Unable to locate subtitle

Amazon Web Services: 위험 및 규정 준수

Amazon Web Services: 위험 및 규정 준수: ***Unable to locate subtitle***

Table of Contents

Amazon Web Services: 위험 및 규정 준수

게시 날짜: 2021년 3월 11일(문서 개정)

요약

AWS는 규제 대상 산업에 속하는 고객을 포함하여 다양한 고객에게 서비스를 제공합니다. AWS는 공동 책임 모델을 통해 고객이 IT 환경에서 위험을 효과적이고 효율적으로 관리할 수 있도록 지원하며, 확립되고 널리 인정받는 프레임워크 및 프로그램을 준수함으로써 효과적인 위험 관리를 보장합니다. 이 백서에서는 공동 책임 모델 차원에서 AWS가 위험을 관리하기 위해 구현한 메커니즘과 이러한 메커니즘이 효과적으로 구현되고 있는지 확인하기 위해 고객이 활용할 수 있는 도구에 대해 설명합니다.

소개

AWS와 고객은 IT 환경을 함께 제어합니다. 따라서 보안은 공동 책임입니다. AWS 클라우드에서 보안 및 규정 준수를 관리할 때는 각 당사자에게 고유한 책임이 있습니다. 고객의 책임은 사용하는 서비스에 따라 다릅니다. 그러나 일반적으로 고객은 특정 보안 및 규정 준수 요구 사항에 부합하는 방식으로 IT 환경을 구축할 책임이 있습니다.

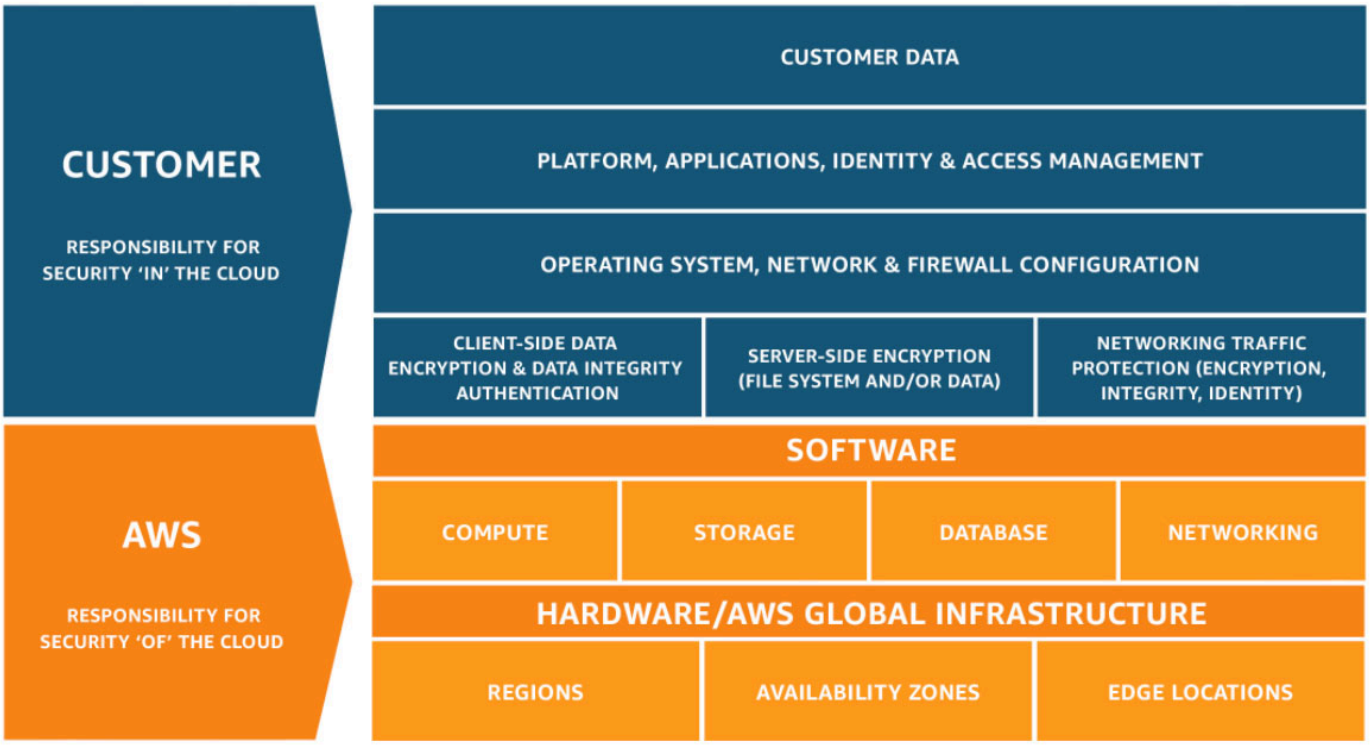
이 백서에서는 각 당사자의 보안 책임과 고객이 AWS 위험 및 규정 준수 프로그램의 혜택을 누릴 수 있는 방법에 대해 자세히 설명합니다.

공동 책임 모델

보안 및 규정 준수는 AWS와 고객의 공동 책임입니다. 배포된 서비스에 따라 이 공동 책임 모델은 고객의 운영 부담을 완화하는 데 도움이 될 수 있습니다. AWS가 호스트 운영 체제 및 가상화 계층부터 서비스 운영 시설의 물리적인 보안에 이르기까지 구성 요소를 운영, 관리 및 제어하기 때문입니다. 고객의 책임 및 관리 범위에는 게스트 운영 체제(업데이트 및 보안 패치 포함) 및 기타 관련 애플리케이션 소프트웨어 그리고 AWS가 제공하는 보안 그룹 방화벽의 구성이 포함됩니다.

고객은 사용하는 서비스, 서비스를 IT 환경에 통합하는 과정 및 준거법과 규제에 따라 책임 범위가 다르기 때문에 신중하게 서비스를 선택해야 합니다. 고객은 호스트 기반 방화벽, 호스트 기반 침입 탐지 및 방지, 암호화 및 키 관리와 같은 기술을 활용하여 보안을 강화하고 더 엄격한 규정 준수 요건을 충족할 수 있습니다.

또한 이 공동 책임을 통해 고객은 업종별 인증 요건을 충족하는 솔루션을 배포할 수 있는 유연성과 제어 능력을 보유할 수 있습니다.



이 공동 책임 모델은 IT 제어까지도 확대 적용됩니다. AWS와 해당 고객 간에 IT 환경 운영 책임을 공유하는 것과 마찬가지로 IT 제어의 관리, 운영 및 확인도 공동 책임입니다. AWS는 AWS 환경에 배포된 물리적 인프라와 관련된 제어 항목을 관리하여 고객을 지원할 수 있습니다. 고객은 제공되는 AWS 제어 및 규정 준수 설명서를 사용하여 필요에 따라 제어 평가 및 확인 절차를 수행할 수 있습니다. AWS와

고객 간에 특정 제어에 대한 책임이 어떻게 공유되는지에 대한 예는 AWS 공동 책임 모델을 참조하십시오.

AWS 제어 평가 및 통합

AWS는 기술 백서, 보고서, 인증 및 기타 외부 기관 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 제어가 효과적으로 작동하고 있는지를 설명하고 검증하는 데에도 도움이 됩니다.

전통적으로 내부 및/또는 외부 감사자는 프로세스 안내 및 증거 평가를 통해 제어의 설계 및 운영 효율성을 검증합니다. 고객 또는 고객 측 외부 감사자에 의한 이러한 유형의 직접 관찰 및 검증은 일반적으로 기존 온프레미스 배포에서 제어를 검증하기 위해 수행되었습니다.

서비스 공급자(예: AWS)를 사용하는 경우 고객은 외부 기관 증명 및 인증을 요청하고 평가할 수 있습니다. 이러한 증명 및 인증은 자격을 갖춘 외부 독립 기관이 검증한 제어 목표 및 제어 기능의 설계 및 운영 효과를 고객에게 보장하는 데 도움이 될 수 있습니다. 따라서, 일부 제어 항목은 AWS에서 관리할 수 있지만 제어 환경은 고객이 제어가 효과적으로 작동하고 규정 준수 검토 프로세스를 촉진하는지 설명하고 검증할 수 있는 통합 프레임워크가 될 수 있습니다.

AWS의 외부 기관 증명 및 인증은 고객에게 제어 환경에 대한 가시성과 독립적인 검증을 제공합니다. 이러한 증명 및 인증은 고객이 AWS 클라우드의 IT 환경에 대해 특정 검증 작업을 직접 수행해야 하는 요구 사항을 완화할 수 있습니다.

AWS 위험 및 규정 준수 프로그램

AWS는 조직 전체에서 위험 및 규정 준수 프로그램을 통합했습니다. 이 프로그램은 서비스 설계 및 배포의 모든 단계에서 위험을 관리하고 조직의 위험 관련 활동을 지속적으로 개선 및 재평가하는 것을 목표로 합니다. AWS 통합 위험 및 규정 준수 프로그램의 구성 요소는 다음 섹션에서 자세히 설명합니다.

AWS 비즈니스 위험 관리

AWS는 AWS 사업부와 협력하여 AWS 이사회 및 AWS 고위 경영진에게 AWS 전반의 주요 위험에 대한 종합적 관점을 제공하는 비즈니스 위험 관리(BRM) 프로그램을 운영하고 있습니다. BRM 프로그램은 AWS 기능에 대한 독립적인 위험 감독입니다. 특히 BRM 프로그램은 다음 기능을 수행합니다.

- 주요 AWS 기능 영역에 대한 위험 평가 및 위험 모니터링을 수행
- 위험 식별 및 해결 추진
- 알려진 위험의 목록을 유지 관리

위험을 해결하기 위해 BRM 프로그램은 노력의 결과를 보고하고 필요한 경우 비즈니스 전반의 이사 및 부사장에게 에스컬레이션하여 비즈니스 의사 결정을 위한 정보를 제공합니다.

운영 및 비즈니스 관리

AWS는 주별, 월별, 분기별 회의 및 보고서를 조합하여 위험 관리 프로세스의 모든 구성 요소에 걸쳐 위험이 전달될 수 있도록 합니다. 또한 AWS는 에스컬레이션 프로세스를 구현하여 조직 전체에서 우선순위가 높은 위험에 대한 관리 가시성을 제공합니다. 이러한 노력을 종합하면 AWS 비즈니스 모델의 복잡성과 일관되게 위험을 관리할 수 있습니다.

또한 계단식 책임 구조를 통해 부사장(비즈니스 소유자)이 비즈니스 감독을 담당합니다. 이를 위해 AWS는 매주 회의를 개최하여 운영 지표를 검토하고 주요 추세 및 위험을 비즈니스에 영향을 미치기 전에 식별합니다.

경영진 및 선임 책임자는 AWS의 분위기 및 핵심 가치를 형성하는 데 있어서 중요한 역할을 합니다. 모든 직원은 회사의 기업 행동 및 윤리 강령을 제공받고 정기적으로 교육을 수료합니다. 준수성 감사는 직원들이 확립된 정책을 이해하고 따르도록 하기 위해 수행됩니다.

AWS 조직 구조는 비즈니스 운영을 계획, 실행 및 규제할 수 있는 프레임워크를 제공합니다. 조직 구조에는 적절한 인력 구성, 운영 효율성 및 업무 분담을 위해 역할과 책임이 포함됩니다. 또한 경영진에서는 주요 관계자를 위해 적절한 보고 라인을 구축했습니다. 기업의 고용 확인 프로세스에는 직원을 위한

법률 및 규정에서 허용하는 범위 내에서 직원의 직위와 AWS 시설에 대한 접근 권한에 상응하는 교육, 이전 채용 기록, 경우에 따라 배경 조회가 포함됩니다. 기업은 체계적인 온보딩 프로세스에 따라 직원이 Amazon 도구, 프로세스, 시스템, 정책 및 절차를 익힐 수 있도록 돕습니다.

제어 환경 및 자동화

AWS는 조직 전체의 위험을 관리하기 위한 기본 요소로 보안 제어를 구현합니다. AWS 제어 환경은 AWS 전반에 걸쳐 최소한의 보안 요구 사항을 구현하기 위한 기반을 제공하는 표준, 프로세스 및 구조로 구성됩니다.

AWS 제어 환경의 일부로 포함된 프로세스 및 표준은 자체적으로 적용되지만 AWS는 Amazon의 전체 제어 환경의 일부 측면도 활용합니다. 다음과 같은 도구가 활용됩니다.

- 모든 Amazon 비즈니스에서 사용되는 도구(예: 업무 분리를 관리하는 도구)
- 법률, 인사 관리, 재무와 같은 특정 Amazon 전체 비즈니스 기능

AWS가 Amazon의 전체 제어 환경을 활용하는 경우 이러한 메커니즘을 관리하는 표준 및 프로세스는 AWS 비즈니스에 맞게 조정됩니다. 따라서 AWS 제어 환경 내에서의 사용 및 적용에 대한 기대치는 전체 Amazon 환경에서의 사용 및 적용에 대한 기대치와 다를 수 있습니다. AWS 제어 환경은 궁극적으로 AWS 서비스 제품을 안전하게 제공하기 위한 토대의 역할을 합니다.

제어 자동화는 AWS가 AWS 제어 환경을 구성하는 일부 반복 프로세스에서 인적 개입을 줄이기 위한 방법입니다. 이는 효과적인 정보 보안 제어 구현 및 관련 위험 관리의 핵심입니다. 제어 자동화는 반복 프로세스를 수행하는 작업자의 결함 특성으로 인해 발생할 수 있는 프로세스 실행의 불일치 가능성을 사전에 최소화하려고 합니다. 제어 자동화를 통해 잠재적인 프로세스 편차가 제거됩니다. 이렇게 하면 제어가 설계된 대로 적용될 것이라는 보장이 높아집니다.

AWS의 보안 부서 전반에서 엔지니어링 팀은 가능한 한 높은 수준의 제어 자동화를 지원하도록 AWS 제어 환경을 엔지니어링할 책임이 있습니다. AWS에서 자동 제어의 예는 다음과 같습니다.

- 거버넌스 및 감독: 정책 버전 관리 및 승인
- 인사 관리: 자동화된 교육 제공, 신속한 직원 퇴사 처리
- 개발 및 구성 관리: 코드 배포 파이프라인, 코드 검사, 코드 백업, 통합 배포 테스트
- 자격 증명 및 액세스 관리: 자동화된 업무 분리, 액세스 검토, 권한 관리
- 모니터링 및 로깅: 자동화된 로그 수집 및 상관 관계 분석, 경보
- 물리적 보안: AWS 데이터 센터와 관련된 자동화된 프로세스(하드웨어 관리, 데이터 센터 보안 교육, 접근 경보, 물리적 접근 관리 등)

- 검사 및 패치 관리: 자동화된 취약성 검사, 패치 관리 및 배포

제어 평가 및 지속적 모니터링

AWS는 AWS 환경 내에서 위험을 더욱 줄이기 위해 서비스 배포 전후에 다양한 활동을 구현합니다. 이러한 활동은 각 AWS 서비스의 설계 및 개발 과정에서 보안 및 규정 준수 요구 사항을 통합한 다음 서비스가 프로덕션으로 이동(출시)된 후 안전하게 작동하는지 확인합니다.

위험 관리 및 규정 준수 활동에는 두 가지 출시 전 활동과 두 가지 출시 후 활동이 포함됩니다. 출시 전 활동은 다음과 같습니다.

- AWS 애플리케이션 보안 위험 관리 검토를 통해 보안 위험이 식별되고 완화되었는지 검증
- 아키텍처 준비 상태 검토를 통해 고객이 규정 준수 체제를 준수할 수 있도록 지원

배포 시점에서 서비스는 AWS의 높은 보안 기준을 충족하기 위해 세부 보안 요구 사항에 대한 엄격한 평가를 거친 상태입니다. 출시 후 활동은 다음과 같습니다.

- AWS 애플리케이션 보안의 지속적인 검토를 통해 서비스 보안 태세를 유지할 수 있도록 지원
- 지속적인 취약성 관리 검사

이러한 제어 평가 및 지속적 모니터링을 통해 규제 대상 고객은 AWS 서비스에서 규정 준수 솔루션을 자신 있게 구축할 수 있습니다. 다양한 규정 준수 프로그램 범위에 속하는 서비스의 목록은 AWS 범위 내 서비스 웹 페이지를 참조하십시오.

AWS 자격증, 프로그램, 보고서 및 외부 기관 증명

AWS는 제어 활동이 의도한 대로 운영되고 있음을 증명하기 위해 정기적으로 외부 독립 기관에 의한 감사를 거칩니다. 구체적으로 말하면, AWS는 지역 및 산업에 의존하는 다양한 글로벌 및 지역 보안 프레임워크에 대해 감사를 받습니다. AWS는 50개 이상의 다양한 감사 프로그램에 참여하고 있습니다.

이러한 감사 결과는 평가 기관에서 문서화하며 AWS Artifact를 통해 모든 AWS 고객에게 제공됩니다. AWS Artifact는 AWS 규정 준수 보고서에 온디맨드로 액세스할 수 있는 무료 셀프 서비스 포털입니다. 새 보고서가 릴리스되면 AWS Artifact에서 사용할 수 있으므로 고객은 새로운 보고서에 즉시 액세스하여 AWS의 보안 및 규정 준수를 지속적으로 모니터링할 수 있습니다.

국가 또는 업계의 현지 규제 또는 계약 요구 사항에 따라 AWS는 고객 또는 정부 감사자에게 직접 감사를 받을 수도 있습니다. 이러한 감사는 AWS 제어 환경에 대한 추가 감독을 제공하여 고객이 AWS 서비

스를 사용하여 자신 있고 규정을 준수하며 위험 기반 방식으로 운영할 수 있는 도구를 확보할 수 있도록 합니다.

AWS 자격증 프로그램, 보고서 및 외부 기관 증명에 대한 자세한 내용은 AWS 규정 준수 프로그램 웹 페이지를 참조하십시오. 또한 AWS 범위 내 서비스 웹 페이지를 방문하여 서비스별 정보를 확인할 수 있습니다.

Cloud Security Alliance

AWS는 자발적 Cloud Security Alliance(CSA) Security, Trust and Assurance Registry(STAR) 자체 평가에 참여하여 CSA에서 게시한 모범 사례를 준수함을 문서화했습니다. CSA는 '안전한 클라우드 컴퓨팅 환경을 보장하기 위해 모범 사례를 정의하고 인식을 제고하는 데 전념하는 세계 최고의 조직'입니다. CSA 공동 평가 이니셔티브 질문서(CAIQ)는 CSA에서 클라우드 소비자 및/또는 클라우드 감사자가 클라우드 공급자에게 질문할 것이라고 예상하는 질문 세트를 제공합니다. 이 질문서는 클라우드 공급자 선정 및 보안 평가 등 다양한 활동에 사용할 수 있는 일련의 보안, 제어 및 프로세스 질문을 제공합니다.

고객이 AWS의 CSA CAIQ 준수를 문서화하는 데 사용할 수 있는 리소스에는 두 가지가 있습니다. 첫 번째는 CSA CAIQ 백서이고, 두 번째는 AWS Artifact를 통해 사용할 수 있는 SOC-2 제어에 대한 보다 자세한 제어 매핑입니다. AWS의 CSA CAIQ 참여에 대한 자세한 내용은 AWS CSA 사이트를 참조하십시오.

고객 클라우드 규정 준수 거버넌스

AWS 고객은 IT 배포 방법 또는 장소에 관계없이 전체 IT 제어 환경에 대해 적절한 거버넌스를 유지할 책임이 있습니다. 주요 관행에는 다음이 포함됩니다.

- 필요한 규정 준수 목표 및 요구 사항의 이해(관련 소스를 통해)
- 이러한 목표와 요구 사항을 충족하는 제어 환경 구축
- 조직의 위험 허용치에 따라 필요한 검증 이해
- 제어 환경의 운영 효과 확인

AWS 클라우드 기반 배포를 통해 대기업에게 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. AWS 공동 책임 모델, AWS 보안 설명서, AWS 규정 준수 보고서 및 AWS에서 제공하는 기타 정보를 다른 고객별 문서와 함께 검토합니다. 전체 IT 환경을 최대한 파악한 다음 모든 규정 준수 요구 사항을 포괄적인 클라우드 제어 프레임워크에 문서화합니다.
2. AWS 공동 책임 모델에 명시된 대로 엔터프라이즈 규정 준수 요구 사항을 충족하기 위한 제어 목표를 설계하고 구현합니다.
3. 외부 당사자가 소유한 제어 항목을 식별하고 문서화합니다.
4. 모든 제어 목표가 충족되었으며 모든 주요 컨트롤이 효과적으로 설계 및 운영되고 있는지 확인합니다.

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

결론

AWS의 최우선 과제는 고객에게 매우 안전하고 복원력이 뛰어난 인프라 및 서비스를 제공하는 것입니다. 고객에 대한 AWS의 약속은 지속적으로 고객의 신뢰를 얻고 고객이 AWS에서 워크로드를 안전하게 운영할 수 있다는 확신을 유지할 수 있도록 노력하는 데 중점을 두고 있습니다. 이를 위해 AWS는 다음을 포함하는 위험 및 규정 준수 메커니즘을 통합했습니다.

- 다양한 보안 제어 및 자동화된 도구의 구현
- AWS 운영 효과 및 규정 준수 체제의 엄격한 준수를 보장하는 데 도움이 되는 보안 제어에 대한 지속적인 모니터링 및 평가
- AWS 비즈니스 위험 관리 프로그램에 의한 독립적인 위험 평가
- 운영 및 비즈니스 관리 메커니즘

또한 AWS는 제어 활동이 의도한 대로 운영되고 있음을 증명하기 위해 정기적으로 외부 독립 기관에 의한 감사를 거칩니다. 이러한 감사는 AWS가 획득한 많은 인증과 함께 고객에게 도움이 되는 AWS 제어 환경에 대한 추가 수준의 검증을 제공합니다.

고객이 관리하는 보안 제어와 함께 이러한 노력을 통해 AWS는 고객을 대신하여 안전하게 혁신하고 AWS에서 구축하는 고객이 보안 태세를 개선할 수 있도록 지원할 수 있습니다.

기여자

이 문서를 작성하는 데 도움을 주신 분들입니다.

- Marta Taggart, 선임 프로그램 관리자, AWS Security
- Bradley Roach, 위험 관리자, AWS Business Risk Management
- Patrick Woods, 선임 보안 전문가, AWS Security

추가 자료

AWS는 다음을 통해 고객에게 보안 및 제어 환경에 관한 정보를 제공합니다.

- AWS 규정 준수 프로그램 페이지에 나열된 업계 인증 및 외부 독립 기관 증명을 획득하고 유지 관리합니다.
- AWS 보안 블로그와 같은 백서 및 웹 콘텐츠에 AWS 보안 및 제어 사례에 대한 정보를 지속적으로 게시합니다.
- AWS Builders Library에서 AWS가 대규모 자동화를 활용하여 서비스 인프라를 관리하는 방법에 대한 상세한 설명을 제공합니다.
- AWS Artifact라는 셀프 서비스 포털을 통해 규정 준수 인증서, 보고서 및 기타 문서를 AWS 고객에게 직접 제공하여 투명성을 향상합니다.
- AWS 규정 준수 리소스를 제공하고 AWS 규정 준수 FAQ 웹 페이지에서 쿼리에 대한 답변을 일관되게 문서화 및 게시합니다.
- 고객은 AWS Well-Architected Framework의 설계 원칙에 따라 AWS에서 구축한 워크로드의 핵심 구성에 접근하는 방법에 대한 지침을 얻을 수 있습니다.

문서 수정

이 백서의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

업데이트 기록-변경	update-history-description	update-history-date
마이너 업데이트	기술적 정확성 검토됨	2021년 3월 10일
백서 업데이트됨	이 버전에는 규정 준수 프로그램 및 제도에 대한 참조 정보를 제거하는 등 상당한 변경 내용이 포함되어 있습니다. 이 정보는 AWS 규정 준수 프로그램 및 규정 준수 프로그램 제공 AWS 범위 내 서비스 웹 페이지에서 확인할 수 있기 때문입니다. 또한 일반적인 규정 준수 질문에 대한 내용은 이제 AWS 규정 준수 FAQ 웹 페이지에서 확인할 수 있으므로 해당 섹션을 삭제했습니다.	2020년 11월 1일
최초 게시	Amazon Web Services: 위험 및 규정 준수 백서 게시됨	2011년 5월 1일

고지 사항

고객은 본 문서에 포함된 정보를 독자적으로 평가할 책임이 있습니다. 본 문서는 (a) 정보 제공만을 위한 것이며, (b) 사전 고지 없이 변경될 수 있는 현재의 AWS 제품 제공 서비스 및 사례를 보여 주며, (c) AWS 및 자회사, 공급업체 또는 라이선스 제공자로부터 어떠한 약정 또는 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 '있는 그대로' 제공됩니다. 고객에 대한 AWS의 책임과 법적 책임은 AWS 계약서에 준하며 본 문서는 AWS와 고객 간의 계약에 포함되지 않고 계약을 변경하지도 않습니다.