CSA 공동 평가 질문서

2017년 1월

고지 사항

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

목차

요약

CSA 평가 질문서에는 CSA에서 클라우드 소비자 및/또는 클라우드 감사자가 클라우드 공급자에게 문의할 것이라고 예상되는 질문 세트가 나와 있습니다. 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.

서론

CSA(Cloud Security Alliance)는 “클라우드 컴퓨팅 내에서 보안 보증을 제공하는 모범 사례 사용을 촉진하고 기타 모든 형태의 컴퓨팅을 보호할 수 있도록 클라우드 컴퓨팅 사용에 대한 교육을 제공하는 비영리 단체입니다.” 자세한 내용은 https://cloudsecurityalliance.org/about/을 참조하십시오.

광범위한 산업 보안 실무자, 기업 및 협회가 이 조직에 참여해 임무를 수행하고 있습니다.

CSA 공동 평가 질문서

제어 그룹	CID	평가 질문	AWS 답변
애플리케이션 및 인터페이스 보안 *애플리케이션 보안*	AIS-01.1	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. AWS는 새로운 리소스 개발을 관리하는 절차를 마련했습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 14항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	AIS-01.2	프로덕션 전에 자동 소스 코드 분석 도구를 사용해 코드에서 보안 결함을 탐지합니까?	
	AIS-01.3	프로덕션 전에 수동 소스 코드 분석을 통해 코드에서 보안 결함을 탐지합니까?	
	AIS-01.4	모든 소프트웨어 공급업체가 시스템/소프트웨어 개발 수명 주기(SDLC) 보안에 대한 산업 표준을 준수하는지 확인합니까?	
	AIS-01.5	(SaaS만 해당) 프로덕션으로 배포하기 전에 애플리케이션에서 보안 취약성을 검토하고 문제를 모두 해결합니까?	

제어 그룹	CID	평가 질문	AWS 답변
애플리케이션 및 인터페이스 보안 *고객 액세스 요건*	AIS-02.1	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 관련 법규를 준수하여 AWS를 사용할 책임이 있습니다. AWS는 산업 인증, 제3자 증명, 백서(http://aws.amazon.com/compliance에서 제공)를 통해 고객에게 보안 및 제어 환경을 전달하고, AWS 고객에게 직접 인증, 보고서 및 기타 관련 문서를 제공합니다.
	AIS- 02.2	고객 액세스에 대한 모든 요건 및 신뢰 수준이 정의되고 문서화되어 있습니까?	
애플리케이션 및 인터페이스 보안 *데이터 무결성*	AIS-03.1	수동 또는 시스템 처리 오류 또는 데이터 손상을 방지하기 위해 애플리케이션 인터페이스와 데이터베이스에 데이터 입력 및 출력 무결성 루틴(조정 및 수정 검사)이 구현되어 있습니까?	AWS SOC 보고서에 설명된 것처럼 AWS 데이터 무결성 컨트롤은 전송, 저장 및 처리를 포함한 모든 단계에서 유지되는 데이터 무결성 컨트롤을 설명합니다. ISO 27001 표준, 부록 A, 14항에서도 자세한 내용을 확인하실 수 있습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
애플리케이션 및 인터페이스 보안 *데이터 보안/무결성*	AIS-04.1	산업 표준(예: CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)을 사용해 데이터 보안 아키텍처를 설계했습니까?	AWS 데이터 보안 아키텍처는 주요 산업 표준을 통합하도록 설계되었습니다. AWS가 준수하는 다양한 주요 산업 표준에 대한 자세한 내용은 http://aws.amazon.com/compliance에서 AWS 인증, 보고서 및 백서를 참조하십시오.
감사 보장 및 규정 준수 *감사 계획*	AAC-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 제3자 증명을 획득하고, AWS 고객에게 특정 인증, 보고서 및 기타 관련 문서를 직접 제공합니다.
감사 보장 및 규정 준수 *독립 감사*	AAC-02.1	테넌트가 SOC2/ISO 27001 또는 이와 유사한 제3자 감사 또는 인증 보고서를 볼 수 있도록 허용합니까?	AWS는 NDA에 의거하여 제3자 증명, 인증, Service Organization Controls(SOC) 보고서 및 기타 관련 규정 준수 보고서를 고객에게 직접 제공합니다. AWS ISO 27001 인증은 여기에서 다운로드할 수 있습니다.

제어 그룹	CID	평가 질문	AWS 답변
	AAC-02.2	산업 모범 사례 및 지침에 규정된 대로 정기적으로 클라우드 서비스 인프라에 대해 네트워크 침투 테스트를 수행합니까?	AWS SOC 3 보고서를 여기에서 다운로드할 수 있습니다. 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 감사와 위험 평가를 거칩니다. AWS는 외부 인증 기관 및 독립 감사 기관과 협력하여 AWS 전체 제어 환경을 검토하고 테스트합니다.
	AAC-02.3	산업 모범 사례 및 지침에 규정된 대로 정기적으로 클라우드 인프라에 대해 애플리케이션 침투 테스트를 수행합니까?	
	AAC-02.4	산업 모범 사례 및 지침에 규정된 대로 정기적으로 내부 감사를 실시합니까?	
	AAC-02.5	산업 모범 사례 및 지침에 규정된 대로 정기적으로 외부 감사를 실시합니까?	
	AAC-02.6	테넌트가 요청할 경우 침투 테스트 결과를 제공합니까?	
	AAC-02.7	테넌트가 요청할 경우 내부 및 외부 감사 결과를 제공합니까?	
	AAC-02.8	복수의 부서에서 평가를 감사할 수 있는 내부 감사 프로그램이 있습니까?	
감사 보장 및 규정 준수 *정보 시스템 규제 매핑*	AAC-03.1	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

제어 그룹	CID	평가 질문	AWS 답변
	AAC-03.2	장애 발생 또는 데이터 손실 시 특정 고객의 데이터를 복구할 수 있습니까?	지원합니다. VPC에 대한 IPSec 터널도 암호화됩니다. 또한 고객은 AWS Key Management Systems(KMS)를 이용하여 암호화 키를 생성 및 제어할 수 있습니다(https://aws.amazon.com/kms/ 참조). 자세한 내용은 http://aws.amazon.com/security 에서 AWS 클라우드 보안 백서를 참조하십시오. AWS는 고객이 자체 데이프 백업 서비스 공급자를 사용해 데이프에 백업할 수 있도록 허용합니다. 그러나 AWS에서는 데이프 백업 서비스를 제공하지 않습니다. Amazon S3 및 Glacier 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.
	AAC-03.3	고객 데이터의 저장을 특정 국가 또는 지리적 위치로 제한할 수 있습니까?	AWS 고객은 콘텐츠가 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. 사용할 수 있는 리전의 전체 목록을 확인하려면 AWS Global Infrastructure 페이지를 방문하십시오.
	AAC-03.4	해당 관할 지역의 규제 요건 변화를 모니터링하고, 법률 요건 변화에 따라 보안 프로그램을 조정하고, 관련 규제 요건의 준수를 보장하는 기능을 포함하는 프로그램이 마련되어 있습니까?	AWS는 관련 법률 및 규제 요건을 모니터링합니다. 자세한 내용은 ISO 27001 표준 부록 18을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
비즈니스 연속성 관리 및 운영 복원성 *비즈니스 연속성 계획*	BCR-01.1	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 클라우드 보안 개요 백서를 참조하십시오.
	BCR-01.2	테넌트에게 다른 공급자에 대한 인프라 서비스 failover 기능을 제공합니까?	

제어 그룹	CID	평가 질문	AWS 답변
비즈니스 연속성 관리 및 운영 복원성 *비즈니스 연속성 테스트*	BCR-02.1	지속적인 효과를 보장하기 위해 정기적으로 또는 중요 조직 또는 환경이 변경될 경우 비즈니스 연속성 계획을 테스트합니까?	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, 17항을 참조하십시오.
비즈니스 연속성 관리 및 운영 복원성 *전력/전화통신*	BCR-03.1	데넌트에게 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 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.
	BCR-03.2	데넌트가 데이터 전송 방식과 데이터가 통과하는 법정 관할 지역을 정의할 수 있습니까?	
비즈니스 연속성 관리 및 운영 복원성 설명서	BCR-04.1	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/security/에서 AWS 클라우드 보안 백서를 참조하십시오. ISO 27001 부록 A 12항을 참조하십시오.
비즈니스 연속성 관리 및 운영 복원성 *환경 위험*	BCR-05.1	자연적 원인, 자연 재해, 의도적 공격 등으로 인한 손상을 예상하여 이로부터 보호하는 물리적인 조치를 고안하고 대책을 적용했습니까?	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. ISO 27001 표준, 부록 A, 11항을 참조하십시오.
비즈니스 연속성 관리 및 운영 복원성 *장비 위치*	BCR-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. 환경 위험에 대한 AWS의 물리적 보호 조치는 독립적인 감사 기관으로부터 검증을 받았으며 ISO 27002 모범 사례를 준수함을 인증받았습니다. ISO 27001 표준, 부록 A, 11항을 참조하십시오.
비즈니스 연속성 관리 및 운영 복원성 *장비 관리*	BCR-07.1	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 수 있습니다(소프트웨어 라이선스 제한이 적용됨). 자세한 내용은

제어 그룹	CID	평가 질문	AWS 답변
	BCR-07.2	가상 인프라를 사용할 경우 테넌트에게 가상 머신을 제 때에 이전 상태로 복원할 수 있는 기능을 제공합니까?	http://aws.amazon.com/security에서 AWS 클라우드 보안 백서를 참조하십시오.
	BCR-07.3	가상 인프라를 사용할 경우 가상 머신 이미지를 다운로드하여 새 클라우드 공급자에 이식할 수 있습니까?	
	BCR-07.4	가상 인프라를 사용할 경우 고객이 그러한 이미지를 자체 오프사이트 스토리지 위치에 복제할 수 있도록 머신 이미지를 제공합니까?	
	BCR-07.5	클라우드 솔루션에 소프트웨어/공급자 독립적인 복원 및 복구 기능이 포함되어 있습니까?	
비즈니스 연속성 관리 및 운영 복원성 *장비 정전*	BCR-08.1	유틸리티 서비스 중단(예: 정전, 네트워크 장애 등)으로부터 장비를 보호할 수 있는 보안 메커니즘과 중복성이 구현되어 있습니까?	AWS 장비는 ISO 27001 표준에 따라 유틸리티 서비스 중단으로부터 보호됩니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. AWS SOC 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 클라우드 보안 백서도 참조하십시오.
비즈니스 연속성 관리 및 운영 복원성 *영향 분석*	BCR-09.1	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/cloudwatch 를 참조하십시오. AWS는 서비스 상태 대시보드에 서비스 가용성에 대한 최신 정보도 게시합니다. status.aws.amazon.com을 참조하십시오.
	BCR-09.2	테넌트들에게 표준 기반의 정보 보안 측정치(CSA, CAMM 등)를 제공하고 있습니까?	
	BCR-09.3	고객이 SLA 성능을 지속적으로 파악하고 보고받을 수 있도록 지원합니까?	

제어 그룹	CID	평가 질문	AWS 답변
비즈니스 연속성 관리 및 운영 복원성 *정책*	BCR-10.1	서비스 운영 역할을 적절하게 지원할 수 있도록 정책과 절차가 확립되어 있고 모두에게 제공됩니까?	NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 표준 및 PCI DSS 요건을 기반으로 AWS 보안 프레임워크를 통해 정책 및 절차가 확립되었습니다. 자세한 내용은 http://aws.amazon.com/compliance에서 AWS 위험 및 규정 준수 백서를 참조하십시오.
비즈니스 연속성 관리 및 운영 복원성 *보존 정책*	BCR-11.1	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 데이터 보존을 관리할 책임은 고객에게 있습니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 클라우드 보안 백서를 참조하십시오. 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. 자세한 내용은 https://aws.amazon.com/compliance/data-privacy-faq/를 참조하십시오.
	BCR-11.2	정부 또는 제3자의 테넌트 데이터 요청에 대응할 수 있는 문서화된 절차가 있습니까?	
	BCR-11.4	규제, 법규, 계약 또는 비즈니스 요건을 준수할 수 있도록 백업 또는 중복성 메커니즘을 구현했습니까?	AWS 백업 및 중복성 메커니즘은 ISO 27001 표준에 따라 개발 및 테스트되었습니다. AWS 백업 및 중복성 메커니즘에 대한 자세한 내용은 ISO 27001 표준, 부록 A, 12항과 AWS SOC 2 보고서를 참조하십시오.
	BCR-11.5	백업 또는 중복성 메커니즘을 최소한 1년에 한 번 이상 테스트합니까?	
변경 제어 및 구성 관리. *새로운 개발/인수*	CCC-01.1	새로운 애플리케이션, 시스템, 데이터베이스, 인프라, 서비스, 운영 및 시설 개발 또는 인수를 위한 관리 권한 부여에 대한 정책과 절차가 확립되어 있습니까?	NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 표준 및 PCI DSS 요건을 기반으로 AWS 보안 프레임워크를 통해 정책 및 절차가 확립되었습니다. AWS를 처음 사용하는 고객이든 고급 사용자든 상관없이 AWS 웹 사이트 https://aws.amazon.com/documentation/의 AWS 설명서 단원에서 소개에서부터 고급 기능에 이르기까지 서비스에 대한 유용한 정보를 얻을 수 있습니다.
	CCC-01.2	제품/서비스/기능의 설치, 구성 및 사용에 대해 설명하는 설명서가 제공됩니까?	

제어 그룹	CID	평가 질문	AWS 답변
변경 제어 및 구성 관리. *아웃소싱 개발*	CCC-02.1	모든 소프트웨어 개발 시 품질 표준을 충족할 수 있도록 보장하는 제어가 마련되어 있습니까?	AWS는 일반적으로 소프트웨어 개발을 아웃소싱하지 않습니다. AWS는 시스템 개발 수명 주기(SDLC) 프로세스의 일환으로 품질 표준을 통합합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 14항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	CCC-02.2	아웃소싱 소프트웨어 개발 활동에서 소스 코드 보안 결함을 탐지할 수 있는 제어가 마련되어 있습니까?	
변경 제어 및 구성 *관리* *품질 테스트*	CCC-03.1	테넌트에게 품질 보증 프로세스를 설명하는 문서를 제공합니까?	AWS는 ISO 9001 인증을 유지합니다. 이 인증은 AWS 품질 시스템에 대한 독립적인 검증으로, AWS 활동이 ISO 9001 요건을 준수함을 확인했습니다. AWS 보안 게시판이 보안 및 개인 정보 보호 이벤트를 고객에게 알립니다. 고객은 AWS 웹 사이트에서 AWS 보안 게시판 RSS 피드를 구독할 수 있습니다. aws.amazon.com/security/security-bulletins/를 참조하십시오. AWS는 서비스 상태 대시보드에 서비스 가용성에 대한 최신 정보도 게시합니다. status.aws.amazon.com을 참조하십시오. AWS 시스템 개발 수명 주기(SDLC)는 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, 14항에서도 자세한 내용을 확인하실 수 있습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	CCC-03.2	특정 제품/서비스에서 알려진 문제를 설명하는 문서가 제공됩니까?	
	CCC-03.3	제품 및 서비스에 대해 보고된 버그 또는 보안 취약성을 분류하고 해결하기 위한 정책 및 절차가 마련되어 있습니까?	
	CCC-03.4	릴리즈된 소프트웨어 버전에서 모든 디버깅 및 테스트 코드 요소를 제거하도록 하는 메커니즘이 마련되어 있습니까?	
변경 제어 및 구성 관리. *권한 없는 소프트웨어 설치*	CCC-04.1	권한 없는 소프트웨어가 시스템에 설치되는 것을 제한하고 모니터링하는 제어가 마련되어 있습니까?	악성 소프트웨어를 관리하는 AWS의 프로그램, 프로세스 및 절차는 ISO 27001 표준을 준수합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 12항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
변경 제어 및 구성 관리. *프로덕션 변경*	CCC-05.1	테넌트에게 프로덕션 변경 관리 절차와 이에 대한 테넌트의 역할/권한/책임을 설명하는 문서를 제공합니까?	AWS SOC 보고서는 AWS 환경에서 변경 관리를 관리하기 위해 마련된 제어를 개괄적으로 설명합니다. ISO 27001 표준, 부록 A, 12항에서도 자세한 내용을 확인하실 수 있습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.

제어 그룹	CID	평가 질문	AWS 답변
데이터 보안 및 정보 수명 주기 관리 *분류*	DSI-01.1	정책 태그/메타데이터를 통해 가상 머신을 식별할 수 있는 기능을 제공합니까(예를 들어 태그는 잘못된 국가에서 게스트 운영 체제의 부팅/설치/데이터 전송을 제한하는 데 사용될 수 있음)?	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.
	DSI-01.2	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.
	DSI-01.3	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.
	DSI-01.4	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(오레곤), 미국 서부(캘리포니아 북부), AWS GovCloud(미국, 오레곤), EU(아일랜드), EU(프랑크푸르트), 아시아 태평양(서울), , 아시아 태평양(싱가포르), 아시아 태평양(도쿄), 아시아 태평양(시드니), 중국(베이징) 리전, 남아메리카(상파울루) 등 12개 리전이 있습니다.
	DSI-01.5	테넌트의 데이터가 보관된 스토리지의 물리적 위치/지역을 미리 제공할 수 있습니까?	
	DSI-01.6	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.

제어 그룹	CID	평가 질문	AWS 답변
	DSI-01.7	데넌트가 데이터 라우팅 및 리소스 인스턴스화를 위해 허용 가능한 지리적 위치를 정의할 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(오레곤), 미국 서부(캘리포니아 북부), AWS GovCloud(미국, 오레곤), EU(아일랜드), EU(프랑크푸르트), 아시아 태평양(서울), 아시아 태평양(싱가포르), 아시아 태평양(도쿄), 아시아 태평양(시드니), 중국(베이징) 리전, 남아메리카(상파울루) 등 12개 리전이 있습니다.
데이터 보안 및 정보 수명 주기 관리 *데이터 인벤토리/흐름*	DSI-02.1	서비스의 애플리케이션과 인프라 네트워크 및 시스템 내부에 상주(영구적 또는 일시적)하는 데이터에 대해 데이터 흐름을 인벤토리, 문서화, 유지합니까?	AWS 고객은 콘텐츠가 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(오레곤), 미국 서부(캘리포니아 북부), AWS GovCloud(미국, 오레곤), EU(아일랜드), EU(프랑크푸르트), 아시아 태평양(서울), 아시아 태평양(싱가포르), 아시아 태평양(도쿄), 아시아 태평양(시드니), 중국(베이징) 리전, 남아메리카(상파울루) 등 12개 리전이 있습니다.
	DSI-02.2	데이터가 정의된 지리적 위치를 벗어나 마이그레이션되지 않도록 할 수 있습니까?	
데이터 보안 및 정보 수명 주기 관리 *전자상거래*	DSI-03.1	퍼블릭 네트워크(예: 인터넷)를 통해 이동하는 데 필요한 경우, 데넌트 데이터를 보호하기 위해 개방형 암호화 방법(3.4ES, AES 등)을 제공합니까?	모든 AWS API는 SSH로 보호되는 엔드포인트를 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. 또한 고객은 AWS Key Management Systems(KMS)를 이용하여 암호화 키를 생성 및 제어할 수 있습니다(https://aws.amazon.com/kms/ 참조). 고객은 제3자 암호화 기술을 사용할 수도 있습니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 클라우드 보안 백서를 참조하십시오.
	DSI-03.2	인프라 구성 요소가 퍼블릭 네트워크를 통해 서로 통신해야 하는 경우(예: 한 환경에서 다른 환경으로 인터넷 기반 데이터 복제) 항상 개방형 암호화 방법을 사용합니까?	
데이터 보안 및 정보 수명 주기 관리 *취급/레이블*	DSI-04.1	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.

제어 그룹	CID	평가 질문	AWS 답변
지정/보안 정책	DSI-04.2	데이터 통합 컨테이너 역할을 하는 객체에 대한 레이블 상속 메커니즘이 구현되어 있습니까?	
데이터 보안 및 정보 수명 주기 관리 *비 프로덕션 데이터*	DSI-05.1	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 보안 및 정보 수명 주기 관리 *소유권/관리 의무*	DSI-06.1	데이터 관리 의무에 관한 책임이 정의, 할당, 문서화 및 전달됩니까?	AWS 고객은 데이터에 대한 관리 및 소유권을 보유합니다. 자세한 내용은 AWS 고객 계약서를 참조하십시오.
데이터 보안 및 정보 수명 주기 관리 *안전한 폐기*	DSI-07.1	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 관행에 따라 디바이스의 저장을 제거하거나 디바이스를 물리적으로 파괴합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 클라우드 보안 백서를 참조하십시오. Amazon EBS 볼륨은 제공되기 전에 초기화한 포맷되지 않은 원시 블록 디바이스의 형태로 고객에게 제공됩니다. 재사용 직전에 초기화가 진행되므로 삭제 프로세스가 완료된 것으로 안심해도 됩니다. DoD 5220.22-M("National Industrial Security Program Operating Manual") 또는 NIST 800-88("Guidelines for Media Sanitization")에서 자세히 설명한 대로 특정 방법을 통해 모든 데이터를 초기화해야 하는 절차를 따르는 경우 Amazon EBS에서 이와 같이 할 수 있습니다. 정해진 요구 사항을 준수하기 위해 볼륨을 삭제하기 전에 특수화된 초기화 절차를 진행해야 합니다. 중요한 데이터의 암호화는 보편적으로 유용한 보안 사례이며, AWS는 AES-256을 사용하여 EBS 볼륨과 해당 스냅샷을 암호화할 수 있는 기능을 제공합니다. EC2 인스턴스를 호스트하는 서버에서 암호화가 이루어지기 때문에 EC2 인스턴스와 EBS 스토리지 간 이동하는 데이터도
	DSI-07.2	고객이 환경을 종료하거나 리소스를 사용하지 않을 경우 모든 컴퓨팅 리소스를 삭제하는 보증을 포함해 서비스 제공을 종료할 수 있는 게시된 절차를 제공할 수 있습니까?	

제어 그룹	CID	평가 질문	AWS 답변
			암호화됩니다. 지연 시간을 단축하면서 효율적으로 이 과정을 수행할 수 있도록 EBS 암호화 기능은 EC2의 보다 강력한 인스턴스 유형(예: M3, C3, R3, G2)에서만 제공됩니다.
데이터 센터 보안 *자산 관리*	DCS-01.1	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, 8항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	DCS-01.2	모든 중요 공급업체의 재고를 빠짐없이 보유하고 있습니까?	
데이터 센터 보안 *제어된 액세스 지점*	DCS-02.1	물리적 보안 경계(예: 울타리, 벽, 장벽, 경비, 게이트, 전자 감시, 물리적 인증 메커니즘, 안내 데스크, 보안 순찰대)가 구현되어 있습니까?	물리적 보안 제어에는 울타리, 벽, 보안 직원, 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단(단, 이에 제한되지 않음)과 같은 경계 제어가 포함됩니다. AWS SOC 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 11항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
데이터 센터 보안 *장비 식별*	DCS-03.1	알려진 장비 위치를 기반으로 연결 인증 무결성을 검증하기 위한 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.
데이터 센터 보안 *오프사이트 승인*	DCS-04.1	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 클라우드 보안 백서를 참조하십시오.

제어 그룹	CID	평가 질문	AWS 답변
데이터 센터 보안 *오프사이트 장비*	DCS-05.1	테넌트에게 자산 관리 및 장비 용도 변경을 관할하는 정책 및 절차를 증빙하는 문서를 제공할 수 있습니까?	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, 8항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
데이터 센터 보안 *정책*	DCS-06.1	사무실, 방, 시설 및 보안 영역에서 안전하고 안정적인 업무 환경을 유지할 수 있는 정책, 표준 및 절차가 마련되어 있음을 증명할 수 있습니까?	AWS는 외부 인증 기관 및 독립적 감사 기관과 협력하여 규정 준수 프레임워크 준수를 검토하고 검증합니다. AWS SOC 보고서는 AWS에서 실행하는 특정 물리적 보안 제어 활동에 대한 자세한 정보를 제공합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 11항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	DCS-06.2	직원 및 관련 제3자가 문서화된 정책, 표준 및 절차에 대해 교육을 받았음을 증명할 수 있습니까?	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 클라우드 보안 백서를 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증을 준수함을 검증 및 인증받았습니다. AWS SOC 1 및 SOC 2 보고서에서도 자세한 내용을 확인하실 수 있습니다.
데이터 센터 보안 *보안 영역 승인*	DCS-07.1	테넌트가 데이터가 저장되거나 액세스되는 위치를 기반으로 법정 관할 고려사항을 처리하기 위해 데이터를 가져오거나 내보낼 수 있는 지리적 위치를 지정할 수 있습니까?	AWS 고객은 데이터가 위치할 물리적 리전을 지정합니다. 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(오레곤), 미국 서부(캘리포니아 북부), AWS GovCloud(미국, 오레곤), EU(아일랜드), EU(프랑크푸르트), 아시아 태평양(서울), 아시아 태평양(싱가포르), 아시아 태평양(도쿄), 아시아 태평양(시드니), 중국(베이징) 리전, 남아메리카(상파울루) 등 12개 리전이 있습니다.

제어 그룹	CID	평가 질문	AWS 답변
데이터 센터 보안 *권한 없는 개인의 진입*	DCS-08.1	서비스 영역과 같은 진입점 및 진출점과 권한 없는 개인이 구내에 진입할 수 있는 기타 지점이 모니터링되고 통제되고 데이터 스토리지 및 프로세스로부터 격리되어 있습니까?	건물 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. SOC, PCI DSS, ISO 27001 및 FedRAMP 준수 여부에 대한 감사 중 외부의 독립적 감사 기관에서 AWS 물리적 보안 메커니즘을 검토합니다.
데이터 센터 보안 *사용자 액세스*	DCS-09.1	사용자 및 지원 담당자별로 정보 자산과 기능에 대한 물리적 액세스를 제한합니까?	
암호화 및 키 관리 *권한*	EKM-01.1	키를 식별 가능한 소유자와 바인딩하는 키 관리 정책이 마련되어 있습니까?	AWS는 고객에게 S3, EBS 및 EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있는 기능을 제공합니다. VPC 세션도 암호화됩니다. 또한 고객은 AWS Key Management Systems(KMS)를 이용하여 암호화 키를 생성 및 제어할 수 있습니다(https://aws.amazon.com/kms/ 참조). 내부적으로 AWS는 AWS 인프라 내에서 사용되는 필수 암호화용 암호화 키를 설정하고 관리합니다. 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 준수를 위해 외부의 독립적 감사 기관으로부터 AWS 암호화 프로세스를 검토 받습니다.
암호화 및 키 관리 *키 생성*	EKM-02.1	테넌트별로 고유한 암호화 키를 생성할 수 있습니까?	AWS는 고객이 S3, EBS 및 EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있도록 지원합니다. VPC에 대한 IPSec 터널도 암호화됩니다. 또한 고객은 AWS Key Management Systems(KMS)를 이용하여 암호화 키를 생성 및 제어할 수 있습니다(https://aws.amazon.com/kms/ 참조). KMS에 대한 자세한 내용은 AWS SOC 보고서를 참조하십시오. AWS 클라우드 보안 백서(http://aws.amazon.com/security)에서도 자세한 내용을 확인하실 수 있습니다.
	EKM-02.2	테넌트를 대신해 암호화 키를 관리할 수 있습니까?	
	EKM-02.3	키 관리 절차를 관리합니까?	
	EKM-02.4	암호화 키 수명 주기의 각 단계에 대해 소유권을 문서화했습니까?	

제어 그룹	CID	평가 질문	AWS 답변
	EKM-02.5	암호화 키를 관리하기 위한 타사/오픈 소스/자체 프레임워크를 사용합니까?	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 준수를 위해 외부의 독립적 감사 기관으로부터 AWS 암호화 프로세스를 검토 받습니다.
암호화 및 키 관리 *암호화*	EKM-03.1	환경 내에서 디스크 또는 스토리지에 저장된 데넌트 데이터를 암호화합니까?	AWS는 고객이 S3, EBS 및 EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있도록 지원합니다. VPC에 대한 IPSec 터널도 암호화됩니다. 또한 고객은 AWS Key Management Systems(KMS)를 이용하여 암호화 키를 생성 및 제어할 수 있습니다(https://aws.amazon.com/kms/ 참조). KMS에 대한 자세한 내용은 AWS SOC 보고서를 참조하십시오. AWS 클라우드 보안 백서(http://aws.amazon.com/security)에서도 자세한 내용을 확인하실 수 있습니다.
	EKM-03.2	네트워크와 하이퍼바이저 인스턴스 간에 데이터와 가상 머신 이미지를 전송할 때 암호화를 활용해 이러한 데이터를 보호합니까?	
	EKM-03.3	데넌트가 생성한 암호화 키를 지원하거나 데넌트가 공개 키 인증서에 액세스하지 않고도 ID 데이터를 암호화할 수 있도록 허용합니까(예: ID 기반 암호화)?	
	EKM-03.4	암호화 관리 정책, 절차 및 지침을 설정 및 정의하는 문서가 있습니까?	
암호화 및 키 관리 *스토리지 및 액세스*	EKM-04.1	개방형/검증된 형식 및 표준 알고리즘을 사용하는, 플랫폼 및 데이터에 적합한 암호화가 마련되어 있습니까?	AWS는 고객이 S3, EBS 및 EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있도록 지원합니다. 또한 고객은 AWS Key Management Systems(KMS)를 이용하여 암호화 키를 생성 및 제어할 수

제어 그룹	CID	평가 질문	AWS 답변
	EKM-04.2	암호화 키를 클라우드 소비자 또는 신뢰할 수 있는 키 관리 공급자가 유지합니까?	있습니다(https://aws.amazon.com/kms/ 참조). KMS에 대한 자세한 내용은 AWS SOC 보고서를 참조하십시오. 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 준수를 위해 외부의 독립적 감사 기관으로부터 AWS 암호화 프로세스를 검토 받습니다.
	EKM-04.3	암호화 키를 클라우드 안에 저장합니까?	
	EKM-04.4	키 관리 및 키 사용 업무가 분리되어 있습니까?	
거버넌스 및 위험 관리 *기준 요건*	GRM-01.1	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, 14 및 18항을 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.
	GRM-01.2	정보 보안 기준에 따라 인프라의 규정 준수를 지속적으로 모니터링 및 보고할 수 있습니까?	
	GRM-01.3	고객이 내부 표준을 준수할 수 있도록 신뢰할 수 있는 가상 머신 이미지를 제공하도록 허용합니까?	
거버넌스 및 위험 관리 *위험 평가*	GRM-02.1	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, 제어에 대한 다양한 정보를 제공하기 위해 독립 감사 기관 보고서와 인증을 발행합니다. 관련 인증 및 보고서를 AWS 고객에게 제공할 수 있습니다. 고객이 시스템에서 논리적 제어 연속 모니터링을 실행할 수 있습니다.

제어 그룹	CID	평가 질문	AWS 답변
	GRM-02.2	최소한 1년에 한 번 이상 데이터 거버넌스 요건과 관련된 위험 평가를 실시합니까?	ISO 27001 표준에 따라 AWS는 위험을 완화하고 관리하는 위험 관리 프로그램을 유지합니다. 또한 AWS는 AWS ISO 27018 인증도 유지합니다. ISO 27018 준수는 AWS가 고객 콘텐츠에 대한 개인 정보 보호를 전적으로 처리하는 일련의 제어를 실시하고 있다는 점을 고객에게 보여줍니다. 자세한 내용은 http://aws.amazon.com/compliance/iso-27018-faqs/에서 AWS 규정 준수 ISO 27018 FAQ를 참조하십시오.
거버넌스 및 위험 관리 *관리 감독*	GRM-03.1	관리자 및 직원의 책임 영역과 관련하여 관리자 자신과 소속 직원 모두에게 적용되는 보안 정책, 절차 및 표준에 대한 인식 및 준수를 유지할 책임이 기술, 업무 및 경영 관리자에게 있습니까?	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/compliance에서 AWS 위험 및 규정 준수 백서를 참조하십시오.
거버넌스 및 위험 관리 *관리 프로그램*	GRM-04.1	테넌트에게 정보 보안 관리 프로그램(ISMP)을 설명하는 문서를 제공합니까?	AWS는 고객에게 ISO 27001 인증을 제공합니다. ISO 27001 인증은 특히 AWS ISMS에 중점을 두고 어떻게 AWS 내부 프로세스가 ISO 표준을 따르는지 측정합니다. 인증은 외부의 독립적 공인 감사 기관이 AWS의 프로세스 및 제어를 평가하고 이들이 ISO 27001 인증 표준을 준수하여 운영되고 있음을 확인한 것을 의미합니다. 자세한 내용은 AWS 규정 준수 ISO 27001 FAQ 웹 사이트를 참조하십시오. http://aws.amazon.com/compliance/iso-27001-faqs/.
	GRM-04.2	최소한 1년에 한 번 이상 정보 보안 관리 프로그램(ISMP)을 검토합니까?	
거버넌스 및 위험 관리 *관리 지원/개입*	GRM-05.1	공급자가 정보 보안과 개인 정보 보호 정책을 준수하도록 보장합니까?	AWS는 ISO 27002 제어, 미국 공인 회계사 협회(AICPA) 신뢰 서비스 원칙, PCI DSS v3.1 및 NIST(국립 표준 기술 연구소) 간행물 800-53(연방 정보 시스템 및 조직을 위한 보안 통제 권고)을 기반으로 ISO 27001 인증 가능 프레임워크를 통합한 정보 보안 프레임워크 및 정책을 수립했습니다. AWS는 ISO 27001 표준에 따라 타사 관계를 관리합니다. 또한 PCI DSS, ISO 27001 및 FedRAMP 준수 여부에 대한 감사 중 외부의 독립적 감사 기관에서 AWS 타사 요구 사항을 검토합니다. AWS 규정 준수 프로그램에 대한 자세한 내용은 AWS 웹 사이트
거버넌스 및 위험 관리 *정책*	GRM-06.1	정보 보안과 개인 정보 보호 정책이 산업 표준(ISO-27001, ISO-22307, CoBIT 등)을 준수합니까?	
	GRM-06.2	공급자가 정보 보안과 개인 정보 보호 정책을 준수하도록 보장하는 계약이 있습니까?	

제어 그룹	CID	평가 질문	AWS 답변
	GRM-06.3	제어, 아키텍처, 규정 및/또는 표준 프로세스의 실사 매핑 증거를 제공할 수 있습니까?	http://aws.amazon.com/compliance/에 공개적으로 게시되어 있습니다.
	GRM-06.4	AWS가 준수하는 제어, 표준, 인증 및/또는 규정을 공시합니까?	
거버넌스 및 위험 관리 *정책 시행*	GRM-07.1	보안 정책 및 절차를 위반한 직원에 대한 공식적인 징계 및 제재 정책이 마련되어 있습니까?	AWS는 직원에게 정보 보안과 관련한 역할 및 책임을 교육하기 위해 보안 정책 및 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/security에서 AWS 클라우드 보안 백서를 참조하십시오. 자세한 내용은 ISO 27001 표준, 부록 A, 7항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	GRM-07.2	직원이 정책 및 절차를 통해 위반 발생 시 취할 수 있는 조치를 인지할 수 있습니까?	
거버넌스 및 위험 관리 *비즈니스/정책 변경의 영향*	GRM-08.1	보안 정책, 절차, 표준 및 제어가 관련성 및 유효성을 유지할 수 있도록 위험 평가 결과에 이러한 항목에 대한 업데이트가 포함됩니까?	AWS 보안 정책, 절차, 표준 및 제어 업데이트는 ISO 27001 표준에 따라 매년 진행됩니다. 자세한 내용은 ISO 27001을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증을 준수함을 검증 및 인증받았습니다.
거버넌스 및 위험 관리 *정책 검토*	GRM-09.1	정보 보안 및/또는 개인 정보 보호 정책 자료를 변경한 경우 테넌트에게 알립니까?	http://aws.amazon.com/security 및 http://aws.amazon.com/compliance에서 제공되는 AWS 클라우드 보안 프로세스 개요 백서와 위험 및 규정 준수 백서는 AWS 정책 업데이트를 반영하기 위해 정기적으로 업데이트됩니다.
	GRM-09.2	개인 정보 보호 및 보안 정책을 최소한 매년 검토합니까?	AWS SOC 보고서는 개인 정보 보호 및 보안 정책 검토와 관련된 세부 정보를 제공합니다.
거버넌스 및 위험 관리 *평가*	GRM-10.1	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. AWS 위험 관리 프레임워크에 대한 자세한 내용은 AWS 위험 및 규정 준수 백서(aws.amazon.com/security에서 제공)를 참조하십시오.

제어 그룹	CID	평가 질문	AWS 답변
	GRM-10.2	모든 위험 범주(예: 감사 결과, 위협 및 취약성 분석, 규제 준수)를 고려하여 내재 및 잔존 위험과 관련된 발생 가능성과 영향을 독립적으로 판단합니까?	
거버넌스 및 위험 관리 *프로그램*	GRM-11.1	위험을 관리하기 위해 조직 전반에 걸친 프로그램을 문서화하여 실시하고 있습니까?	ISO 27001에 따라 AWS는 위험을 완화하고 관리하는 위험 관리 프로그램을 유지합니다. 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. PCI DSS, ISO 27001 및 FedRAMP 규정 준수 여부에 대한 감사 중 독립적인 외부 감사 기관에서 AWS 사고 관리 프로그램을 검토합니다.
	GRM-11.2	조직 전반에 걸친 위험 관리 프로그램에 대한 설명서를 제공합니까?	
인사 관리 *자산 수익률*	HRS-01.1	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 보고서는 AWS 관리 환경을 모니터링하기 위해 마련된 제어에 대한 개요를 제공합니다.
	HRS-01.2	개인 정보 보호 정책이 산업 표준을 준수합니까?	
인사 관리 *배경 조회*	HRS-02.1	현지 법률, 규정, 윤리 및 계약 제약조건에 의거하여 모든 입사지원자, 계약업체 및 관련 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. AWS SOC 보고서는 배경 조회를 위해 실시하는 제어에 대한 자세한 정보를 제공합니다.
인사 관리 *고용 계약*	HRS-03.1	직원이 수행해야 할 역할 및 정보 보안 제어에 대해 명시적으로 직원을 교육합니까?	ISO 27001 표준에 따라 모든 AWS 직원들은 정기적으로 AWS 보안 교육을 포함하고 수료증을 받아야 하는 역할 기반 교육을 수료합니다. 준수성 감사는 직원들이 확립된 정책을 이해하고 따르는지 검증하기 위해 정기적으로 수행됩니다. 자세한 내용은 SOC 보고서를 참조하십시오.
	HRS-03.2	직원이 수료한 교육의 수료증을 문서화합니까?	

제어 그룹	CID	평가 질문	AWS 답변
	HRS-03.3	모든 직원이 고객/테넌트 정보를 보호하기 위한 고용 조건으로 NDA 또는 기밀 협약에 서명해야 합니까?	AWS 시스템 및 디바이스를 지원하는 모든 개인은 액세스 권한이 부여되기에 앞서 비밀 유지 계약서에 서명해야 합니다. 또한, 고용 시 직원은 Amazon 기업 행동강령 및 윤리강령(행동강령) 정책을 읽고 수락해야 합니다.
	HRS-03.4	교육 프로그램을 지정된 시간 내에 성공적을 이수하는 것이 민감한 시스템에 대한 액세스를 획득하고 유지하기 위한 전제조건입니까?	
	HRS-03.5	직원을 대상으로 최소한 1년에 한 번 이상 인식 제고 프로그램을 교육합니까?	
인사 관리 *고용 종료*	HRS-04.1	고용 변경 및/또는 종료를 규제하는 문서화된 정책, 절차 및 지침이 마련되어 있습니까?	AWS 인사관리 팀은 직원 및 벤더의 종료 및 역할 변경 시 따라야 할 내부 관리 책임을 정의합니다. AWS SOC 보고서에 자세한 정보가 나와 있습니다.
	HRS-04.2	상기 절차 및 지침이 적시의 접근 권한 취소 및 자산 반환을 고려합니까?	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 보고서는 사용자 액세스 취소에 대한 자세한 내용을 제공합니다. AWS 보안 백서의 "직원 수명 주기" 단원에도 자세한 내용이 나와 있습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 7항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
인사 관리 *이동식/모바일 디바이스*	HRS-05.1	일반적으로 비 이동식 디바이스(예: 공급자 조직의 시설에 설치된 데스크톱 컴퓨터)보다 위험이 더 높은 이동식 및 모바일 디바이스(예: 노트북, 휴대폰, 개인 정보 단말기(PDA) 등)의 중요한 데이터와 테넌트 데이터에 대한 액세스를 엄격하게 제한하기 위한 정책과 절차를 확립하고 조치를 마련했습니까?	고객은 데이터와 관련 미디어 자산에 대한 관리 권한과 책임을 보유합니다. 모바일 디바이스의 보안과 고객 콘텐츠에 대한 액세스를 관리해야 할 책임은 고객에게 있습니다.

제어 그룹	CID	평가 질문	AWS 답변
인사 관리 *비밀 유지 계약*	HRS-06.1	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.
인사 관리 *역할/책임*	HRS-07.1	테넌트에게 관리자 책임과 테넌트의 책임을 명료하게 설명하는 역할 정의 문서를 제공합니까?	AWS 클라우드 보안 백서와 AWS 위험 및 규정 준수 백서는 AWS와 고객의 역할 및 책임에 대한 자세한 정보를 제공합니다. 백서는 http://aws.amazon.com/security 및 http://aws.amazon.com/compliance에서 참조할 수 있습니다.
인사 관리 *사용 제한*	HRS-08.1	테넌트 데이터 및 메타데이터를 활용하거나 액세스할 수 있는 방법에 대한 문서를 제공합니까?	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. 고객은 데이터와 관련 미디어 자산에 대한 관리 권한과 책임을 보유합니다. 모바일 디바이스의 보안과 고객 콘텐츠에 대한 액세스를 관리해야 할 책임은 고객에게 있습니다. 자세한 내용은 ISO 27001 표준과 ISO 27018 실천 강령을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 및 ISO 27018 인증을 준수함을 검증 및 인증받았습니다.
	HRS-08.2	검사 기술(검색 엔진 등)을 사용해 테넌트 데이터 사용에 대한 메타데이터를 수집 또는 생성합니까?	
	HRS-08.3	테넌트가 검사 기술을 통한 데이터/메타데이터 액세스를 옵트아웃할 수 있습니까?	
인사 관리 *교육/인식*	HRS-09.1	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 공식적인 역할 기반 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. SOC, PCI DSS, ISO 27001 및 FedRAMP 준수 여부에 대한 감사 중 외부의 독립적 감사 기관에서 AWS 역할 및 책임을 검토합니다.
	HRS-09.2	관리자와 데이터 관리자가 보안 및 데이터 무결성과 관련한 각자의 법적 책임에 대해 적절한 교육을 받았습니까?	

제어 그룹	CID	평가 질문	AWS 답변
인사 관리 *사용자 책임*	HRS-10.1	사용자가 게시된 보안 정책, 절차, 표준, 적용 가능한 규제 요건을 인식하고 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. ISO 27001 표준, 부록 A, 7 및 8항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. http://aws.amazon.com/security에서 제공되는 AWS 클라우드 보안 백서에서도 자세한 내용을 확인하실 수 있습니다.
	HRS-10.2	사용자가 안전하고 안정적인 업무 환경을 유지할 책임을 인지하도록 돕고 있습니까?	
	HRS-10.3	사용자가 자리를 비울 때 장비를 안전하게 보관해야 할 책임을 인지하도록 돕고 있습니까?	
인사 관리 *작업 영역*	HRS-11.1	데이터 관리 정책과 절차에 테넌트 및 서비스 차원의 이해충돌이 설명되어 있습니까?	AWS 데이터 관리 정책은 ISO 27001 표준을 준수합니다. ISO 27001 표준, 부록 A, 8 및 9항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. AWS SOC 보고서는 AWS에서 AWS 리소스에 대한 무단 액세스를 방지하기 위해 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. 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. 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.
	HRS-11.2	데이터 관리 정책 및 절차에 테넌트 데이터에 대한 무단 액세스를 방지할 수 있는 변조 감사 또는 소프트웨어 기능이 포함되어 있습니까?	
	HRS-11.3	가상 머신 관리 인프라에 가상 머신의 빌드/구성 변경을 탐지할 수 있는 변조 감사 또는 소프트웨어 무결성 기능이 포함되어 있습니까?	
자격 증명 및 액세스 관리 *감사 도구* *액세스*	IAM-01.1	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 보고서는 AWS 리소스에 대한 액세스 프로비저닝을 관리하기 위해 마련된 제어를 개략적으로 설명합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 클라우드 보안 백서를 참조하십시오.

제어 그룹	CID	평가 질문	AWS 답변
	IAM-01.2	정보 보안 관리 시스템에 대한 권한 액세스(관리자 수준)를 모니터링 및 기록합니까?	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. AWS는 지속적인 SOC, PCI DSS, ISO 27001 및 FedRAMP 준수를 위해 외부의 독립적 감사 기관으로부터 AWS 로깅 및 모니터링 프로세스를 검토받습니다.
자격 증명 및 액세스 관리 *사용자 액세스 정책*	IAM-02.1	더 이상 비즈니스에 필요하지 않은 시스템 액세스를 적시에 제거할 수 있는 제어가 마련되어 있습니까?	AWS SOC 보고서는 사용자 액세스 취소에 대한 자세한 내용을 제공합니다. AWS 보안 백서의 "직원 수명 주기" 단원에도 자세한 내용이 나와 있습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 9항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	IAM-02.2	더 이상 비즈니스에 필요하지 않은 시스템 액세스를 제거할 수 있는 속도를 추적하는 측정치를 제공합니까?	
자격 증명 및 액세스 관리 *진단/포트 액세스 구성*	IAM-03.1	전용 보안 네트워크를 활용해 클라우드 서비스 인프라에 대한 관리 액세스를 제공합니까?	배포된 제어가 AWS 액세스 정책에 따라 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, ISO 27001, PCI, ITAR 및 FedRAMP 감사 중 독립적 감사 기관으로부터 권한 사용자 액세스 제어를 검토받습니다.
자격 증명 및 액세스 관리 *정책 및 절차*	IAM-04.1	IT 인프라에 액세스할 수 있는 모든 직원의 자격 증명(액세스 수준 포함)을 관리 및 저장합니까?	
	IAM-04.2	네트워크 액세스 권한을 보유한 모든 직원의 사용자 자격 증명(액세스 수준 포함)을 관리 및 저장합니까?	

제어 그룹	CID	평가 질문	AWS 답변
자격 증명 및 액세스 관리 *업무 분담*	IAM-05.1	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, 6항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
자격 증명 및 액세스 관리 *소스 코드 액세스 제한*	IAM-06.1	애플리케이션, 프로그램 또는 객체 소스 코드에 대한 무단 액세스를 방지하고 권한 있는 사람에게만 액세스를 허용하는 제어가 마련되어 있습니까?	ISO 27001 표준에 따라 AWS는 AWS 리소스에 대한 논리적 액세스에 대한 최소 표준을 규정하는 공식적인 정책 및 절차를 확립했습니다. AWS SOC 보고서는 AWS 리소스에 대한 액세스 프로비저닝을 관리하기 위해 마련된 제어를 개략적으로 설명합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
	IAM-06.2	테넌트 애플리케이션, 프로그램 또는 객체 소스 코드에 대한 무단 액세스를 방지하고 권한 있는 사람에게만 액세스를 허용하는 제어가 마련되어 있습니까?	
자격 증명 및 액세스 관리 *제3자 액세스*	IAM-07.1	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 보고서에 자세한 정보가 나와 있습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 15항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증을 준수함을 검증 및 인증받았습니다.
	IAM-07.2	공급자 실패 시 업스트림 공급자를 통해 서비스 연속성을 모니터링합니까?	
	IAM-07.3	각 서비스에 공급자가 둘 이상 있습니까?	
	IAM-07.4	사용하는 서비스를 포함하여 운영 중복성 및 연속성 요약에 대한 액세스 권한을 제공합니까?	
	IAM-07.5	테넌트에게 재해를 선언할 수 있는 기능을 제공합니까?	
	IAM-07.6	테넌트가 트리거하는 failover 옵션을 제공합니까?	
	IAM-07.7	비즈니스 연속성 및 중복성 계획을 테넌트와 공유합니까?	

제어 그룹	CID	평가 질문	AWS 답변
자격 증명 및 액세스 관리 *사용자 액세스 제한/승인*	IAM-08.1	테넌트 데이터에 대한 액세스를 허용하고 승인하는 방법을 문서화합니까?	AWS 고객은 데이터에 대한 관리 및 소유권을 보유합니다. 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, ISO 27001, PCI, ITAR 및 FedRAMP 감사 중 독립적 감사 기관으로부터 권한 사용자 액세스 제어를 검토받습니다.
	IAM-08.2	액세스 제어 목적으로 공급자 및 테넌트 데이터 분류 방법론을 조정할 수 있는 방법이 있습니까?	
자격 증명 및 액세스 관리 *사용자 액세스 승인*	IAM-09.1	관리 팀이 사용자(예: 직원, 계약업체, 고객(테넌트), 비즈니스 파트너 및/또는 공급업체)가 데이터 또는 모든 소유형 또는 관리형 (물리적 및 가상) 애플리케이션, 인프라 시스템 및 네트워크 구성 요소에 액세스하기 전에 사용자 액세스 승인 및 제한을 프로비저닝합니까?	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.
	IAM-09.2	데이터 또는 모든 소유형 또는 관리형 (물리적 및 가상) 애플리케이션, 인프라 시스템 및 네트워크 구성 요소에 대한 사용자 액세스(예: 직원, 계약업체, 고객(테넌트), 비즈니스 파트너 및/또는 공급업체)를 요청 시 제공합니까?	AWS는 부적절한 내부자 액세스 위협을 해결하기 위한 제어를 확립했습니다. 모든 인증 및 제3자 증명은 논리적 액세스와 관련한 사전적 및 사후적 제어를 평가합니다. 또한 정기적인 위험 평가를 통해 내부자 액세스가 어떻게 제어 및 모니터링되고 있는지 집중적으로 검토합니다.
자격 증명 및 액세스 관리 *사용자 액세스 검토*	IAM-10.1	모든 시스템 사용자 및 관리자에게 최소한 1년에 한 번 자격 증명을 요구합니까(테넌트가 관리하는 사용자 제외)?	ISO 27001 표준에 따라 정기적으로 모든 액세스 권한이 검토되며 명시적 재승인을 받지 않으면 리소스에 대한 액세스가 자동으로 취소됩니다. 사용자 액세스 검토와 관련한 제어가 SOC 보고서에 개략적으로 설명되어 있습니다. 사용자 권한 제어 예외가 SOC 보고서에 설명되어 있습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 9항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	IAM-10.2	사용자의 권한이 부적절하다고 판명된 경우 모든 수정 및 인증 조치가 기록됩니까?	

제어 그룹	CID	평가 질문	AWS 답변
	IAM-10.3	테넌트 데이터에 대한 무단 액세스가 허용될 수 있는 경우 테넌트와 권한 수정 및 인증 보고서를 공유합니까?	
자격 증명 및 액세스 관리 *사용자 액세스 취소*	IAM-11.1	직원, 계약업체, 고객, 비즈니스 파트너 또는 관련 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 보고서는 사용자 액세스 취소에 대한 자세한 내용을 제공합니다. AWS 보안 백서의 "직원 수명 주기" 단원에도 자세한 내용이 나와 있습니다. 자세한 내용은 ISO 27001 표준, 부록 A, 9항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	IAM-11.2	사용자 액세스 상태 변경은 고용, 계약 또는 합의 종료, 고용 변경 또는 조직 내 인사 이동을 반영합니까?	
자격 증명 및 액세스 관리 *사용자 ID 자격 증명*	IAM-12.1	기존 고객 기반 SSO(Single Sign On) 솔루션 사용을 지원하거나 이러한 솔루션을 서비스에 통합합니까?	AWS Identity and Access Management(IAM) 서비스는 AWS Management Console에 자격 증명 연동을 제공합니다. 다중 요소 인증은 고객이 선택적으로 활용할 수 있는 기능입니다. 자세한 내용은 AWS 웹 사이트(http://aws.amazon.com/mfa)를 참조하십시오. AWS Identity and Access Management(IAM)는 AWS Management Console 또는 AWS API에 대한 액세스 위임을 위해 자격 증명 연동을 지원합니다. 자격 증명 연동을 사용하면 IAM 사용자를 생성할 필요 없이 외부 자격 증명(연동 사용자)에게 AWS 계정 내 리소스에 보안 액세스가 허용됩니다. 이러한 외부 자격 증명은 기업 자격 증명 공급자(예: Microsoft Active Directory) 또는 웹 자격 증명 공급자(예: Amazon Cognito, Amazon 로그인, Facebook, Google 또는 OpenID Connect(OIDC) 호환 공급자)가 제공할 수 있습니다.
	IAM-12.2	개방형 표준을 사용해 테넌트에게 인증 기능을 위임합니까?	
	IAM-12.3	사용자 인증/권한 부여의 수단으로 자격 증명 연동 표준(SAML, SPML, WS-Federation 등)을 지원합니까?	
	IAM-12.4	사용자 액세스에 대한 지역의 법적 및 정책 제한을 적용하는 Policy Enforcement Point 기능(예: XACML)이 있습니까?	
	IAM-12.5	데이터에 대한 역할 기반 및 컨텍스트 기반 권한 부여를 지원하는 ID 관리 시스템이 마련되어 있습니까(테넌트 데이터 분류 지원)?	

제어 그룹	CID	평가 질문	AWS 답변
	IAM-12.6	테넌트에게 강력한(멀티 팩터) 사용자 액세스 인증 옵션(디지털 인증, 토큰, 생체 인식 등)을 제공하고 있습니까?	
	IAM-12.7	테넌트가 제3자 신원 확인 서비스를 사용하도록 허용합니까?	
	IAM-12.8	암호(최소 길이, 사용 기간, 이력, 복잡성) 및 계정 잠금(잠금 기준, 잠금 기간) 정책 시행을 지원합니까?	AWS Identity and Access Management(IAM)를 통해 고객은 AWS 서비스와 리소스에 대한 사용자의 액세스를 안전하게 제어할 수 있습니다. IAM에 대한 자세한 내용은 웹 사이트 https://aws.amazon.com/iam/에서 확인할 수 있습니다. AWS SOC 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다.
	IAM-12.9	테넌트/고객이 계정에서 암호 및 계정 잠금 정책을 정의하도록 허용합니까?	
	IAM-12.10	최초 로그인 시 의무적으로 암호를 변경하도록 하는 기능을 지원합니까?	
	IAM-12.11	잠긴 계정의 잠금을 해제하는 메커니즘이 마련되어 있습니까(예: 이메일을 통한 셀프 서비스, 정의된 챌린지 질문, 수동 잠금 해제)?	
자격 증명 및 액세스 관리 *유틸리티 프로그램 액세스*	IAM-13.1	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 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
	IAM-13.2	가상 인프라를 직접 대상으로 하는 공격(예: 시밍, Blue Pill, 하이퍼 점핑 등)을 감지하는 기능이 있습니까?	
	IAM-13.3	기술적 제어가 가상 인프라를 표적으로 하는 공격을 방지합니까?	

제어 그룹	CID	평가 질문	AWS 답변
인프라 및 가상화 보안 *감사 로깅/침입 탐지*	IVS-01.1	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 개발되었으며 시스템 유틸리티를 적절하게 제한 및 모니터링합니다. AWS SOC 보고서는 시스템 액세스를 제한하기 위해 마련된 제어에 대한 자세한 정보를 제공합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 보안 프로세스 개요 백서를 참조하십시오.
	IVS-01.2	감사 로그에 대한 물리적 및 논리적 사용자 액세스가 권한 있는 사람에게만 허용됩니까?	
	IVS-01.3	제어/아키텍처/프로세스에 대한 규정 및 표준 실사 매핑이 수행되었다는 증거를 제공할 수 있습니까?	
	IVS-01.4	감사 로그를 중앙집중식으로 저장 및 보존합니까?	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. 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. 자세한 내용은 http://aws.amazon.com/security에서 AWS 클라우드 보안 백서를 참조하십시오.
	IVS-01.5	정기적으로 감사 로그에서 보안 이벤트(예: 자동화 도구) 여부를 검토합니까?	
인프라 및 가상화 보안 *변경 탐지*	IVS-02.1	실행 상태(예: 유휴 상태, 꺼짐 또는 실행 중)와 상관없이 가상 머신 이미지에 대한 변경을 모두 기록하고 알립니까?	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.

제어 그룹	CID	평가 질문	AWS 답변
	IVS-02.2	가상 머신에 대한 변경 사항, 또는 이미지의 이동 및 이후의 이미지 무결성 검증이 즉시 전자적 방식(예: 포털 또는 알림)을 통해 고객에게 제공됩니까?	
인프라 및 가상화 보안 *클록 동기화*	IVS-03.1	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.
인프라 및 가상화 보안 *용량/리소스 계획*	IVS-04.1	상황/시나리오에 따른 시스템 수준별(네트워크, 스토리지, 메모리, I/O 등) 초과 구독에 대해 안내하는 설명서를 제공하고 있습니까?	AWS 서비스 제한에 대한 자세한 내용과 특정 서비스에 대해 한도 상향을 요청하는 방법은 AWS 웹 사이트 http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html을 참조하십시오. AWS는 ISO 27001 표준에 따라 용량 및 사용률 데이터를 관리합니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	IVS-04.2	하이퍼바이저에 있는 메모리 초과 가입 기능의 사용을 제한합니까?	
	IVS-04.3	시스템 용량 요건이 테넌트에게 서비스를 제공하는 데 사용되는 모든 시스템의 현재, 예측 및 예상 용량 요구 사항을 고려합니까?	
	IVS-04.4	테넌트에게 서비스를 제공하는 데 사용되는 모든 시스템에서 규제, 계약 및 비즈니스 요건을 지속적으로 충족하기 위해 시스템 성능을 모니터링하고 튜닝합니까?	

제어 그룹	CID	평가 질문	AWS 답변
인프라 및 가상화 보안 *관리 - 취약점 관리*	IVS-05.1	보안 취약성 평가 도구 또는 서비스가 사용 중인 가상화 기술을 수용합니까(예: 가상화 인식)?	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 감사 기관이 정기적으로 평가합니다. 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 준수의 일환으로, 취약점 검사 및 수정 관행을 정기적으로 검토받습니다.
인프라 및 가상화 보안 *네트워크 보안*	IVS-06.1	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.
	IVS-06.2	보안 도메인/영역 간 데이터 흐름을 포함하는 네트워크 아키텍처 다이어그램을 정기적으로 업데이트합니까?	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.
	IVS-06.3	네트워크 내부의 보안 도메인/영역 사이에 허용되는 액세스/연결(예: 방화벽 규칙)의 적절성을 정기적으로 검토합니까?	
	IVS-06.4	모든 방화벽 액세스 제어 목록을 업무상 근거와 함께 문서화합니까?	

제어 그룹	CID	평가 질문	AWS 답변
인프라 및 가상화 보안 *운영 체제 보안 강화 및 기초 제어*	IVS-07.1	기준 구축 표준 또는 템플릿의 일환으로 기술적 제어(예: 안티바이러스, 파일 무결성 모니터링 및 로깅)을 사용하여 비즈니스 요구 사항을 충족하기 위해 필요한 포트, 프로토콜 및 서비스만 제공하도록 운영 체제가 강화됩니까?	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 FedRAMPsm 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 준수의 일환으로, 취약점 검사 및 수정 관행을 정기적으로 검토받습니다.
인프라 및 가상화 보안 *프로덕션/비 프로덕션 환경*	IVS-08.1	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/).
	IVS-08.2	IaaS 서비스의 경우 테넌트에게 적합한 프로덕션 및 테스트 환경을 구축할 수 있는 방법에 대한 지침을 제공합니까?	
	IVS-08.3	프로덕션 환경과 비 프로덕션 환경을 논리적/물리적으로 구분합니까?	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, 13항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
인프라 및 가상화 보안 *조각화*	IVS-09.1	비즈니스 및 고객 보안 요건을 충족할 수 있도록 시스템과 네트워크 환경이 방화벽 또는 가상 방화벽으로 보호됩니까?	

제어 그룹	CID	평가 질문	AWS 답변
	IVS-09.2	법률, 규제 및 계약 요건을 준수할 수 있도록 시스템과 네트워크 환경이 방화벽 또는 가상 방화벽으로 보호됩니까?	
	IVS-09.3	프로덕션 환경과 비 프로덕션 환경이 분리될 수 있도록 시스템과 네트워크 환경이 방화벽 또는 가상 방화벽으로 보호됩니까?	
	IVS-09.4	중요 데이터를 보호 및 격리할 수 있도록 시스템과 네트워크 환경이 방화벽 또는 가상 방화벽으로 보호됩니까?	
인프라 및 가상화 보안 *VM 보안 - vMotion 데이터 보호*	IVS-10.1	물리적 서버, 애플리케이션 또는 데이터를 가상 서버로 마이그레이션할 때 보안 및 암호화된 통신 채널을 사용합니까?	AWS는 고객에게 S3, EBS 및 EC2를 포함한 거의 모든 서비스에 자체 암호화 메커니즘을 사용할 수 있는 기능을 제공합니다. VPC 세션도 암호화됩니다.
	IVS-10.2	물리적 서버, 애플리케이션 또는 데이터를 가상 서버로 마이그레이션할 때 프로덕션 레벨 내트워크와 분리된 네트워크를 사용합니까?	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.
인프라 및 가상화 보안 *VMM 보안 - 하이퍼바이저 보안 강화*	IVS-11.1	가상 시스템을 호스팅하는 시스템을 위한 모든 하이퍼바이저 관리 기능 또는 관리 콘솔에 대한 직원 액세스를 최소 권한 원칙을 기반으로 제한하며 기술적 제어(예: 이중 인증, 감사 트레일, IP 주소 필터링, 방화벽, 관리 콘솔과 TLS 캡슐화된 통신)를 통해 지원됩니까?	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. 액세스 제어에 대한 자세한 내용은 AWS SOC 보고서를 참조하십시오.

제어 그룹	CID	평가 질문	AWS 답변
인프라 및 가상화 보안 *무선 보안*	IVS-12.1	무선 네트워크 환경 매개 변수를 보호하고 권한이 없는 무선 트래픽을 제한하기 위한 정책, 절차, 메커니즘이 확립, 구현 및 구성되어 있습니까?	AWS 네트워크 환경을 보호하기 위한 정책, 절차 및 메커니즘이 마련되어 있습니다. SOC, PCI DSS, ISO 27001 및 FedRAMP 준수 여부에 대한 감사 중 외부의 독립적 감사 기관에서 AWS 보안 제어를 검토합니다.
	IVS-12.2	강력한 암호화로 무선 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)	
	IVS-12.3	무선 네트워크 환경을 보호하고 권한 없는(불법) 네트워크 디바이스를 탐지하여 적시에 네트워크에서 분리할 수 있는 정책, 절차 및 메커니즘이 확립 및 구현되었습니까?	
인프라 및 가상화 보안 *네트워크 아키텍처*	IVS-13.1	네트워크 아키텍처 다이어그램이 법규 준수에 영향을 미칠 수 있는 고위험 환경 및 데이터 흐름을 명확하게 식별합니까?	AWS 고객은 정의된 요건에 따라 네트워크 조각화를 관리할 책임이 있습니다. 내부적으로 AWS 네트워크 조각화는 ISO 27001 표준을 따릅니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	IVS-13.2	변칙적 수신 또는 송신 트래픽 패턴(예: MAC 스푸핑 및 ARP 중독 공격) 및/또는 DDoS(분산 서비스 거부) 공격과 관련된 네트워크 기반 공격을 탐지 및 적시 대응하기 위한 기술 조치를 구현하고 심층적 방어 기법(예: 심층 패킷 분석, 트래픽 스로틀링, 블랙홀링)을 적용합니까?	AWS 보안 팀은 정기적으로 모든 인터넷 연결 서비스 엔드포인트 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 감사 기관과 협력하여 AWS 전체 제어 환경을 검토하고 테스트합니다. SOC, PCI DSS, ISO 27001 및 FedRAMP 준수 여부에 대한 감사 중 외부의 독립적 감사 기관에서 AWS 보안 제어를 검토합니다.

제어 그룹	CID	평가 질문	AWS 답변
상호 운용성 및 이동성 *API*	IPY-01	서비스에서 사용 가능한 모든 API의 목록을 게시하고 표준형이고 어느 API가 사용자 지정되었는지 표시합니까?	AWS API에 대한 자세한 내용은 AWS 웹 사이트(https://aws.amazon.com/documentation/)를 참조하십시오. ISO 27001 표준에 따라 AWS는 AWS 리소스에 대한 논리적 액세스에 대한 최소 표준을 규정하는 공식적인 정책 및 절차를 확립했습니다. AWS SOC 보고서는 AWS 리소스에 대한 액세스 프로비저닝을 관리하기 위해 마련된 제어를 개략적으로 설명합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 클라우드 보안 백서를 참조하십시오.
상호 운용성 및 이동성 *데이터 요청*	IPY-02	요청 시 비정형 고객 데이터를 산업 표준 형식(예: .doc, .xls, .pdf)으로 제공합니까?	
상호 운용성 및 이동성 *정책 및 법규*	IPY-03.1	AWS 서비스와 타사 애플리케이션 간 상호 운용성을 위해 API 사용을 관할하는 정책 및 절차(예: 서비스 수준 계약)를 제공합니까?	
	IPY-03.2	AWS 서비스로부터 또는 AWS 서비스로 애플리케이션 데이터 마이그레이션을 관할하는 정책 및 절차(예: 서비스 수준 계약)를 제공합니까?	고객은 자신의 콘텐츠에 대한 관리 권한과 소유권을 보유합니다. 고객은 AWS 플랫폼으로 또는 외부로 애플리케이션 및 콘텐츠를 마이그레이션하는 방법을 재량에 따라 선택할 수 있습니다.
상호 운용성 및 이동성 *표준화된 네트워크 프로토콜*	IPY-04.1	데이터 가져오기, 데이터 내보내기 및 서비스 관리를 업계에서 인정되는 표준화된 보안(예: 비 클리어 텍스트 및 인증) 네트워크 프로토콜로 수행할 수 있습니까?	AWS는 고객이 필요에 따라 AWS 스토리지에서 데이터를 가져오거나 내보낼 수 있도록 허용합니다. 스토리지 옵션에 대한 자세한 내용은 http://aws.amazon.com/choosing-a-cloud-platform을 참조하십시오.
	IPY-04.2	고객(테넌트)에게 사용되는 상호 운용성 및 이동성 네트워크 프로트콜 표준을 자세하게 설명하는 문서를 제공합니까?	
상호 운용성 및 이동성 *가상화*	IPY-05.1	상호 운용성을 확보하기 위해 업계에서 인정되는 가상화 플랫폼 및 표준 가상화 형식(예: OVF)을 사용합니까?	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 감사 기관이 정기적으로 평가합니다. 자세한 내용은 http://aws.amazon.com/security에서 AWS 클라우드 보안 백서를 참조하십시오.
	IPY-05.2	사용되는 하이퍼바이저에 대한 사용자 지정 변경 사항과 모든 솔루션별 가상화 후크를 문서화하여 고객이 검토할 수 있습니까?	

제어 그룹	CID	평가 질문	AWS 답변
모바일 보안 *맬웨어 방지 소프트웨어*	MOS-01	정보 보안 인식 교육의 일환으로 모바일 디바이스에 고유한 멀웨어 방지 교육을 제공합니까?	안티바이러스/악성 소프트웨어를 관리하는 AWS의 프로그램, 프로세스 및 절차는 ISO 27001 표준을 준수합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 12항을 참조하십시오.
모바일 보안 *애플리케이션 저장*	MOS-02	회사 데이터 및/또는 회사 시스템을 액세스 또는 저장하는 모바일 디바이스를 위한 승인된 애플리케이션 스토어를 문서화하고 목록을 제공합니까?	AWS는 정보 보안 체계 및 정책을 수립했으며 ISO 27002 제어, 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(연방 정보 시스템 및 조직을 위한 보안 통제 권고)에 근거하여 ISO 27001 인증 가능한 체계를 효과적으로 통합했습니다. 고객은 데이터와 관련 미디어 자산에 대한 관리 권한과 책임을 보유합니다. 모바일 디바이스의 보안과 고객 콘텐츠에 대한 액세스를 관리해야 할 책임은 고객에게 있습니다.
모바일 보안 *승인된 애플리케이션*	MOS-03	승인된 애플리케이션 또는 승인된 애플리케이션 스토어에서 공급하는 애플리케이션만 모바일 디바이스에 로드되도록 보장하는 정책 시행 기능(에: XACML)이 있습니까?	
모바일 보안 *승인된 BYOD용 애플리케이션*	MOS-04	BYOD 정책 및 교육이 어느 애플리케이션 및 애플리케이션 스토어가 BYOD 디바이스에서 사용하도록 승인되었는지 명시합니까?	
모바일 보안 *인식 및 교육*	MOS-05	모바일 디바이스와 허용되는 모바일 디바이스 사용 및 요건을 명확하게 정의하는 모바일 디바이스 정책을 문서화하여 직원 교육에 사용합니까?	
모바일 보안 *클라우드 기반 서비스*	MOS-06	모바일 디바이스를 통해 회사 비즈니스 데이터를 이용 또는 저장하는 데 사용하도록 허용되는 사전 승인된 클라우드 기반 서비스의 목록이 문서화되어 있습니까?	
모바일 보안 *호환성*	MOS-07	디바이스, 운영 체제 및 애플리케이션 호환성 문제를 테스트하기 위한 애플리케이션 검증 프로세스가 문서화되어 있습니까?	

제어 그룹	CID	평가 질문	AWS 답변
모바일 보안 *디바이스 적격성*	MOS-08	BYOD 사용에 허용되는 디바이스 및 적격성 요건을 정의하는 BYOD 정책이 있습니까?	
모바일 보안 *디바이스 재고*	MOS-09	디바이스 상태(운영 체제 및 패치 레벨, 분실 또는 폐기, 디바이스 할당자)를 포함하여 회사 데이터를 저장 및 액세스하는 모든 모바일 디바이스의 인벤토리를 유지합니까?	
모바일 보안 *디바이스 관리*	MOS-10	회사 데이터를 저장, 전송 또는 처리하도록 허용된 모든 모바일 디바이스에 배포되는 중앙 집중식 모바일 디바이스 관리 솔루션이 있습니까?	
모바일 보안 *암호화*	MOS-11	모바일 디바이스 정책이 전체 디바이스에서 또는 중요 데이터로 식별된 데이터에 대해 모든 모바일 디바이스를 위한 기술 제어를 통해 암호화를 사용하도록 요구합니까?	
모바일 보안 *모바일 보안탈옥(jailbreaking) 및 루팅*	MOS-12.1	모바일 디바이스 정책이 모바일 디바이스에 내장된 보안 제어의 우회(예: 탈옥(jailbreaking) 또는 루팅)를 금지합니까?	
	MOS-12.2	내장된 보안 제어의 우회를 금지하는 탐지 및 예방 제어가 디바이스에서 또는 중앙 집중식 디바이스 관리 시스템을 통해 구현됩니까?	
모바일 보안 *법적 고지*	MOS-13.1	BYOD 정책이 개인 정보 보호, 소송 요건, 전자증거개시(E-Discovery) 및 법적 보존에 대한 예상을 명확하게 정의합니까?	고객은 데이터와 관련 미디어 자산에 대한 관리 권한과 책임을 보유합니다. 모바일 디바이스의 보안과 고객 콘텐츠에 대한 액세스를 관리해야 할 책임은 고객에게 있습니다.

제어 그룹	CID	평가 질문	AWS 답변
	MOS-13.2	내장된 보안 제어의 우회를 금지하는 탐지 및 예방 제어가 디바이스에서 또는 중앙 집중식 디바이스 관리 시스템을 통해 구현됩니까?	
모바일 보안 *화면 잠금*	MOS-14	BYOD 및 회사 소유 디바이스에서 자동 화면 잠금을 요구하고 기술적 제어를 통해 시행합니까?	
모바일 보안 *운영 체제*	MOS-15	회사의 변경 관리 프로세스를 통해 모바일 디바이스 운영 체제, 패치 레벨 및 애플리케이션의 모든 변경 사항을 관리합니까?	
모바일 보안 *암호*	MOS-16.1	회사에서 지급한 모바일 디바이스 및/또는 BYOD 모바일 디바이스에 대한 암호 정책이 있습니까?	
	MOS-16.2	암호 정책이 기술적 제어(예: MDM)를 통해 시행됩니까?	
	MOS-16.3	암호 정책이 모바일 디바이스를 통한 인증 요건(예: 암호/PIN 길이) 변경을 금지합니까?	
모바일 보안 *정책*	MOS-17.1	BYOD 사용자에게 지정된 회사 데이터를 백업하도록 요구하는 정책이 있습니까?	
	MOS-17.2	BYOD 사용자에게 승인되지 않은 애플리케이션 스토어의 사용을 금지하는 정책이 있습니까?	
	MOS-17.3	BYOD 사용자에게 멀웨어 방지 소프트웨어(지원되는 경우)를 사용하도록 요구하는 정책이 있습니까?	

제어 그룹	CID	평가 질문	AWS 답변
모바일 보안 *원격 삭제*	MOS-18.1	IT 팀이 회사에서 허용한 모든 BYOD 디바이스에서 원격 삭제 또는 회사 데이터 삭제를 제공합니까?	
	MOS-18.2	IT 팀이 회사에서 할당한 모든 모바일 디바이스에 대해 원격 삭제 또는 회사 데이터 삭제를 제공합니까?	
모바일 보안 *보안 패치*	MOS-19.1	디바이스 제조업체 또는 통신업체가 일반 릴리즈하는 즉시 최신 보안 관련 패치를 모바일 디바이스에 설치합니까?	
	MOS-19.2	모바일 디바이스가 회사 IT 직원이 최신 보안 패치를 다운로드하기 위한 원격 검증을 허용합니까?	
모바일 보안 *사용자*	MOS-20.1	BYOD 정책이 BYOD 지원 디바이스에서 사용 또는 액세스하도록 허용되는 시스템 및 서버를 명확하게 지정합니까?	
	MOS-20.2	BYOD 정책이 BYOD 지원 디바이스를 통해 액세스가 허용되는 사용자 역할을 지정합니까?	
보안 인시던트 관리, 전자증거개시(E-Discovery) 및 클라우드 과학수사 *연락/기관 유지*	SEF-01.1	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. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
보안 인시던트 관리, 전자증거개시(E-Discovery) 및 클라우드 과학수사	SEF-02.1	보안 인시던트 대응 계획을 문서화했습니까?	AWS의 인시던트 대응 프로그램, 계획 및 절차는 ISO 27001 표준에 따라 개발되었습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다. AWS SOC 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다.
	SEF-02.2	맞춤화된 테넌트 요건을 보안 인시던트 대응 계획에 통합합니까?	

제어 그룹	CID	평가 질문	AWS 답변
인시던트 관리	SEF-02.3	보안 인시던트 도중 AWS와 테넌트가 책임져야 할 영역을 지정하는 역할 및 책임 문서를 게시합니까?	고객을 대신해 AWS에 저장된 모든 데이터는 강력한 테넌트 격리 보안 및 제어 기능을 갖고 있습니다. AWS 클라우드 보안 백서(http://aws.amazon.com/security에서 제공)에도 자세한 내용이 나와 있습니다.
	SEF-02.4	작년에 보안 인시던트 대응 계획을 테스트했습니까?	
보안 인시던트 관리, 전자증거개시(E-Discovery) 및 클라우드 과학수사 *인시던트 보고*	SEF-03.1	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?	
	SEF-03.2	인시던트를 특정 테넌트에서 격리할 수 있도록 프레임워크를 기록하고 모니터링합니까?	
보안 인시던트 관리, 전자증거개시(E-Discovery) 및 클라우드 과학수사 *인시던트 대응 법적 준비*	SEF-04.1	인시던트 대응 계획이 법적으로 허용되는 연계보관성(chain-of-custody) 관리 프로세스 및 제어에 대한 산업 표준을 준수합니까?	
	SEF-04.2	인시던트 대응 기능에 법적으로 허용되는 과학 수사 데이터 수집 및 분석 기법 사용이 포함되어 있습니까?	
	SEF-04.3	다른 테넌트 데이터를 동결시키지 않고 특정 테넌트의 증거 보존(일정 기간 동안 데이터 동결)을 지원할 수 있습니까?	
	SEF-04.4	법적 소환에 대응해 데이터를 생성할 때 테넌트 데이터 분리를 강화하고 증명합니까?	
보안 인시던트 관리, 전자증거개시(E-Discovery)	SEF-05.1	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, 16항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001

제어 그룹	CID	평가 질문	AWS 답변
및 클라우드 과학수사 *인시던트 대응 측정치*	SEF-05.2	테넌트가 요청할 경우 보안 인시던트 데이터 통계 정보를 공유합니까?	인증 표준을 준수함을 검증 및 인증받았습니다.
공급망 관리, 투명성 및 책임 *데이터 품질 및 무결성*	STA-01.1	데이터 품질 오류와 관련 위험을 검사 및 설명하고 클라우드 공급망 파트너와 협력하여 해결합니까?	고객은 데이터 품질에 대한 관리 권한 및 소유권을 유지하므로 AWS 서비스를 사용하면서 발생할 수 있는 품질 오류도 고객의 책임입니다. 데이터 무결성 및 액세스 관리(최소 권한 액세스 포함)와 관련한 자세한 내용은 AWS SOC 보고서를 참조하십시오.
	STA-01.2	공급망 내부의 모든 담당자를 대상으로 한 업무 분담, 역할 기반 액세스, 최소 권한 액세스를 통해 데이터 보안 위험을 경감하고 제한하기 위한 제어를 고한하고 구현합니까?	
공급망 관리, 투명성 및 책임 *인시던트 보고*	STA-02.1	정기적으로 전자적 방법(예: 포털)을 통해 보안 인시던트 정보를 모든 관련 고객 및 공급자에게 제공합니까?	AWS의 인시던트 대응 프로그램, 계획 및 절차는 ISO 27001 표준에 따라 개발되었습니다. AWS SOC 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다. AWS 클라우드 보안 백서(http://aws.amazon.com/security에서 제공)에도 자세한 내용이 나와 있습니다.
공급망 관리, 투명성 및 책임 *네트워크/인프라 서비스*	STA-03.1	클라우드 서비스의 모든 관련 구성 요소에 대한 용량 및 사용 데이터를 수집합니까?	AWS는 ISO 27001 표준에 따라 용량 및 사용률 데이터를 관리합니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	STA-03.2	테넌트에게 용량 계획 및 사용 보고서를 제공합니까?	
공급망 관리, 투명성 및 책임 *공급자 내부 평가*	STA-04.1	정책, 절차 및 지원 조치/측정치의 적합성 및 유효성의 연간 내부 평가를 실시합니까?	AWS 조달 및 공급망 팀은 모든 AWS 공급업체와의 관계를 유지합니다. 자세한 내용은 ISO 27001 표준, 부록 A, 15항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
공급망 관리, 투명성 및 책임 *제3자 계약*	STA-05.1	데이터가 처리, 저장 및 전송되는 국가의 법률에 따라 아웃소싱 공급자를 선정하고 모니터링합니까?	AWS 시스템 및 디바이스를 지원하는 타사 공급자에 대한 개인 보안 요구 사항이 모회사인 AWS, Amazon.com 및 해당하는 타사 공급자 간의 상호 비밀 유지 계약서에 규정되어 있습니다. Amazon 법률 지문 및 AWS 조달 팀은

제어 그룹	CID	평가 질문	AWS 답변
	STA-05.2	데이터가 시작되는 국가의 법률에 따라 아웃소싱 공급자를 선정하고 모니터링합니까?	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. AWS는 일반적으로 AWS 서비스의 개발을 하청 업체로 아웃소싱하지 않습니다.
	STA-05.3	법률 자문 팀이 모든 제3자 계약을 검토합니까?	
	STA-05.4	제3자 계약이 정보와 자산의 보안 및 보호 규정을 포함합니까?	
	STA-05.5	클라이언트에게 모든 하위 처리 계약의 목록 및 사본을 제공하고 그 내용을 업데이트합니까?	
공급망 관리, 투명성 및 책임 *공급망 거버넌스 검토*	STA-06.1	특정 파트너의 공급망에 속하는 다른 구성원으로부터 전가되는 위험을 분석하기 위해 파트너의 위험 관리 및 거버넌스 프로세스를 검토합니까?	AWS는 주요 타사 공급자와 공식 계약을 유지하고 이들과의 비즈니스 관계에 따라 적절한 관계 관리를 실시합니다. AWS는 지속적인 SOC 및 ISO 27001 준수의 일환으로 독립적인 감사 기관으로부터 AWS의 제3자 관리 프로세스를 검토받습니다.
공급망 관리, 투명성 및 책임 *공급망 측정치*	STA-07.1	공급자와 고객(테넌트) 사이에서 완전하고 정확하며 관련성 있는 계약을 유지하기 위해 정책 및 절차가 확립되고 지원 비즈니스 프로세스 및 기술적 조치(예: SLA)가 구현되어 있습니까?	
	STA-07.2	전체 공급망(업스트림/다운스트림)에 걸쳐 규정 및/또는 조건의 비적합성을 측정하고 해결할 능력을 보유하고 있습니까?	
	STA-07.3	상이한 공급자 관계로 인한 서비스 수준 충돌 또는 불일치를 관리할 수 있습니까?	
	STA-07.4	최소한 1년에 한 번 이상 모든 계약, 정책 및 프로세스를 검토합니까?	

제어 그룹	CID	평가 질문	AWS 답변
공급망 관리, 투명성 및 책임 *평가 대행*	STA-08.1	연간 검토를 실시하여 정보 공급망에서 합리적인 정보 보안을 보장합니까?	
	STA-8.2	연간 검토에 정보 공급망이 이용하는 모든 파트너/타사 공급자가 포함됩니까?	
공급망 관리, 투명성 및 책임 *제3자 감사*	STA-09.1	테넌트가 독립적인 취약성 평가를 수행할 수 있도록 허용합니까?	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 보고서는 AWS에서 실행하는 특정 제어 활동에 대한 자세한 정보를 제공합니다.
	STA-09.2	외부 기관이 애플리케이션 및 네트워크에 대한 취약성 검사와 정기적인 침투 테스트를 수행합니까?	
위협 및 취약점 관리 *안티바이러스/악성 소프트웨어*	TVM-01.1	모든 시스템에 클라우드 서비스를 지원하거나 클라우드 서비스와 연결되는 맬웨어 방지 프로그램이 설치되어 있습니까?	안티바이러스/악성 소프트웨어를 관리하는 AWS의 프로그램, 프로세스 및 절차는 ISO 27001 표준을 준수합니다. 자세한 내용은 AWS SOC 보고서를 참조하십시오. ISO 27001 표준, 부록 A, 12항에서도 자세한 내용을 확인하실 수 있습니다. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	TVM-01.2	업계에서 허용하는 기간 내에 모든 인프라 구성 요소에서 서명, 목록 또는 행동 패턴을 사용하는 보안 침입 탐지 시스템을 업데이트합니까?	
위협 및 취약점 관리 *취약성/패치 관리*	TVM-02.1	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
	TVM-02.2	산업 모범 사례에 규정된 대로 애플리케이션 계층 취약성 검사를 정기적으로 수행하고 있습니까?	

제어 그룹	CID	평가 질문	AWS 답변
	TVM-02.3	산업 모범 사례에 규정된 대로 로컬 운영 체제 계층 취약점 검사를 정기적으로 수행하고 있습니까?	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 내용은 http://aws.amazon.com/security에서 AWS 클라우드 보안 백서를 참조하십시오. 자세한 내용은 ISO 27001 표준, 부록 A, 12항을 참조하십시오. AWS는 독립적인 감사 기관으로부터 ISO 27001 인증 표준을 준수함을 검증 및 인증받았습니다.
	TVM-02.4	테넌트가 요청할 경우 취약성 검사 결과를 제공합니까?	
	TVM-02.5	모든 컴퓨팅 디바이스, 애플리케이션, 시스템 전반에서 신속하게 취약성에 패치를 적용할 수 있습니까?	
	TVM-02.6	테넌트가 요청할 경우 위험 기반 시스템 패치 적용 기간을 제공합니까?	
위협 및 취약점 관리 *모바일 코드*	TVM-03.1	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.
	TVM-03.2	권한이 없는 모든 모바일 코드는 실행되지 않습니까?	

참고 문헌

추가 정보는 다음 출처를 참조하십시오.

- AWS 위험 및 규정 준수 개요
- AWS 인증, 프로그램, 보고서 및 제3자 증명
- 규정 준수 관련 주요 질문에 대한 AWS의 답변

문서 수정

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