의 일부를 삭제하는 경우 다른 고객에게 가용 공간으로 제공되기 전에 스토리지 미디어를 폐기하는 데 사용되는 프로세스는 무엇이며 해당 프로세스가 DSD ISM에 의해 적절한 것으로 간주되는 프로세스입니까?	고객은 자신의 콘텐츠에 대한 소유권 및 관리 권한을 보유하고 있으며 고객에게는 데이터 삭제 기능이 제공됩니다. 스토리지 디바이스의 수명이 다했을 경우 권한이 없는 개인에게 고객 데이터가 노출되는 것을 방지하기 위해 고안된 폐기 프로세스가 AWS 내에 마련되어 있습니다. AWS는 DoD 5220.22-M("국가 산업 보안 프로그램 운영 매뉴얼") 또는 NIST 800-88("미디어 삭제 가이드라인")에서 설명하는 기술을 사용해 폐기 프로세스에 따라 데이터를 제거합니다. 이 절차를 사용하여 하드웨어 디바이스를 폐기할 수 없는 경우 산업 표준 관행에 따라 디바이스의 저장을 제거하거나 디바이스를 물리적으로 파괴합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.

주요 영역	질문	AWS 답변
악의적인 공급업체 직원에 의한 무단 액세스로부터 데이터 보호	a. 데이터 암호화 키 관리. 내 데이터의 암호를 해독하는 데 사용되는 암호나 키를 공급업체에서 알고 있습니까? 또는 공급업체만 데이터를 암호화하도록 내 컴퓨터에서 데이터를 암호화 및 해독해야 합니까?	AWS 고객은 AWS 서버 측 암호화 서비스를 사용하는 경우를 제외하고 자체적으로 암호화를 관리합니다. 이 경우 AWS는 테넌트별로 고유한 암호화 키를 생성합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
	b. 공급업체 직원에 대한 조사. 공급업체에서 직원이 신뢰할 수 있는 사람인지 확인하기 위해 수행하는 개인 고용 확인 및 조사 프로세스는 무엇입니까?	AWS는 준거법에서 허용하는 범위 내에서 채용 전 적격 심사 관행의 일환으로 직원의 직위와 AWS 시설에 대한 접근 권한에 따라 범죄 경력 조회를 실시합니다.
	c. 공급업체 직원에 대한 감사. 공급업체 직원은 어떤 강력한 Identity and Access Management 시스템을 사용합니까? 공급업체 직원이 수행하는 작업을 기록하고 검토하는 데 사용되는 감사 프로세스는 무엇입니까?	ISO 27001 표준에 따라 AWS는 AWS 리소스에 대한 논리적 액세스에 대한 최소 표준을 규정하는 공식적인 정책 및 절차를 확립했습니다. AWS SOC 1 Type 2 보고서는 AWS 리소스에 대한 액세스 프로비저닝을 관리하기 위해 마련된 컨트롤을 개략적으로 설명합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
	d. 데이터 센터 방문자. 데이터 센터 방문자는 항상 안내자와 함께 하며, 모든 방문자의 이름 및 기타 개인 정보를 확인 및 기록합니까?	모든 방문자 및 계약자는 신분증을 제시해야 하며, 통과한 후에는 허가받은 직원의 지속적인 안내를 받습니다. AWS는 합법적인 업무 목적으로 이러한 권한이 필요한 계약업체와 직원에게만 데이터 센터 접근 권한 및 정보를 제공합니다. 직원에게 사업상 이러한 권한이 더 이상 필요 없게 되면, 접근 권한은 즉시 해지됩니다. 이는 해당 직원이 Amazon 또는 Amazon Web Services의 직원 신분을 유지해도 마찬가지입니다. AWS 직원의 데이터 센터에 대한 모든 물리적인 접근 기록되며 정기적으로 감사를 받습니다.

주요 영역	질문	AWS 답변
	e. 공급업체 직원에 의한 물리적 훼손. 공급업체 직원이 실수로 케이블을 다른 컴퓨터에 잘못 연결하는 일을 방지하고 공급업체 직원에 의한 고의적인 케이블 훼손 시도가 강조되도록 오스트레일리아 표준 또는 국제적으로 허용되는 표준에 따라 네트워크 케이블을 설치합니까?	물리적 보안 컨트롤에는 울타리, 벽, 보안 직원, 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단(단, 이에 제한되지 않음)과 같은 경계 컨트롤이 포함됩니다. 여기에는 네트워크 케이블에 대한 적절한 보호도 포함됩니다. AWS SOC 1 Type 2 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 9.1항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	f. 공급업체의 하청 업체. 이러한 질문에 대한 답변이 공급업체의 모든 하청 업체에도 똑같이 적용됩니까?	조달 계약업체/공급업체의 접근 권한은 직원과 계약업체에 대해 똑같이 관리되며, 책임은 HRT(인사관리부), 기업 경영 및 서비스 소유자가 분담합니다. 공급업체에 직원과 동일한 접근 요구 사항이 적용됩니다.
보안 사고 처리	a. 공급업체 적시 지원. 공급업체가 연락하기 쉽고 지원 요청에 신속히 대응하며 이런 대응이 SLA에 명시된 최대 허용 응답 시간 내에 이루어집니까? 아니면 단순히 공급업체에서 최선을 다하고 있음을 의미하는 마케팅 문구에 불과합니까? 지원이 로컬로 제공됩니까? 아니면 해외 또는 여러 해외 국가(태양의 이동 방향을 따라)에서 제공됩니까? 공급업체에서 지원을 제공할 수 있도록 사용자의 공급업체 서비스 사용에 대한 보안 태세를 실시간으로 파악하는 데 사용하는 메커니즘은 무엇입니까?	AWS Support는 경험이 풍부한 기술 지원 엔지니어가 365일 24시간 내내 대기하며 일대일로 신속한 지원을 제공하는 지원 창구입니다. 어떤 규모의 기업 고객이든 이 서비스를 통해 Amazon Web Services에서 제공하는 제품 및 기능을 성공적으로 활용할 수 있습니다. 모든 AWS Support 티어는 AWS Infrastructure Services 고객에게 장기 계약 없이 월 정액 요금제를 통해 건수 무제한 고객 지원을 제공합니다. 4가지 티어를 통해 개발자와 기업마다 특정한 요구를 충족하는 고객 지원 티어를 유연하게 선택할 수 있습니다.

주요 영역	질문	AWS 답변
	b. 공급업체의 사고 대응 계획. 공급업체에는 DSD ISM에 설명된 사고 처리 절차와 유사한 방식으로 보안 사고를 감지하고 이에 대응하는 방법을 명시한 보안 사고 대응 계획이 마련되어 있습니까? 고객이 이러한 계획의 복사본을 자세히 검토해 볼 수 있습니까?	Amazon 사고 관리 팀은 비즈니스에 영향을 미치는 이벤트 발생 시 해결책을 모색하기 위해 업계 표준의 진단 절차를 사용합니다. 관리 직원은 상시 사고를 감지하고 이들이 미치는 영향과 해결방안을 관리합니다. AWS의 인시던트 대응 프로그램, 계획 및 절차는 ISO 27001 표준에 따라 개발되었습니다. AWS SOC 1 Type 2 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. AWS 보안 프로세스 개요 백서(http://aws.amazon.com/security에서 제공)에도 자세한 내용이 나와 있습니다.
	c. 공급업체 직원에 대한 교육. 공급업체 시스템을 안전하게 사용하고 잠재적인 보안 사고를 식별하기 위해 공급업체 직원에게 필요한 자격, 인증 및 정규 정보 보안 인식 교육은 무엇입니까?	ISO 27001 표준에 따라 모든 AWS 직원들은 정기적으로 정보 보안 교육을 수료하고 수료증을 받아야 합니다. 준수성 감사는 직원들이 확립된 정책을 이해하고 따르는지 검증하기 위해 정기적으로 수행됩니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
	d. 보안 사고에 대한 알림. 공급업체는 합의된 임계값보다 더 심각한 보안 사고(특히 공급업체에 책임이 있는 경우)를 보안 통신을 통해 고객에게 알려 줍니까? 공급업체에서는 데이터를 저장하거나 처리하는 데 사용되는 컴퓨팅 장비를 압수할 수 있는 법 집행 기관이나 다른 기관에 자동으로 알립니까?	보안 사고 알림은 해당 법률에서 요구하는 대로 각 경우마다 그에 맞게 처리됩니다. 모든 알림은 보안 통신을 통해 이루어집니다.
	e. 공급업체 지원 범위. 데이터의 무단 공개와 같은 보안 위반이 있는 경우 또는 법적 전자 증거 수색을 수행해야 하는 경우 수사와 관련하여 공급업체에서는 고객을 얼마나 지원합니까?	AWS는 인프라를 제공하고, 고객은 운영 체제, 네트워크 구성, 설치된 애플리케이션을 포함한 그 밖의 모든 구성 요소를 관리합니다. 고객은 AWS를 사용해 보관하거나 처리하는 전자 문서의 식별, 수집, 처리, 분석 및 작성을 포함하는 소송 절차에 적절하게 대응할 책임이 있습니다. 요청 시 AWS는 소송 절차에서 AWS의 지원이 필요한 고객과 협력할 수 있습니다.

주요 영역	질문	AWS 답변
	f. 로그에 대한 액세스 권한. 법의학 수사를 수행하기 위해 시간 동기화된 감사 로그와 다른 로그에 액세스하려면 어떻게 해야 합니까? 그리고 로그를 적절한 법원 제출용 증거물로 어떻게 생성하고 저장합니까?	고객은 게스트 운영 체제, 소프트웨어 및 애플리케이션에 대한 관리 및 소유권을 보유하고 있으므로 이러한 시스템의 상태에 대한 논리적 모니터링을 개발해야 할 책임은 고객에게 있습니다. ISO 27001 표준에 따라 AWS 정보 시스템은 NTP(Network Time Protocol)를 통해 동기화되는 내부 시스템 클록을 사용합니다. AWS CloudTrail은 사용자 활동을 기록하는 간단한 솔루션을 제공하여 복잡한 로깅 시스템을 실행해야 하는 부담을 줄여 줍니다. 자세한 내용은 aws.amazon.com/cloudtrail을 참조하십시오. AWS Cloudwatch는 고객이 AWS에서 실행하는 AWS 클라우드 리소스와 애플리케이션을 모니터링합니다. 자세한 내용은 aws.amazon.com/cloudwatch를 참조하십시오. AWS는 서비스 상태 대시보드에 서비스 가용성에 대한 최신 정보도 게시합니다. status.aws.amazon.com을 참조하십시오.
	g. 보안 사고 보상. 공급업체의 조치, 결함 있는 소프트웨어 또는 하드웨어로 인해 보안 위반이 발생하는 경우 공급업체는 고객에게 어떻게 적절히 보상하겠습니까?	AWS의 인시던트 대응 프로그램, 계획 및 절차는 ISO 27001 표준에 따라 개발되었습니다. AWS SOC 1 Type 2 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. AWS 보안 프로세스 개요 백서(http://aws.amazon.com/security에서 제공)에도 자세한 내용이 나와 있습니다.
	h. 데이터 유출. 너무 중요하여 클라우드에 저장할 수 없다고 생각하는 데이터를 실수로 클라우드에 저장한 경우(즉, 데이터 유출) 법의학적 폐기 기술을 사용하여 유출된 데이터를 어떻게 삭제할 수 있습니까? 데이터를 삭제할 때마다 물리적 스토리지 미디어의 관련 부분이 0으로 초기화됩니까? 아니면 클라우드에 일반적으로 사용되지 않은 많은 예비 스토리지 용량이 있으므로 고객이 일반적인 작업의 일부로서 삭제된 데이터를 덮어쓸 때까지 얼마나 걸립니까? 유출된 데이터를 공급업체의 백업 미디어에서 법의학적으로 삭제할 수 있습니까? 유출된 데이터는 어디에 저장되며 법의학적으로 삭제할 수 있습니까?	고객은 콘텐츠에 대한 소유권 및 관리 권한을 보유합니다. 고객을 대신해 AWS에 저장된 모든 데이터는 강력한 테넌트 격리 보안 및 제어 기능을 갖고 있습니다. AWS는 고객이 S3, EBS 및 EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있도록 지원합니다. VPC에 대한 IPSec 터널도 암호화됩니다. Amazon S3도 고객을 위한 옵션으로 Server Side Encryption을 제공합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 위험 및 규정 준수 백서를 참조하십시오. 자세한 내용은 http://aws.amazon.com/security에서 AWS 위험 및 규정 준수 백서를 참조하십시오.

부록 D: 용어 정의

DSS: 신용카드 산업 DSS(데이터 보안 표준)는 신용카드 산업의 보안 표준 위원회에서 규정하고 관리하는 전 세계적 정보 보안 표준입니다.

EBS: Amazon Elastic Block Store(EBS)는 Amazon EC2 인스턴스와 함께 사용할 블록 수준의 스토리지 볼륨을 제공합니다. Amazon EBS 볼륨은 인스턴스 수명과 관계없이 지속되는 오프 인스턴스 스토리지입니다.

FedRAMPsm: 연방정부의 위험 및 인증 관리 프로그램(FedRAMPsm)은 클라우드 제품 및 서비스의 보안 평가, 권한 부여 및 지속적 모니터링을 위한 표준 방식을 지시하는 범정부 프로그램입니다. FedRAMPsm는 위험 수준이 보통에서 낮은 정도의 연방 기관 클라우드 배포 및 서비스 모델에 대한 의무 규정입니다.

FIPS 140-2: FIPS(Federal Information Processing Standard) Publication 140-2는 미국 정부 보안 표준으로서, 기밀 정보를 보호하는 암호 모듈의 보안 요건을 규정하고 있습니다.

FISMA: 2002년 미연방 정보 보안 관리법입니다. 이 법은 다른 기관, 협력업체 또는 다른 출처에서 제공하거나 관리하는 정보 및 시스템을 포함하여, 연방 기관의 자산과 업무를 뒷받침하는 정보 시스템 및 정보에 대해 기관 전체의 정보 보안 프로그램을 개발, 기록 및 구현할 것을 각 기관에 요구하고 있습니다.

GLBA: GLB 또는 GLBA(Gramm-Leach-Bliley 법), 즉 1999년 금융 서비스 현대화법은 특히 비공개 고객 정보의 노출 및 보안/데이터 무결성의 위협 차단과 관련된 금융 기관의 요구 사항을 명시하고 있습니다.

HIPAA: 1996년 HIPAA(건강 보험 이전 및 책임법)에서는 의료 제공자, 건강 보험 상품, 기업에 대한 전국적인 식별 정보 및 전자 의료 트랜잭션에 대한 국가 표준을 수립할 것을 요구합니다. 행정 단순화 조항도 건강 기록의 보안 및 개인 정보 보호를 규정하고 있습니다. 이러한 표준은 미국 건강 관리 시스템의 전자 문서 교환을 널리 사용하도록 권장하여 국가의 건강 관리 시스템의 효율성과 효과를 개선하려는 의도로 제정되었습니다.

IAM: AWS Identity and Access Management(IAM)는 AWS 고객이 자신의 AWS 계정 내에서 사용자 및 사용자 권한을 관리할 수 있도록 하는 웹 서비스입니다.

ISAE 3402: ISAE 3402(International Standards for Assurance Engagements No. 3402)는 보험 가입에 관한 국제 표준입니다. 이 표준은 국제 회계사 연맹(IFAC) 내의 표준 제정 기구인 국제 감사 인증 기준 위원회(IAASB)에서 제정했습니다. ISAE 3402는 현재 서비스 조직을 위한 세계적인 보증 보고 표준입니다.

ISO 27001: ISO/IEC 27001은 ISO(국제 표준화 기구) 및 IEC(국제 전자기술 위원회)에서 발행하는 ISMS(정보 보안 관리 시스템) 표준입니다. ISO 27001은 명시적인 관리 제어 하에서 정보 보안을 제공하도록 고안된 관리 시스템을 공식적으로 지정합니다. 공식 지정이란 특정 요건을 지시할 수 있음을 의미합니다. 따라서 ISO/IEC 27001을 채택한 조직은 이 표준에 따라 감사와 인증을 받을 수 있습니다.

ISO 9001: 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.

ITAR: ITAR(국제 무기 거래 규정)은 USML(미국 군수물자 목록)에 등재된 방위 관련 물품 및 서비스의 수출입을 통제하기 위한 미국 정부의 규정 모음입니다. 정부 기관과 계약업체는 ITAR을 준수하고 보호된 데이터에 대한 액세스를 제한해야 합니다.

NIST: 미국 국립 표준 기술 연구소입니다. 이 기관은 산업 또는 정부 프로그램에서 요구하는 세부적인 보안 표준을 설정합니다. FISMA를 준수하려는 기관은 NIST 표준을 따라야 합니다.

PCI: 신용카드 산업 보안 표준 위원회를 참조하십시오. 이 위원회는 American Express, Discover Financial Services, JCB, MasterCard Worldwide 및 Visa International이 신용카드 산업 데이터 보안 표준의 지속적인 발전을 관리할 목적으로 구성한 독립 기구입니다.

QSA: PCI(신용카드 산업) QSA(정식 보안 평가자) 자격은 PCI 보안 표준 위원회에서 특정한 자격 요건을 충족하여 PCI 준수 평가를 실시할 권한이 부여된 개인에게 수여하는 자격입니다.

SAS 70: 감사 표준 선언 제70호: 미국 공인회계사 협회(AICPA) 감사 표준 위원회에서 발행하는 서비스 조직 관련 감사 규정입니다. SAS 70은 서비스 감사자에게 서비스 조직(AWS 등)의 내부 컨트롤 평가 및 서비스 감사자 보고서 발행 절차를 안내합니다. SAS 70은 또한 하나 이상의 서비스 조직을 이용하는 엔터티의 재무 제표 감사 절차를 안내합니다. SAS 70 보고서는 Service Organization Controls 1 보고서로 대체되었습니다.

SOC 1: SOC 1(Service Organization Controls 1) Type II 보고서(구 SAS(Statement on Auditing Standards) 제70호), 서비스 조직 보고서(구 SSAE 16 보고서)는 미국 공인회계사 협회(AICPA)가 개발한 감사 표준으로

SOC 2: SOC 2(Service Organization Controls 2) 보고서는 보안, 가용성, 처리 무결성, 기밀성 및 개인 정보 보호에 관한 서비스 조직 내부의 통제 방식을 광범위한 사용자가 이해할 수 있도록 하기 위해 만들어졌습니다. 이러한 보고서는 "AICPA 가이드: 서비스 조직의 보안, 가용성, 처리 무결성, 기밀성 또는 개인 정보 보호 관련 컨트롤 보고"를 사용하여 수행되며 서비스 조직과 내부 컨트롤을 완벽하게 이해해야 하는 서비스 조직의 이해관계자(예: 고객, 규제 담당자, 비즈니스 파트너, 공급업체, 책임자)가 사용할 수 있도록 고안되었습니다.

SOC 3: SOC 3(Service Organization Controls 3) 보고서는 보안, 가용성, 처리 무결성, 기밀성 및 개인 정보 보호에 관한 서비스 조직의 통제 방식을 보장받고자 하나 SOC 2 보고서를 실무에 이용할 만한 지식 또는 그러한 필요성이 없는 사용자를 위해 고안된 것입니다. 이러한 보고서는 가용성, 처리 무결성, 기밀성, 개인 정보 보호에 대한 AICPA/캐나다 공인 회계사 협회(CICA) 트러스트 서비스 원칙, 기준 및 예를 사용해 작성됩니다. 범용 보고서이므로 SOC 3 보고서는 직인 표시가 있는 한 자유롭게 배포하거나 웹 사이트에 게시할 수 있습니다.

SSAE 16 [deprecated]: SSAE 16(Statement on Standards for Attestation Engagements No. 16)은 미국 공인회계사 협회(AICPA) 감사 표준 위원회(ASB)에서 발행하는 인증 표준입니다. 서비스 조직의 컨트롤은 사용자 엔터티 재무 보고에 관한 내부 통제(ICFR)와 관련성이 높으므로 이 표준은 사용자 엔터티에 서비스를 제공하는 조직의 컨트롤을 보고하기 위해 서비스 감사자가 수행하는 감사를 규정합니다. 2011년 6월 15일 마감하는 서비스 감사 기관의 보고 기간에 대해서는 SSAE 16이 SAS 70(Statement on Auditing Standards No. 70)을 실질적으로 대체합니다.

Virtual Instance: AMI를 실행하고 나면, 결과 실행 시스템이 인스턴스로 참조됩니다. 같은 AMI를 갖는 모든 인스턴스는 동일하게 시작되며, 인스턴스가 종료되거나 장애가 발생하는 경우 인스턴스의 모든 정보는 손실됩니다.

가용 영역: Amazon EC2 지점은 리전과 가용 영역으로 구성됩니다. 가용 영역은 다른 가용 영역에 장애가 발생할 경우 분리되도록 설계된 개별적인 지점으로, 동일 리전 내의 다른 가용 영역에 비해 저렴하고 지연 시간이 짧은 네트워크 연결을 제공합니다.

객체: Amazon S3에 저장되는 기본 요소입니다. 객체는 객체 데이터와 메타데이터로 구성됩니다. 이 데이터 부분은 Amazon S3에서 볼 수 없습니다. 메타데이터는 객체를 설명하는 이름-값 페어의 집합입니다. 여기에는 마지막으로 수정한 날짜와 같은 몇 가지 기본 메타데이터 및 콘텐츠 형식과 같은 표준 HTTP 메타데이터가 포함됩니다. 개발자는 또한 객체를 저장할 때 사용자 정의 메타데이터를 지정할 수도 있습니다.
널리 통용되고 있습니다. 국제 표준은 ISAE 3402(International Standards for Assurance Engagements No. 3402)라고 합니다.

서비스 수준 계약(SLA): 서비스 수준 계약은 서비스 계약에서 서비스의 수준을 공식적으로 정의하는 부분입니다. SLA는 계약한 (서비스) 납품 시간 또는 성과를 명시하는 데 사용됩니다.

서비스: 네트워크 전체에 걸쳐 제공되는 소프트웨어 또는 컴퓨팅 기능(예: EC2, S3, VPC 등)입니다.
인증: 인증은 누군가 또는 무언가를 어떤 사람 또는 어떤 사물로 선언할 것인지를 정하는 프로세스입니다.
하이퍼바이저: VMM(Virtual Machine Manager)이라고도 하며, 호스트 컴퓨터에서 여러 운영 체제를 동시에 실행할 수 있는 소프트웨어/하드웨어 플랫폼 가상화 소프트웨어입니다.

버전 기록

2015년 8월
- PCI 3.1에 대한 범위 내 서비스 업데이트
- PCI 3.1에 대한 범위 내 리전 업데이트

2015년 5월
- 열 번째 리전 추가(EU 프랑크푸르트)
- SOC 3에 대한 범위 내 서비스 업데이트
- SSAE 16 언어 사용되지 않음

2015년 4월
- 범위 내 서비스 업데이트: FedRAMPsm, HIPAA, SOC 1, ISO 27001, ISO 9001

2015년 2월
- FIPS 140-2 VPN 엔드포인트 및 SSL 종료 로드 밸런서에 대한 업데이트
- PCI DSS verbiage 업데이트

2014년 12월
- 인증 및 제3자 증명 요약 업데이트

2013년 11월 버전
- IPsec 터널 암호화 verbiage 수정

2013년 6월 버전
- 인증 및 제3자 증명 요약 업데이트
- 부록 C: 용어집 업데이트
- 사소한 서식 변경

2013년 1월 버전
- 인증 및 제3자 증명 요약 수정
- MPAA 콘텐츠 보안 모델에 부합하는 AWS(부록 B) 추가

2012년 11월 버전
- 콘텐츠 및 업데이트된 인증서 범위 수정
- SOC 2 및 MPAA에 대한 참조 추가

2012년 7월 버전
- 콘텐츠 및 업데이트된 인증서 범위 수정
- CSA 평가 질문서(부록 A) 추가

2012년 1월 버전
- 업데이트된 인증 범위에 기반한 사소한 콘텐츠 수정
- 사소한 문법 수정

2011년 12월 버전
- SOC 1/SSAE 16, FISMA Moderate, International Traffic in Arms Regulations, FIPS 140-2를 반영하기 위한 인증 및 제3자 증명 변경
- S3 서버 측 암호화 추가
- 추가 클라우드 컴퓨팅 사안 추가

2011년 5월 버전
- 최초 릴리스

고지 사항