AWS 위험 및 규정 준수 개요

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

이 문서에는 AWS 제어를 평가하는 기본 방식이 포함되어 있으며 고객이 AWS를 기존 제어 프레임워크에 통합할 수 있도록 지원하는 정보가 담겨 있습니다.

서론

AWS와 고객은 IT 환경을 함께 제어합니다. 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 규정 준수에 대한 자세한 내용은 AWS 규정 준수 페이지를 참조하십시오.

또한 AWS 보안 프로세스 개요 백서에서는 AWS의 일반적인 보안 제어 및 서비스별 보안을 다룹니다.

공동 책임 환경

IT 인프라를 AWS 서비스로 이전할 경우 고객과 AWS 간에 공동 책임 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 공동 책임를 통해 고객은 업종별 인증 요건을 충족하는 솔루션을 배포할 수 있는 유연성과 규제 능력을 보유할 수 있습니다.

이 고객/AWS 공동 책임 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(AWS 인증 및 외부 기관 검증에 설명)를 참조하여 필요한 제어 평가 및 검증 절차를 실시할 수 있습니다.

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.

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. AWS는 FISMA Moderate 표준과 PCI 데이터 보안 표준을 준수합니다. 이러한 PCI 및 FISMA 표준은 상당한 권위가 있으며 AWS가 게재된 표준을 준수하는지 독립적으로 검증합니다.

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 제어 및 보안 프로세스의 포괄적 특성에 대한 깊이 있는 정보를 제공합니다.

AWS 글로벌 리전

데이터 센터는 전 세계 여러 리전에 클러스터 형태로 구축되며, 여기에는 미국 동부(버지니아 북부), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), AWS GovCloud(미국, 오레곤), EU(프랑크푸르트), EU(아일랜드), 아시아 태평양(서울), 아시아 태평양(싱가포르), 아시아 태평양(도쿄), 아시아 태평양(시드니), 중국(베이징), 남아메리카(상파울루) 등 11개 리전이 있습니다.

전체 리전 목록을 확인하려면 AWS Global Infrastructure 페이지를 방문하십시오.

AWS 위험 및 규정 준수 프로그램

AWS는 고객이 거버넌스 프레임워크에 AWS 컨트롤을 통합할 수 있도록 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 AWS가 고객 데이터를 안전하게 보호하는 방법을 설명한 보안 백서를 게시합니다.

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, mailto:awscompliance@amazon.com으로 직접 문의해 주십시오.

참고 문헌

추가 정보는 다음 출처를 참조하십시오.

- CSA 공동 평가 질문서
- AWS 인증, 프로그램, 보고서 및 제3자 증명
- 규정 준수 관련 주요 질문에 대한 AWS의 답변

문서 수정

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