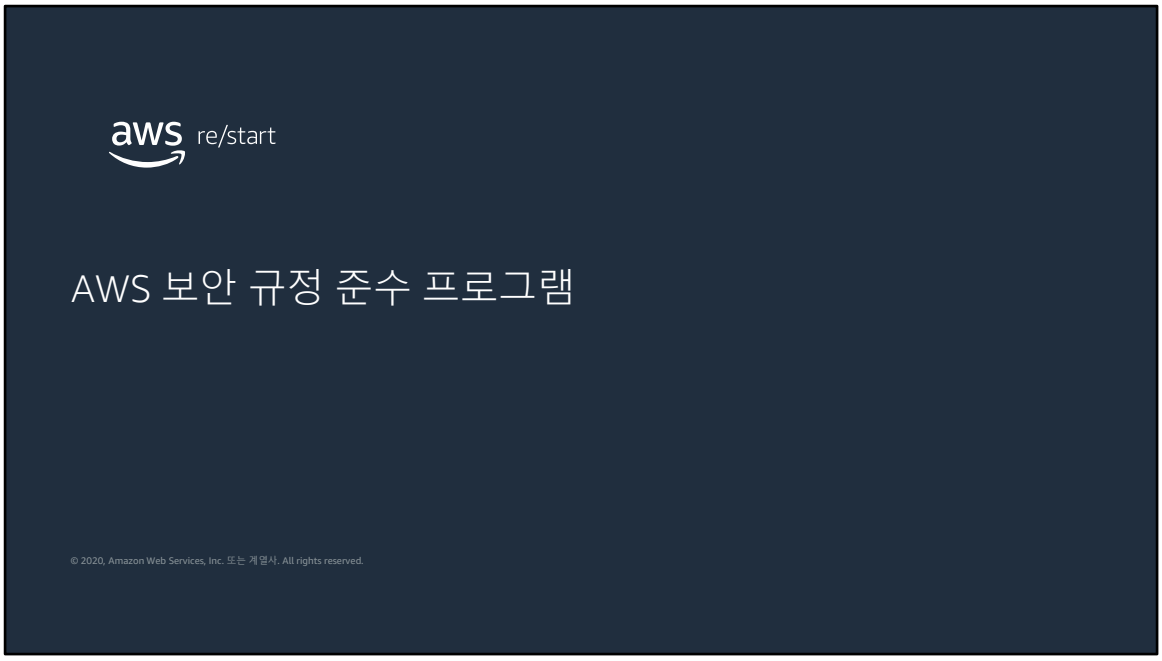

AWS 보안 규정 준수 프로그램을 시작하겠습니다.

교육 내용

이 강의의 핵심

배울 내용은 다음과 같습니다.

- AWS 보안 규정 준수 프로그램을 설명합니다.
- AWS 위험 및 규정 준수 프로그램의 세 가지 구성 요소를 알아봅니다.

aws re/start

이 강의에서는 다음 주제를 다룹니다.

- 보증 프로그램을 비롯하여 AWS의 규정 준수 접근 방식
- AWS 위험 및 규정 준수 프로그램(예: 위험 관리, 제어 환경 및 정보 보안)
- AWS 고객 규정 준수 책임

AWS 규정 준수 접근 방식

AWS의 책임

- 매우 안전하고 제어된 환경을 제공합니다.
- 다양한 보안 기능을 제공합니다.

고객의 책임:

- IT를 구성합니다.

보안을 위한 공동 책임 모델에 설명된 것처럼 AWS와 고객은 IT 환경에 대한 제어를 공유합니다. 즉, 양측이 모두 IT 환경을 관리하는 데 책임이 있습니다. 이 모델에서 AWS의 책임은 매우 안전하고 제어된 환경에서 서비스를 제공하고 고객이 사용할 수 있는 다양한 보안 기능을 제공하는 것입니다.

고객의 책임에는 목적에 따라 안전하고 제어된 방식으로 IT 환경을 구성하는 것이 포함됩니다.

AWS 보안 정보

AWS가 보안 정보를 공유하는 방식

- 산업 인증을 획득합니다.
- 보안 및 제어 사례를 게시합니다.
- 비밀 유지 계약(NDA)을 통해 직접 문서를 제공합니다.

AWS는 관련 보안 및 제어 환경에 대한 정보를 고객에게 전달합니다. AWS가 보안 정보를 공유하는 방법은 다음과 같습니다.

- 산업 인증을 비롯해 제3자의 독립적인 증명 획득
- 기술 문서와 웹 사이트 콘텐츠를 통해 AWS 보안 및 제어 관행에 대한 정보 공개
- 필요에 따라 비밀 유지 계약(NDA) 체결 후 AWS 고객에게 인증서, 보고서 및 기타 문서 직접 제공

AWS 보증 프로그램

AWS, 인증 기관 및 독립 감사자는 다음을 제공합니다.

- 인증 및 증명
- 법률, 규정 및 개인 정보 보호
- 산업 규정 준수 및 거버넌스 프레임워크

AWS는 인증 기관 및 독립 감사자와 협력하여 AWS에서 수립하고 운영하는 정책, 프로세스 및 제어 조치에 관한 정보를 고객에게 제공합니다.

- **인증 및 증명** - 독립적인 제3자 감사자가 평가한 규정 준수 인증 및 증명. 인증서, 감사 보고서, 규정 준수 증명으로 나타납니다.

- **법률, 규정, 개인 정보 보호 -** 관련 규정 준수 법률 및 규제를 준수할 책임은 AWS 고객에게 있습니다. 경우에 따라 AWS는 고객의 규정 준수를 지원하는 기능을 제공합니다. 이런 기능에는 보안 기능, 지원, 법률 계약(AWS 데이터 처리 계약 및 비즈니스 제휴 계약 등)이 있습니다.

- **산업 규정 준수 및 프레임워크** - 규정 준수 편성 및 프레임워크에는 특정 업계나 기능과 같은 특정 목적으로 게시된 보안 또는 규정 준수 요건이 포함됩니다. AWS는 이러한 유형의 프로그램에 맞는 기능(보안 기능 등)과 규정 준수 플레이북, 매핑 문서, 기술 문서를 제공합니다.

AWS 위험 및 규정 준수 프로그램

AWS 위험 및 규정 준수 프로그램

- AWS 제어 조치에 대한 정보 제공
- 고객의 프레임워크 문서화 지원

AWS 위험 및 규정 준수의 구성 요소

- 비즈니스 위험 관리
- 제어 환경과 자동화
- 정보 보안(IS)

AWS는 고객이 거버넌스 프레임워크에 AWS 제어 조치를 통합할 수 있도록 위험 및 규정 준수 프로그램에 대한 정보를 제공합니다. 이 정보는 고객이 프레임워크의 중요한 부분으로 AWS가 포함된 완전한 제어 및 거버넌스 프레임워크를 문서화할 수 있도록 지원합니다.

AWS 위험 및 규정 준수 프로그램은 세 가지 요소로 구성됩니다.

- 비즈니스 위험 관리
- 제어 환경과 자동화
- 정보 보안

다음 주제에서는 AWS 위험 및 규정 준수 프로그램을 더 자세히 살펴보겠습니다
.

AWS 위험 관리

비즈니스 계획 및 책임

비즈니스 계획

- 위험 관리를 포함합니다.
- 최소한 1년에 두 번 이상 계획을 재평가합니다.

고객의 책임

- 위험을 식별합니다.
- 위험을 해결하기 위한 적절한 조치를 구현합니다.
- 다양한 내부 또는 외부 위험을 평가합니다.

정보 보안 프레임워크 및 정책

- Control Objectives for Information and related Technology(COBIT)
- American Institute of Certified Public Accountants(AICPA)
- National Institute of Standards and Technology(NIST)

AWS 관리 팀은 위험 식별과 위험을 완화 또는 관리할 수 있는 제어 조치 구현을 포함하는 전략적 비즈니스 계획을 개발합니다. 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 팀은 다음 관리 기관을 기반으로 하는 정보 보안 프레임워크 및 정책을 수립합니다.

- Control Objectives for Information and related Technology(COBIT)
- American Institute of Certified Public Accountants(AICPA)
- National Institute of Standards and Technology(NIST)

AWS 위험 관리(계속)

AWS의 책임
- 보안 정책을 유지 관리합니다.
- 직원에게 보안 교육을 제공합니다.
- 애플리케이션 보안 검토를 수행합니다.
  - 데이터 기밀성, 무결성, 가용성
  - IS 정책 준수 여부

AWS 보안
- 서비스 엔드포인트에서 취약성을 스캔합니다.
- 취약성 해결 알림을 보냅니다.

독립적인 보안 회사
- 스캔은 **고객** 스캔을 대체하는 것이 아닙니다.
- 고객은 클라우드 인프라 스캔을 요청할 수 있습니다.

AWS는 보안 정책을 유지 관리하고, AWS 직원에게 보안 교육을 제공하며, 애플리케이션 보안 검토를 수행합니다. 이러한 검토는 정보 보안(IS) 정책 준수 여부뿐만 아니라 데이터의 기밀성, 무결성 및 가용성도 평가합니다.

AWS

AWS 보안 팀은 모든 퍼블릭 서비스 엔드포인트 IP 주소를 정기적으로 스캔하여 취약성이 있는지 확인합니다. 그러나 고객의 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 인터페이스에서는 스캔을 수행하지 않습니다. AWS 보안 팀은 확인된 취약성을 해결하기 위해 관련 당사자에게 취약성을 알립니다.

독립적인 보안 회사

또한 독립적인 보안 회사에서 정기적으로 외부 취약성 위협 평가를 수행합니다. 이러한 평가 결과 확인된 내용과 권장 사항이 범주화되어 AWS 리더십에 전달됩니다. 이 스캔은 AWS 기본 인프라의 상태와 실행 가능성을 검증하기 위해 수행됩니다. 고객이 특정 규정 준수 요구 사항을 충족하기 위해 수행해야 하는 자체 취약성 스캔을 대체하기 위한 것이 아닙니다. 고객은 스캔이 고객의 인스턴스에 국한되고 AWS의 이용 목적 제한 정책을 위반하지 않는 범위에서 클라우드 인프라 스캔을 수행할 수 있는 권한을 요청할 수 있습니다.

AWS 제어 환경

제어 환경

- 정책, 프로세스 및 제어 활동을 포함합니다.
- AWS 서비스 제품군을 안전하게 제공합니다.

구성 요소

- 인력
- 프로세스
- 기술

기능

- AWS 제어 프레임워크의 운영 효율성을 지원합니다.
- 업계 최고의 클라우드 기관에서 인정한 제어 조치를 통합합니다.
- 제어 환경을 관리하기 위해 주요 사례 아이디어를 모니터링합니다.

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 인력과 프로세스, 그리고 기술을 포함합니다.

AWS는 선도적인 클라우드 컴퓨팅 산업 기관에서 인정한 적용 가능한 클라우드 관련 제어 조치를 AWS 제어 프레임워크에 통합합니다. AWS는 계속해서 이 산업군을 모니터링하며 구현할 만한 선도적인 사례가 있는지 아이디어를 찾습니다. AWS는 이러한 산업군을 모니터링하여 고객의 제어 환경 관리를 지원합니다.

정보 보안

AWS 정보 보안 프로그램

- 다음을 보호합니다.
  - 기밀성
  - 무결성
  - 가용성
- 보안 기술 문서를 발행합니다.

AWS는 고객 시스템 및 데이터의 기밀성, 무결성, 가용성을 보호하도록 고안된 공식적인 정보 보안 프로그램을 가지고 있습니다.

AWS는 고객의 데이터 보호를 지원하는 방법을 다루는 보안 기술 문서를 발행합니다.

자세한 내용은 AWS 클라우드 보안 웹 사이트의 AWS 규정 준수를 참조하십시오.

고객 규정 준수 요구 사항

- 전체 IT 제어 환경에 대한 거버넌스를 유지 관리합니다.
- 다음을 이해합니다.
  - 필수 규정 준수 목표
  - 검증 기반 위험 허용 수준
- 목표를 충족하는 제어 환경을 구축합니다.
- 제어 환경의 효율성을 확인합니다.
- 규정 준수를 위해 기본적인 접근법을 사용합니다.
  - 검토
  - 설계
  - 식별
  - 확인

AWS 고객은 IT 배포 방식과 관계없이 전체 IT 제어 환경에 대해 적절한 거버넌스를 유지 관리해야 합니다. 관련 소스로부터 필수 규정 준수 목표와 요구 사항을 파악하고, 그 목표와 요구 사항을 충족하는 제어 환경을 구축하는 것이 가장 중요합니다. 또한 조직의 위험 허용 수준에 따라 필요한 검증을 파악하고 제어 환경의 운영 효과를 확인해야 합니다. AWS 클라우드 기반 배포는 기업에 다양한 제어 유형과 다양한 확인 방법을 적용할 수 있는 여러 옵션을 제공합니다.

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

- AWS 정보와 기타 정보를 함께 검토하여 전체 IT 환경을 최대한 이해합니다. 그런 다음 모든 규정 준수 요구 사항을 문서화합니다.
- 기업의 규정 준수 요구 사항을 충족하는 제어 목표를 수립하고 구현합니다.
- 외부 당사자가 소유한 제어 조치를 식별하고 문서화합니다.
- 모든 제어 목표가 달성되었으며 모든 주요 제어 조치가 효과적으로 설계 및 운영되고 있는지 확인합니다.

고객은 AWS로 규정 준수 및 거버넌스 프로세스를 계속 수행함으로써 규정 준수 요구 사항을 충족할 수 있습니다.

핵심 사항

- AWS 클라우드 규정 준수를 통해 고객은 **클라우드에서 보안 및 데이터 보호 유지 관리**를 위한 AWS의 **강력한 제어 조치를 이해**할 수 있습니다.
- 고객은 **AWS 보안에서 제어하는** 환경에서 작업합니다. 고객 시스템이 AWS 클라우드 인프라를 기반으로 하여 구축되기 때문에 **규정 준수 책임은 AWS와 고객 간에 공유**됩니다.
- AWS는 다양한 보안 표준 및 규정 준수 인증을 지원합니다. 이 표준과 인증은 고객이 **전 세계 거의 모든 규제 기관의 규정 준수 요구 사항을 충족**하는 데 도움이 됩니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- AWS 클라우드 규정 준수를 통해 고객은 클라우드에서 보안 및 데이터 보호 유지 관리를 위한 AWS의 강력한 제어 조치를 이해할 수 있습니다.
- 고객은 AWS 보안에서 제어하는 환경에서 작업합니다. 고객 시스템이 AWS 클라우드 인프라를 기반으로 하여 구축되기 때문에 규정 준수 책임은 AWS와 고객 간에 공유됩니다.
- AWS는 다양한 보안 표준 및 규정 준수 인증을 지원합니다. 이 표준과 인증은 고객이 전 세계 거의 모든 규제 기관의 규정 준수 요구 사항을 충족하는 데 도움이 됩니다.