규정 준수 관련 주요 질문에 대한 AWS의 답변

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

본 문서에서는 AWS와 관련된 일반적인 클라우드 컴퓨팅 규정 준수 질문을 다룹니다. 이 답변은 클라우드 컴퓨팅 환경에서 평가 및 운영할 경우에 도움이 될 수 있으며 AWS 고객의 컨트롤 관리 노력을 지원할 수 있습니다.

규정 준수 관련 주요 질문과 답변

카테고리	클라우드 컴퓨팅 질문	AWS 정보
컨트롤 소유권	클라우드 배포 인프라에 있어 누가 어떤 컨트롤을 소유합니까?	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.
IT 감사	클라우드 공급자 감사를 수행하는 방법은 무엇입니까?	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.
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.
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.

카테고리	클라우드 컴퓨팅 질문	AWS 정보
GLBA 규정 준수	클라우드 공급자 환경에 배포할 경우 GLBA 인증 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.
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), FedRAMP(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.
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. 전체 리전 목록을 보려면 aws.amazon.com/about-aws/global-infrastructure를 참조하십시오.
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.
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

카테고리	클라우드 컴퓨팅 질문	AWS 정보
		사본을 요청할 수 있습니다. 또한 데이터 센터 물리적 보안에 대한 독립적인 검토가 ISO 27001 감사, PCI 평가, ITAR 감사 및 FedRAMP[sm] 테스트 프로그램의 일부로 실시됩니다.
제3자 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 액세스와 관련된 특정 컨트롤, 데이터 센터 액세스 권한 부여 및 기타 관련 컨트롤에 대한 자세한 내용은 SOC 1 Type II 보고서를 참조하십시오.
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 FedRAMP[sm] 감사 중 독립적 감사 기관으로부터 권한 사용자 액세스 제어를 검토 받습니다.
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.
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. **참고**: 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.

카테고리	클라우드 컴퓨팅 질문	AWS 정보
하이퍼바이저 취약점	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.
취약점 관리	시스템에 적절하게 패치가 적용되었습니까?	AWS는 시스템에 패치를 적용하여 하이퍼바이저 및 네트워킹 서비스 등 고객 서비스를 지원할 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.
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.
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.
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.
조합 서비스	클라우드 공급자가 자체 서비스와 다른 공급자의 클라우드 서비스를 함께 제공합니까?	AWS는 고객에게 AWS 서비스를 제공하기 위해 제3자 클라우드 공급자를 활용하지 않습니다.
물리적 및 환경 컨트롤	이러한 컨트롤은 지정된 클라우드 공급자가 운영합니까?	예. SOC 1 Type II 보고서에 자세하게 설명되어 있습니다. 또한, AWS에서 지원하는 ISO 27001 및 FedRAMP[sm] 같은 다른 인증의 경우에도 물리적 및 환경적 컨트롤로 사용될 모범 사례가 필요합니다.

카테고리	클라우드 컴퓨팅 질문	AWS 정보
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.
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.
ID 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.
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.
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 규모를 확장하거나 축소할 수 있으며 사용한 용량에 대해서만 비용을 지불합니다.
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.
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.
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.
서비스 공급자 비즈니스 연속성	서비스 공급자가 비즈니스 연속성 프로그램을 운영합니까?	AWS는 비즈니스 연속성 프로그램을 운영합니다. 자세한 내용이 AWS 보안 백서에 나와 있습니다.

카테고리	클라우드 컴퓨팅 질문	AWS 정보
고객 비즈니스 연속성	서비스 공급자가 고객이 비즈니스 연속성 계획을 구현할 수 있도록 허용합니까?	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.
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.
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.
가격 인상	서비스 공급자가 예기치 않게 가격을 올립니까?	AWS는 시간이 지나면서 이러한 서비스를 제공하는 비용이 감소에 따라 비용을 낮춘 사례가 자주 있습니다. AWS는 지난 몇 년간 지속적으로 가격을 낮춰 왔습니다.
지속가능성	서비스 공급자가 장기적인 지속가능성 잠재력을 보유하고 있습니까?	AWS는 선도적인 클라우드 공급자로, Amazon.com의 장기적인 비즈니스 전략입니다. AWS는 매우 장기적인 지속가능성 잠재력을 보유하고 있습니다.

참고 문헌

추가 정보는 다음 출처를 참조하십시오.

- AWS 위험 및 규정 준수 개요
- AWS 인증, 프로그램, 보고서 및 제3자 증명
- CSA 공동 평가 질문서

문서 수정

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