Coalfire
IT Audit and Compliance

Amazon Web Services에 대한 FFIEC 규정 준수

amazon web services

2015년 3월

목차

요약

본 Federal Financial Institutions Examination Council(FFIEC) 감사 및 규정 준수 워크북은 AWS 서비스의 사용 및 보안 아키텍처에 대해 FFIEC 감사 및 규정 준수 책임이 부과되는 금융 기관 안내를 제공할 목적으로 작성된 것입니다. 본 문서는 AWS 금융 기관 고객, 소속 검사관 및 자문역이 고객 데이터를 위한 금융 기관 환경의 일부로 AWS 서비스를 사용할 때 AWS 서비스 범위, 구현 지침 및 검사를 이해하기 위해 활용할 수 있도록 구성되었습니다.

AWS는 주로 SOC(Service Organization Controls) 보고 표준에 따라 관련 제어에 대해 전 세계적으로 감사를 실시하고 공인회계법인을 통해 인증받고 있습니다. FFIEC를 준수하여 서비스를 사용하려면 특정 구성, 연결 및 아키텍처를 고려해야 합니다. 다음 문서에서는 FFIEC 평가 범위와 관련된 AWS 서비스 공급자 제어에 대해 설명합니다. 또한, AWS의 FFIEC 규정 준수 책임과 금융 기관의 AWS 사용을 예시합니다.

범위 내 서비스 설명

AWS 관리 환경은 서버, 운영 체제, 하이퍼바이저, 그리고 AWS 서비스의 관리 및 운영을 위한 제어 환경을 비롯해 AWS 서비스를 지원하는 물리적 및 논리적 기초 인프라입니다.

FFIEC 제어 검토에 AWS 관리 환경과 다음 서비스가 포함되었습니다.

- Amazon Elastic Compute Cloud(EC2)
- Amazon Virtual Private Cloud(VPC)
- Amazon Elastic Block Storage(EBS)
- Amazon Simple Storage Service(S3)
- Amazon Relational Database Service(RDS)
- Amazon ELB(Elastic Load Balancing)
- Amazon Identity and Access Management(IAM)

각 서비스에 대한 보다 자세한 설명은 AWS 제품 웹사이트 단원을 참조하십시오.

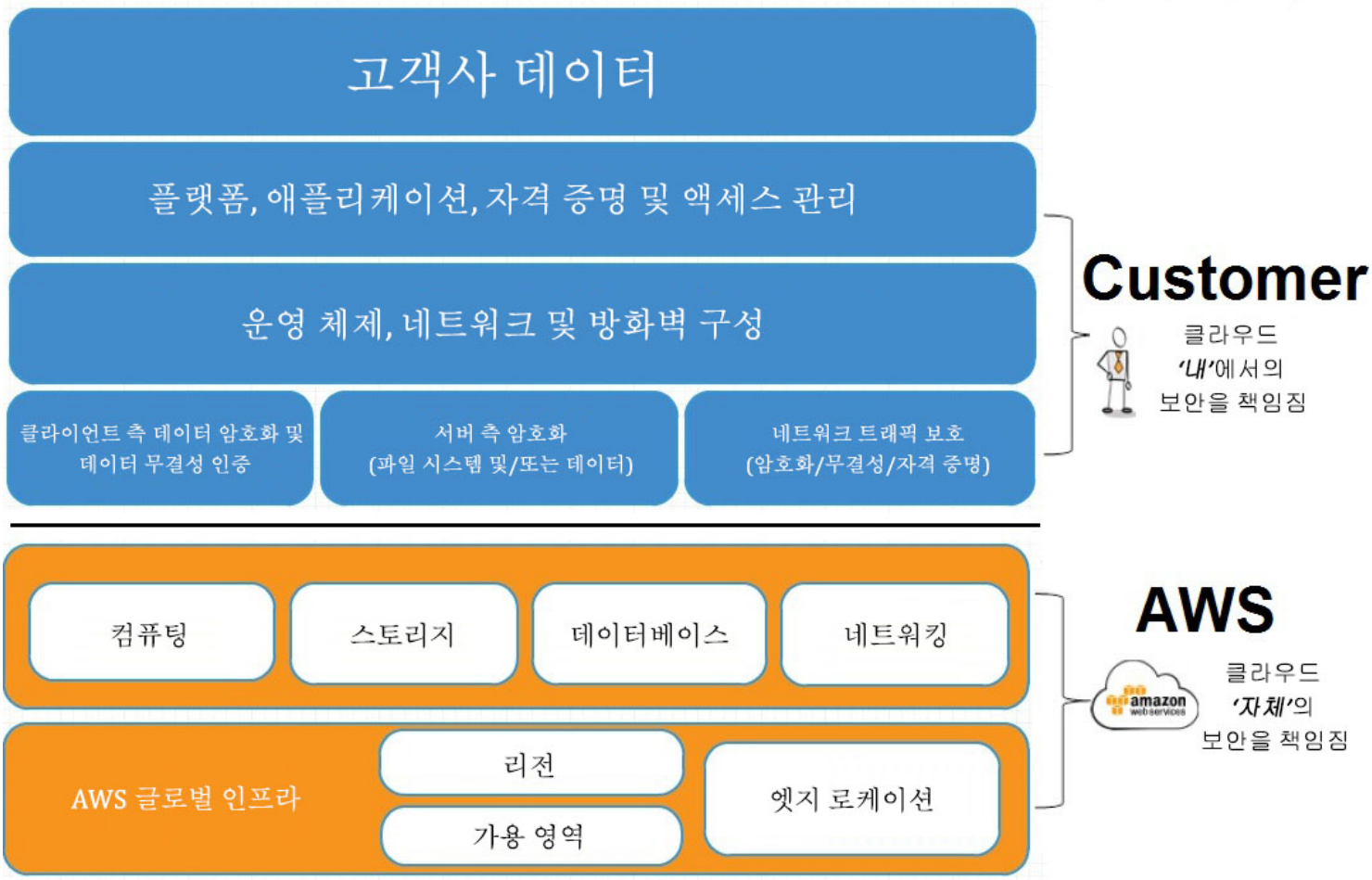
AWS 책임 분담 모델

보안 환경을 구현하기 위해 AWS는 보안 제어의 운영 및 관리에 책임 분담 모델을 활용하고 있습니다. 이 분담 모델은 AWS 및 클라이언트 모두 정보 보안 제어의 자체 구성 요소를 운영하고 관리하므로 운영 부담을 완화하는 데 도움이 됩니다. AWS는 클라우드 자플랫폼 자체의 보안을 제공하고, 이를 사용하는 고객은 클라우드 ***상에서*** 운영되는 업무환경의 보안을 개발 및 유지할 책임을 부담합니다.

"클라우드 보안"은 AWS가 클라우드 인프라 내에서 구현하는 규정 준수 프로그램 및 조치를 의미합니다. AWS는 호스트 운영 체제 및 가상화 계층에서부터 AWS 서비스가 운영되는 시설의 물리적 보안에 이르기까지 광범위한 구성 요소를 운영, 관리 및 제어합니다. **"***클라우드* **내** 보안"은 고객이 AWS 인프라 내에서 자사의 워크로드와 관련된 보안 제어를 구현하는 것을 말합니다.

AWS에 대한 공통되는 질문 하나는 ***"어떻게 AWS 활용이 보안 및 규정 준수 활동을 간소화하는가?" 입니다.***
이 질문은 AWS 클라우드를 두 가지 방식으로 접근함으로써 충족되는 제어를 예시하는 방법으로 답변할 수 있을 것입니다. 첫째, AWS 인프라의 규정 준수에 대한 검토는 "클라우드 규정 준수"라는 개념을 도출합니다. 둘째, AWS 인프라에서 실행되는 워크로드에 대한 고객의 규정 준수 표준 검토는 "클라우드 ***내*** 규정 준수"라는 개념을 도출합니다.

다음 예시는 클라우드 *내* 책임과 클라우드 책임을 잘 보여줍니다.



클라우드 규정 준수

클라우드 규정 준수는 AWS가 클라우드 기초 인프라의 보안을 관리하는 방식을 가리킵니다.

어떻게 조직이 AWS 제어 환경 내에서 운영 시 보안 제어를 검증할 수 있는가?
AWS 인증 및 보고서가 AWS에 독립적인 감사자를 통해 작성되고 AWS 환경의 설계 및 운영 효율성을 인증합니다. 이 인증 및 보고서에는 다음 항목이 포함됩니다.

i. **SOC 1/ ISAE 3402:** AWS는 SOC 1(Service Organization Controls 1), Type II 보고서를 발행합니다. 이 감사는 SAS 70(Statement on Auditing Standards No. 70) Type II 보고서를 대체합니다. SOC 1 보고서는 AWS의 제어 목표가 적절하게 설계되어 있고, 고객 데이터를 보호하도록 정의되어 있는 제어 기능들이 효과적으로 작동하고 있다는 점을 증명하고 있습니다.

ii. **SOC 2 - 보안:** AWS는 SOC 1 보고서 외에도 SOC 2(Service Organization Controls 2), Type II 보고서를 발행합니다. 컨트롤 평가 면에서 SOC 1과 유사한 SOC 2 보고서는 미국 공인 회계사 협회(AICPA) 트러스트 서비스 원칙에 규정된 기준으로 컨트롤 평가를 확장하는 인증 보고서입니다. AWS SOC 2는 AICPA의 신뢰 서비스 원칙 기준에 규정된 보안 원칙 기준에 부합하는 제어 기능의 설계 및 운영 효율성 평가입니다. 이 보고서는 정의된 업계 표준을 기반으로 AWS 보안에 추가적인 투명성을 제공하며 더 나아가 고객 데이터 보호에 대한 AWS의 약속을 보여 줍니다.

iii. **SOC 3-보안**: AWS는 SOC 3(Service Organization Controls 3) 보고서를 발표합니다. SOC 3 보고서는 AWS SOC 2 보고서의 공개 요약본으로, AICPA SysTrust 보안 봉인이 되어 있습니다. 이 보고서에는 제어 운영에 대한 외부 감사 기관의 의견(SOC 2 보고서에 포함된 AICPA 보안 신뢰 원칙 기준), 제어 효과에 관한 AWS 경영진의 주장, 그리고 AWS 인프라 및 서비스 개요 정보가 수록되어 있습니다.

iv. **ISO 27001:** AWS는 ISO(국제 표준화 기구) 27001 표준에 따라 ISO 27001 인증을 획득했습니다. ISO 27001은 널리 채택되는 글로벌 보안 표준으로서, 정보 보안 관리 시스템별 요건을 개략적으로 기술합니다. 주기적인 위험 평가에 기반을 둔 회사 및 고객 정보 관리에 대한 체계적 접근 방식을 제공합니다. 기업이 인증을 획득하기 위해서는 기업 및 고객 정보의 기밀성, 무결성, 가용성에 영향을 미치는 정보 보안 위험 관리에 대한 체계적이고 지속적인 접근법을 갖추고 있음을 증명해야만 합니다.

v. **PCI - 보안:** AWS는 신용카드 업계(PCI)의 데이터 보안 표준(DSS)하에서 레벨 1 정책을 준수합니다. 고객은 PCI 정책 준수 기술 인프라에서 애플리케이션을 실행하여 클라우드상의 신용카드 정보를 저장, 처리, 전송할 수 있습니다. 지난 2013년 2월, PCI 보안 표준 위원회에서는 PCI DSS 클라우드 컴퓨팅 가이드라인을 발표했습니다. 이 가이드라인은 카드 소지자 데이터 환경을 관리하는 고객에게 클라우드상의 PCI DSS 규제 항목을 유지하기 위해 고려해야 할 사항을 제공합니다. AWS는 고객을 위해 PCI DSS 클라우드 컴퓨팅 가이드라인을 AWS PCI 규정 준수 패키지에 통합했습니다.

상기한 보고 이외에, AWS 인프라를 활용하여 미국 건강 보험 이전 및 책임법(HIPAA), 연방 위험 및 인증 관리 프로그램(FedRAMP) Moderate 기준 인증, 국방부 정보 보호 인증 및 승인 프로세스(DIACAP), 국제 무기 거래 규정, CSA(Cloud Security Alliance) 및 기타 요건, 표준 및 모범 사례 등 다양한 규정, 표준 및 모범 사례를 충족할 수 있습니다.

AWS 규정 준수 인증 및 보고서 요청
적용 가능한 AWS 규정 준수 인증 및 보고서를 https://aws.amazon.com/compliance/contact에서 요청할 수 있습니다. 자세한 내용은 AWS 보안 센터에서 제공하는 AWS 보안 백서 및 규정 준수 FAQ를 참조하십시오.

AWS 규정 준수 환경을 설명하는 추가 정보 및 리소스
AWS는 규정 준수 백서를 통해 AWS 고객이 AWS를 기존의 제어 프레임워크와 통합하도록 지원하고 조직의 AWS 사용을 설계하고 보안 평가를 실시하는 데 도움이 되는 정보를 제공하고 있습니다.
AWS 규정 준수 인증, 보고서, 모범 사례 준수 및 표준(예: ISO, PCI-DSS 등)에 대한 자세한 내용은 AWS 규정 준수 사이트에서 확인할 수 있습니다.

클라우드 *내* 규정 준수

클라우드 *내* 규정 준수는 고객이 자사 워크로드(가상 프라이빗 클라우드, 보안 그룹, 운영 체제, 데이터베이스, 인증 등)의 보안을 관리하는 방식을 의미합니다. 다음은 그러한 예입니다.

양자 간 서비스 제어 – 고객이 구현할 책임입니다. 고객의 AWS 이용은 보안 태세 및 제어 해석에서 각각 다르지만 양자 간 서비스 제어는 고객의 서비스 이용 안에서 문서화되어야 합니다.

> **예:** 멀티 팩터 인증은 금융 기관에서 액세스 관리, 인증 및 인증 요구 사항을 충족하기 위해 고객 환경 내에서 IAM 사용자 보안을 지원하는 데 사용할 수 있습니다.

서비스 특정 제어 – Amazon Simple Storage Service(S3) 등 고객이 사용하는 서비스에 특정된 제어입니다. 고객은 특정 제어 목표를 달성하기 위해 S3 사용 범위 내에서 서비스 특정 제어를 문서화해야 할 수 있습니다.

> **예:** 서버 측 암호화(SSE)는 [고객] 데이터 분류 정책에 따라 비밀로 분류되는 모든 객체에 대해 활성화됩니다.

최적화 네트워크, 운영 체제(OS) 및 애플리케이션 제어 – 승인된 OS 이미지의 사용과 관련된 특정 제어 요소를 충족하기 위해 문서화해야 할 수 있는 기관 및/또는 공급업체를 제어합니다.

> **예:** 변경 관리 내에서 특정 제어를 충족하기 위한 [고객] 서버 보안 강화 규칙 또는 최적화된 프라이빗 Amazon 머신 이미지(AMI).

리전, 가용 영역 및 엔드포인트

리전, 가용 영역 및 엔드포인트는 AWS 보안 글로벌 인프라의 구성 요소입니다. AWS 리전을 사용하여 네트워크 지연 시간 및 사고 관리 계획(CP) 요구 사항을 관리합니다. 데이터를 특정 리전에 저장하면 해당 리전 밖으로 복제되지 않습니다. 기관에서 필요한 경우 리전 간에 데이터를 복제하는 일은 고객의 책임입니다. AWS는 국가에 대한 정보를 제공하고 필요한 경우 각 리전이 포함된 지방에 대한 정보를 제공합니다. 고객은 자체 네트워크 지연 시간 요구 사항에 따라 데이터를 저장할 리전을 선택할 책임이 있습니다. 리전은 가용성을 염두에 두고 설계되며 최소 2개 이상의 가용 영역으로 구성됩니다.

가용 영역은 결함 격리를 위해 설계되었습니다. 여러 인터넷 서비스 제공업체(ISP)와 다양한 전력망에 연결되어 있습니다. 고속 링크를 사용해 상호 연결되어 있기 때문에 애플리케이션은 LAN(Local Area Network) 연결을 사용하여 같은 리전 내에 있는 가용 영역 간 통신이 가능합니다. 시스템은 여러 가용 영역을 아우를 수 있습니다. 시스템을 설계할 때 재해 발생 시 가용 영역의 임시적 또는 장기적인 장애에도 유지될 수 있도록 설계하는 것이 좋습니다.

본 워크북 사용을 위한 접근 방법

검사관

AWS 서비스를 사용하는 조직을 평가할 때 반드시 고객과 AWS 간 "책임 분담" 모델을 이해해야 합니다. “Amazon Web Services에 대한 FFIEC 평가 지침” 단원에서는 요구 사항이 공통 보안 프로그램 제어 및 제어 영역으로 체계화되어 있습니다. 각 제어는 FFIEC 요구 사항, 검사관 활동, 고객 책임 및 증거, 규정 준수에 관한 AWS 증거를 참조합니다.

일반적으로 AWS 서비스는 전통적으로 고객이 서비스를 구현하기 위해 사용하던 네트워크 인프라 장치 및 서버와 마찬가지로 취급해야 합니다. 장치와 서버에 적용되는 정책 및 프로세스도 AWS 서비스에서 해당 기능을 제공하는 경우 적용해야 합니다. 정책 또는 절차와 관련된 제어는 일반적으로 공유 또는 이중 제어입니다. 고객이 AWS 서비스 사용에 대한 거버넌스를 확장해야 하기 때문입니다. 이와 비슷하게 AWS 콘솔 또는 명령줄 API를 통한 AWS 관리는 기타 권한이 있는 관리자 액세스처럼 다루어야 합니다.

AWS 서비스는 적용되는 표준 및 요구 사항에 대해 정기적으로 평가됩니다. 참조된 증거는 타사 감사자에 의해 검증된 후 적절한 협의하에 고객에게 공개됩니다.

고객

AWS 고객은 AWS를 활용하여 준수 환경을 구현하므로 다음 단원은 추가로 고려할 정보를 제시합니다.

- **인증 및 권한 부여.** AWS 환경에서 고려할 인증 및 권한 부여는 두 계층이 있습니다. IAM 자격 증명 및 AWS 고객 제어 자격 증명.

  IAM은 로컬 IAM 계정을 사용하거나, Active Directory와 같은 AWS 고객의 기업 디렉터리에 액세스 제어를 통합하는 방식으로 AWS 서비스 직접 액세스를 위한 인증 및 권한 부여를 제공합니다. 계정 위치와 무관하게, AWS 고객은 권한 그룹을 생성 및 할당하고 사용자를 추가하고 AWS 고객이 액세스 관리 제어를 준수할 수 있게 해주는 다른 활동을 추가할 수 있습니다.

  운영 체제, 그리고 EC2 또는 VPC 인스턴스에서 실행되는 모든 서비스 또는 애플리케이션의 인증 및 권한 부여는 AWS 고객이 완벽하게 통제합니다. AWS 고객은 자사의 애플리케이션 환경에 적합하게 인증을 설계해야 합니다.

  AWS도 인증을 “연동”하는 옵션을 제공합니다. 인증 연동은 조직의 Active Directory 또는 기타 LDAP 구현을 사용하는 콘솔 및 API를 비롯하여 AWS 관리 환경에 대한 액세스를 허용합니다.

- **게스트 운영 체제:** AWS 고객이 EC2 및 VPC에서 가상 인스턴스를 제어합니다. AWS 고객은 계정, 서비스 및 애플리케이션에 대한 전체 관리 액세스 및 제어 권한을 가집니다.

  - **운영 체제 선택.** AWS가 호스트 운영 체제 배포에 사용할 수 있는 이미지를 제공하지만, AWS 고객 스스로 각자 운영 체제에 적용되는 FFIEC 요구 사항에 부합하도록 시스템 구성 및 강화 표준을 개발하고 구현해야 합니다. AWS 고객은 자체 인스턴스 운영 체제를 소유 및 관리하며, 제공된 이미지는 준수 플랫폼을 대표하는 것이 아닙니다.

- **운영 체제 저장 위치.** AWS가 기본 운영 체제를 저장할 위치 두 군데, 즉 로컬 인스턴스 스토어와 EBS를 제공합니다. 로컬 인스턴스 스토어 사용은 옵션이지만 이는 데이터 이동성과 고객 환경의 유연성을 제한합니다. 또한, 로컬 인스턴스 스토어 데이터가 해당 인스턴스가 삭제된 이후로도 유지되지 않습니다. 해당 인스턴스를 종료하면 인스턴스 데이터를 검색할 수 없습니다. 운영 체제, 또는 운영 체제 상의 다른 온디맨드 데이터를 저장하기 위해 EBS를 사용하는 것은 로컬 인스턴스 스토리지 사용보다 지속 가능한 모델입니다. EBS도 EBS 스냅샷을 통해 S3로 백업하는 기능을 제공합니다.

- **스토리지.** AWS는 AWS 고객의 데이터가 보다 용이하게 애플리케이션을 통해 액세스되도록 하거나 또는 백업에 사용할 수 있게 EBS, S3, RDS 등 다양한 정보 저장 옵션을 제공합니다. 민감한 데이터가 저장된 시스템에 대한 인바운드 및 아웃바운드 액세스를 제한하는 FFIEC 요구 사항을 충족하기 위해서는 기술 및 인터넷을 통한 데이터 접근성 측면에서 민감한 데이터를 저장할 다양한 스토리지 옵션을 평가해야 합니다. 예를 들어, S3는 SSL을 요구하고 사전 정의된 IP 주소에 대한 액세스를 제한하도록 구성함으로써 인터넷을 통한 데이터 접근성을 제한할 수 있습니다. 정보 사용 및 저장이 관련 요구 사항에 부합하도록 각 스토리지 옵션을 고려 및 설계해야 합니다.

- **AWS 보안 게시판.** AWS는 관리하고 있는 플랫폼 및 애플리케이션 내에 존재하는 보안 취약성을 식별하고 해결하기 위한 프로세스를 시행하고 있습니다. 환경 안에서 이루어지는 지속적인 보안 개선에 따라, 서비스에 영향을 미칠 수 있고 식별된 위험을 완화하는 지침을 제공하는 보안 관련 정보를 수록한 AWS 보안 게시판이 작성되어 AWS 고객에게 제공됩니다. AWS 고객은 자체 취약성 관리 프로그램에 이들 게시판의 검토를 포함시키고 관련 권고 사항을 해당 서비스에 적용해야 합니다.

- **암호화.** AWS 고객은 자체 환경을 위해 민감한 데이터의 암호화를 전송 및 저장할 책임이 있습니다.

- **데이터 백업.** AWS 고객은 복원성을 위해 중복 서버를 구축하고 S3 복제(기본적으로 다중 중복 위치에 저장됨)를 사용할 수 있습니다. AWS 고객이 구현할 수 있는 다른 모든 백업 옵션은 고객의 판단에 의해 구성 및 관리되며, AWS 서비스 범위를 벗어납니다. AWS는 고객 데이터를 이동식 데이터에 백업하지 않습니다.

- **VPC 사용.** VPC는 사내 기존 IT 인프라와 AWS 클라우드를 연결하는 안전한 브리지입니다. 이 서비스는 기업이 가상 프라이빗 네트워크(VPN) 연결을 통해 기존 인프라를 분리된 AWS 컴퓨팅 리소스 세트에 연결하고 보안 서비스, 방화벽, 침입 탐지 시스템과 같은 기존 관리 기능을 확장하여 VPN 리소스를 포함할 수 있도록 합니다. 또한, VPC는 인터넷에 액세스하는 회사 웹서버를 위해 퍼블릭 서브넷을 생성하도록 구성할 수도 있습니다. 현재 VPC는 EC2 및 RDS와 통합되며, 향후 다른 AWS 서비스와도 통합될 수 있습니다. 이 서비스는 필요에 따라 준수 환경을 구현하고 AWS 고객의 네트워크 중 특정 세그먼트는 물론 AWS 데이터 스토리지 옵션의 보안 채널에 대한 퍼블릭 액세스를 줄이는 데 활용할 수 있습니다.

- **감사 로깅.** AWS는 고객이 CloudTrail을 사용하여 모든 AWS 관리 활동을 기록할 수 있는 기능을 제공합니다. 고객이 CloudTrail을 활성화하면 콘솔 및 CLI 모두로부터의 AWS API 호출이 모두 기록됩니다. 로그는 S3 버킷을 통해 제공되며, 따라서 고객이 적절한 권한 및 보존을 구성할 수 있습니다.

- **법의학 수사.** AWS는 법률에 따라 요구되는 법의학 수사에 협조합니다. AWS는 법의학 수사에 필요할 경우 고객 및 지정된 법의학 수사관과 공동으로 작업합니다.

- **기타 AWS 서비스 사용.** 현 시점에서 EC2, VPC, S3, EBS, RDS, ELB 및 IAM은 모두 본 지침이 적용됩니다. AWS가 FFIEC 요구 사항에 대해 평가하지 않는 다른 서비스는 범위에 명시되지 않았습니다.

AWS에서 제공하는 증거

AWS 서비스는 적용되는 표준 및 요구 사항에 대해 정기적으로 평가됩니다. 연방 기관, 국제 기구, 의료 기관, 금융 기관을 비롯해 다양한 산업을 지원하기 위해, AWS는 서비스 및 인프라에 대해 다양한 평가를 실시하고 있습니다. 타사에 의해 실시되는 평가의 전체 목록 및 관련 정보는 AWS 규정 준수 웹 사이트를 참조하십시오.

본 문서의 "Amazon Web Services에 대한 FFIEC 평가 지침" 단원에서 FFIEC 지침에 부합하는 AWS 제어를 증명하는 데 사용할 수 있는 몇몇 기본 감사 문서를 제시합니다.

Amazon Web Services: http://aws.amazon.com/compliance
연락처: http://aws.amazon.com/compliance/contact/

Coalfire: www.coalfire.com
전화: 877-224-8077
이메일: info@coalfire.com

Amazon Web Services에 대한 FFIEC 평가 지침

AWS 규정 준수 프로그램은 AWS 서비스가 관련 표준에 따라 정기적으로 감사를 받도록 보장합니다. 일부 제어는 고객이 AWS를 사용하는 과정에서 충족될 수 있습니다(예: 민감한 데이터에 대한 물리적 액세스). 하지만 대부분의 제어는 AWS 고객과 AWS 간 책임 분담이거나 온전히 고객의 책임입니다. 이 단원에서는 AWS가 제공된 서비스에 대해 부담하는 책임과 고객이 범위 내 AWS 서비스를 사용할 때 부담하는 책임에 대해 설명합니다.

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
IT 보안 프로그램 및 정책						
SP-1	IT 보안 프로그램 및 정책	조직의 크기 및 복잡성, 활동의 성격 및 범위에 적합한 관리, 기술 및 물리적 보호 조치를 포함하고, 프로그램의 목표를 포함하고, 구현의 책임을 지정하고, 규정 준수 및 시행의 방법을 제공하는 포괄적 정보 보안 프로그램을 개발, 문서화, 구현 및 유지합니다. 이사회 또는 적절한 고위 경영진이 이 프로그램을 승인합니까? 경영진이 정보 보안 프로그램의 목표 및 원칙을 지지한다는 경영진 의향서를 포함합니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4, Objective 7 p. A4-A5, p. A7 FFIEC MGT Booklet(2004) Appendix A: Objective 4, Objective 6 p. A5-A6, p. A7-A8	검사관은 AWS 서비스 관리 및 보안 역할 정의의 사용과 관련된 보안 정책 및 프로그램 문서를 검토해야 합니다. 검사관은 AWS 서비스가 정보 보안 프로그램 내에서 적절히 처리되는지 확인해야 합니다. 또한, 검사관은 AWS 사용에 대한 적절한 승인이 있는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 정보 보안 프로그램 선언문 2. 정보 보안 정책 3. AWS 관리 및 보안 역할 정의	조직의 정보 보안, 개인 정보 보호, 데이터 분류 정책을 검토하여 어떤 정책이 AWS 서비스 환경에 적용되는지 확인합니다. AWS 고객은 다음 자산 그룹의 보안을 책임집니다. • Amazon 머신 이미지(AMI) • 운영 체제 • 애플리케이션 • 전송 중인 데이터 • 저장된 데이터 • 데이터 스토어 • 자격 증명 IT 보안 정책은 AWS 서비스의 사용, 그리고 어떻게 기존 정보 보안 정책과 부합하는지를 기반으로 작성해야 합니다.	AWS는 고객 시스템 및 데이터의 기밀성, 무결성, 가용성을 보호할 수 있도록 고안된 공식적인 정보 보안 프로그램을 구현했습니다. 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. **참조:** ISO/IEC 27001:2005 Control: A.5.1.1 Service Organization Controls (SOC) 2 – Section III Area A PCI DSS v3.0 Requirement 12
SP-2	IT 보안 프로그램 및 정책	정보 보안 프로그램을 조정하도록 지명된 직원이 있습니까?	FFIEC IS Booklet(2006) Appendix A: Objective 7	검사관은 조직이 정보 보안 프로그램을 조정할 직원을 지명했는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 직원의 정보 보안 권한을 정의한 문서 2. 권한이 AWS 서비스의 사용 및 보안 구성까지 확장되는지 여부	조직은 보안 책임을 담당할 직원을 지명해야 하며 이 지명이 AWS 서비스의 사용까지 확장되어야 합니다.	AWS CISO(최고 정보 보안 책임자)가 존재하며 조직 전반에 걸친 정보 보안 프로그램의 조정, 개발, 구현 및 유지를 담당합니다. **참조:** ISO/IEC 27001:2005 Control: A.6.1.2 SOC 2 – Section III Area C PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
SP-3	IT 보안 프로그램 및 정책	보안 프로그램이 조직의 운영 및 시스템 변경 사항은 물론 조직이 보유하는 고객 정보에 대한 위협 또는 위험의 변화를 반영하여 주기적으로 업데이트됩니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4.2 p. A5	검사관은 고객 보안 프로그램이 해당 조직에서 사용하는 AWS 서비스의 변경 사항을 반영하여 주기적으로 업데이트되는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 운영 및 시스템 변경 사항 및 고객의 AWS 서비스 사용과 관련된 위협 또는 위험의 변화 2. 위험 평가 및 AWS 서비스 사용과 관련된 위험 및 위협이 식별되고 위험 요소 처리 조치가 시행 중인지 확인 **참조**: AWS 보안 게시판	조직의 보안, 개인 정보 보호, 데이터 분류 정책을 재평가 및 검토하여 어떤 정책이 AWS 서비스 환경에 적용되는지 확인합니다. 연간 위험 평가 내에서 AWS 서비스 사용과 관련된 위협 및 위험을 식별하여 문서화하며 위험 요소 처리 및/또는 완화를 개략적으로 기술합니다.	AWS 관리팀은 최소한 1년에 두 번 이상 보안 프로그램을 재평가합니다. 이 프로세스에서는 관리 팀이 책임 영역 내의 위험을 식별하고 그러한 위험을 해결할 수 있도록 고안된 적절한 대책을 구현해야 합니다. **참조:** NIST SP 800-53 rev.3 FedRAMP Control: CA-2 (2) SOC 2 – Section III Area A PCI DSS v3.0 Requirement 12
SP-4	IT 보안 프로그램 및 정책	정보 보안 정책에 이사회(BOD), 관리자 및 직원의 역할 및 책임이 명확하게 정의되어 있습니까? 각 담당 당사자는 조직 내 보안 프로그램의 구현에서 보안 담당자를 지원할 수 있어야 합니다. 다음은 핵심 역할 및 책임 중 일부입니다. - ISO(정보 보안 책임자) - IT 운영 위원회 - 인시던트 대응 팀 - 비즈니스 연속성 팀	FFIEC IS Booklet(2006) Appendix A: Objective 7 p. A7 FFIEC MGT Booklet(2004) Appendix A: Objective 2, Objective 4 p. A2-A3, A5-A6 FFIEC OPS Booklet(2004) Appendix A: Objective 2 p. A2	검사관은 정보 보안 정책에서 이사회(BOD), 관리자 및 직원의 역할 및 책임이 명확히 정의되어 있고 각 담당 당사자가 AWS 서비스의 사용 및 구성과 관련된 조직 내 보안 프로그램의 구현에서 보안 담당자를 지원할 수 있는지 확인합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 다음 역할 내에서 AWS 서비스 책임이 정의 및 문서화된 경우: - ISO(정보 보안 책임자) - IT 운영 위원회 - 인시던트 대응 팀 - 비즈니스 연속성 팀	AWS 서비스의 관리, 보안, 복원성 및 관리 감독과 관련된 내부 역할 및 책임을 문서화합니다. 조직 프레임 워크를 기반으로 다음 역할 또는 비슷한 역할에 대해 AWS 서비스 책임을 정의합니다. - ISO(정보 보안 책임자) - IT 운영 위원회 - 인시던트 대응 팀 - 비즈니스 연속성 팀	AWS CISO(최고 정보 보안 책임자)가 존재하며 조직 전반에 걸친 정보 보안 프로그램의 조정, 개발, 구현 및 유지를 담당합니다. **참조:** ISO/IEC 27001:2005 Control: A.5.1.3 SOC 2 – Section III, 'Relevant Aspects of Internal Controls' PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
SP-5	IT 보안 프로그램 및 정책	기관이 IT 보안 정책 집합을 보유하고 있습니까? 정책이 기관 규모 및 복잡성을 고려합니까? 다음은 필요한 정책 중 일부입니다. - 사용 제한 - 액세스 제어 - 변경 제어 - 역할 및 책임 - 인력 보안 - 물리적 보안 - 시스템 개발/획득 및 유지 관리 - 공급업체 관리 및 아웃소싱 - 암호화 - 정보 보안 작업 - 백업 - 미디어 폐기, 운반 및 취급 - 보안 검토 및 평가 - 인시던트 대응 - 방화벽 정책 - 평가 및 로깅	FFIEC IS Booklet(2006) Appendix A: Objective 2 p. A2-A3 FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC MGT Booklet(2004) Appendix A: Objective 3, Objective 6 p. A3-A5, A7-A8	검사관은 기관이 보안 정책 집합을 보유하고 AWS 서비스 사용이 배포된 서비스의 조직 규모 및 복잡성을 기반으로 문서화되는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 사용 제한, 액세스 제어, 변경 관리, 공급업체 관리 표준 및 절차 2. AWS 액세스 제어 구성 샘플 3. 변경 요청의 AWS 변경 관리 샘플	고객 정보를 관리하기 위해 공식 IT 보안 프로그램이 개발되어야 합니다. 기관은 기관 규모 및 복잡성을 고려한 IT 보안 정책 집합을 보유해야 합니다. 정책이 AWS 서비스의 사용 및 관리를 포함해야 합니다.	ISMS 프로그램은 보안 정책 및 관련 절차와 함께 계획된 주기마다 검토되며 식별된 문제 영역을 처리하기 위한 실행 계획이 확인됩니다. **참조:** ISO/IEC 27001:2005 Control: A.5.1.2 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
SP-6	IT 보안 프로그램 및 정책	적절한 고객 정보 공개에 대한 정책 및 지침이 문서화되어 있습니까? 직원에게 이러한 정책에 대한 교육을 실시해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Objective 6 p. A6-A7 Standards for Safety and Soundness: Supplement A to Appendix B 12 CFR § 364 (2005)	검사관은 내부 시스템 내에서는 AWS와 같은 외부 서비스 사용에 대해서도 적절한 고객 정보 공개에 대한 정책 및 절차가 문서화되어 있는지 확인해야 합니다. 검사관은 직원에게 이 정책에 대한 교육을 실시하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 데이터 분류 정책/절차 2. 인시던트 대응 프로세스 3. 데이터 관리 및 공개와 관련된 직원 교육	조직은 내부 및 외부 서비스에서 적절한 고객 정보 공개에 대한 정책 및 지침을 수립해야 하며, 이 정책 및 지침은 AWS 서비스 환경에서 정보의 적절한 데이터 분류 표준을 문서화합니다. 또한, 직원에게 정보가 부적절하게 취급되었을 경우 인시던트 보고 프로세스를 비롯해 정책 절차에 대한 교육을 실시해야 합니다.	AWS 직원은 전반적인 회사 표준 및 정보 보안에 대한 책임을 확인하는 고용 계약서에 서명해야 합니다. 여기에 고객 정보 공개 프로세스가 포함됩니다. 모든 Amazon 직원은 정보 보호 요건을 포함하는 비밀 유지 계약에 서명합니다. **참조**: ISO/IEC 27001:2005 Control: A.6.1.5 & A.7.1.3 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
SP-7	IT 보안 프로그램 및 정책	경영진 및 BOD가 정기적으로 검토 및 승인합니까? - 업데이트된 정보 보안 프로그램 - 업데이트된 정책	FFIEC IS Booklet(2006) Appendix A: Objective 4.2 p. A5 FFIEC MGT Booklet(2004) Appendix A: Objective 3, Objective 5 p. A3-A5, A6-A7	검사관은 경영진이 정기적으로 정보 보안 프로그램 및 정책을 업데이트하여 AWS 서비스 사용 및 구성 관련 변경 사항을 포함시키는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스 사용과 관련된 공급업체 관리 보고서 2. 조직 내부에서 사용 중인 모든 서비스가 정보 보안 프로그램 및 정책 내에서 문서화되었는지 검증	조직은 정기적으로 정보 보안 프로그램 및 정책을 업데이트하여 조직 내부의 AWS 서비스 사용 및 구성 관련 변경 사항을 포함시키기 위한 일정을 수립해야 합니다.	ISMS 프로그램은 보안 정책 및 관련 절차와 함께 계획된 간격으로 검토되며 식별된 문제 영역을 처리하기 위한 실행 계획이 확인됩니다. **참조**: ISO/IEC 27001:2005 Control: A.5.1.2 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
SP-8	IT 보안 프로그램 및 정책	보안 정책이 보안 도구를 사용하거나 규정 미준수를 제재하여 시행됩니까? 정책 및 제재가 모든 직원에게 명확히 전달됩니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4.2 p. A5 FFIEC IS Booklet(2006) Appendix A: Tier II: F p. A16	검사관은 보안 정책이 보안 도구를 사용하거나 규정 미준수를 제재하여 시행되는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 환경으로부터 발생하는 경보가 시기 적절하게 식별 및 처리되며 대응이 조직의 정책 및 절차와 부합하는지 확인하기 위해, 조직에 의한 보안 정보 및 이벤트 관리 시스템(SIEM)의 사용 2. 다음과 같은 AWS 보고 도구의 사용을 검토합니다. a. Amazon CloudWatch b. AWS Trusted Advisor	조직은 AWS 서비스를 SIEM(보안 정보 및 이벤트 관리) 도구에 통합하여 조직 내에서 정책, 규정 미준수 절차 및 제재가 명확히 전달되도록 해야 합니다. 또한, 조직은 AWS 도구 및 서비스를 평가 및 사용하여 보안 프로세스 및 구성을 모니터링해야 합니다. 도구 예: 1. Amazon CloudWatch 2. AWS Trusted Advisor	AWS는 Amazon 인사 관리 시스템(HRMS) 내 개발 목록의 사용을 통해 정보 보안 정책 및 절차를 위반한 직원에 대한 공식 제재 프로세스를 운영하고 있습니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: PS-8 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
정보 보안 감독						
OV-1	정보 보안 감독	BOD/고위 경영진이 IS 관리자에게 다음 사항이 실시되는 방식에 대한 기대 및 요건을 서면으로 명확하게 전달했습니까? - 중앙 감독 및 조정 - 조직 보안 프로그램의 역할 및 책임 - 위험 관리 - 모니터링 및 테스트 - 운영 효율성을 테스트하기 위해 조직 보안 프로세스의 보고 기능 - 알림 및 예외에 관한 보안 보고서 - 조직에서 허용되는 잔존 위험	FFIEC IS Booklet(2006) Appendix A: Objective 4.2 p. A5 FFIEC MGT Booklet(2004) Appendix A: Objective 3, Objective 5 p. A3-A5, A6-A7 FFIEC OPS Booklet(2004) Appendix A: Objective 2 p. A2-A3 FFIEC AUD Booklet(2012) Appendix A: Objective 2 p. A2-A3	검사관은 AWS 서비스 사용에 대한 중앙 감독과 관련하여 역할 및 책임이 정의되었는지 검토해야 합니다. AWS 서비스가 위험 평가 프로세스와 통합되었는지 여부를 확인합니다. 통합되었다면, 조직의 전체 위험 프로필 및 위험 허용치에 대한 AWS 배포의 중요성을 평가합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS와 관련된 소프트웨어 개발 수명 주기(SDLC) 프로세스 2. AWS 서비스 테스트 및 모니터링 프로세스 3. AWS 서비스와 관련된 위험 평가 및 위험 관리 계획	조직의 보안, 정책 및 절차를 검토하여 어느 정책 요소(예: 역할 및 책임, 위험 관리, 모니터링 및 보고)가 AWS 서비스 환경에 적용되는지 확인합니다. 조직은 AWS 서비스 사용이 다음에 포함되도록 해야 합니다. 1. SDLC 프로세스 2. 서비스 테스트 및 모니터링 3. 위험 평가 및 처리 계획 4. 보안 보고 AWS 보안 게시판	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. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: RA-1 SOC 2 – Section III PCI DSS v3.0 Requirement 12
OV-2	정보 보안 감독	조직이 매년 외부 기관 평가를 통해 내부 제어의 운영 효율성을 테스트합니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC AUD Booklet(2012) Appendix A: Objective 10 p. A6-A7	검사관은 내부 제어의 운영 효율성을 테스트하는 연례 외부 기관 평가가 조직이 사용하는 AWS 서비스를 통합하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직의 제어에 대한 외부 보고서 **보고서 예:** *2.* SOC(Service Organization Control) 1 *3.* SOC(Service Organization Control) 2 *4.* PCI(Payment Card Industry) 규정 준수 증명	고객은 가상 머신 인스턴스상의 게스트 운영 체제 및 애플리케이션, S3 버킷 또는 RDS 데이터베이스 내 데이터 및 객체 등 조직이 AWS 자산에 추가하거나 AWS 자산과 연결하는 일체의 보안을 책임집니다. 고객은 외부 평가자와 협력하여 AWS 서비스의 사용 및 구성을 이해하도록 지원해야 합니다.	AWS는 AWS가 호스트 운영 체제 및 가상화 계층에서 서비스 운영 시설의 물리적 보안에 이르기까지 구성 요소를 운영, 관리 및 제어하는 보안 글로벌 인프라 및 서비스를 제공합니다. 적용 가능한 AWS 규정 준수 인증 및 보고서를 요청할 수 있습니다. 다음 링크를 참조하십시오. AWS 규정 준수 요청 **참조**: SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
OV-3	정보 보안 감독	BOD 및 고위 경영진이 보안 프로그램 시행과 제어 효율성을 확인하기 위해 정기적으로 보고를 받습니까?	FFIEC MGT Booklet(2004) Appendix A: Objective 3, Objective 5 p. A3-A5, A6-A7 FFIEC OPS Booklet(2004) Appendix A: Objective 3 p. A3	검사관은 이사회 및 고위 경영진이 내부 및 AWS 서비스와 관련된 보안 프로그램 시행과 제어 효율성을 확인하기 위해 제어에 관해 정기적으로 보고를 받는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 고위 직원 정보 보안 브리핑, 2. BOD 회의 안건 및 의사록 3. 제어 보고서	조직은 정보 보안 프로그램이 내부 경영진을 대상으로 정기 보안 브리핑을 실시하고 BOD가 내부 시스템 및 AWS 서비스 모두에 대해 제어에 관해 보고받도록 해야 합니다.	AWS 규정 준수 관리자는 다양한 타사 검토로 구성된 연간 감사 일정에 따라 정기적으로 다양한 제어 보고서를 발표합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CA-2 (1) SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
OV-4	정보 보안 감독	고위 경영진이 IT 평가 결과 및 권고 사항에 대해 시기 적절하고 유효한 조치를 취하고 경영진이 BOD 또는 평가 위원회에게 조치를 보고합니까?	FFIEC IS Booklet(2006) Appendix A: Objective 7 p. A7 FFIEC MGT Booklet(2004) Appendix A: Objective 5 p. A6-A7	검사관은 내부 및 AWS 서비스에 대한 평가 결과를 검토하고 위험 요소를 완화할 적절한 교정 활동이 수립, 추적 및 완료되었는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 위험 요소 처리 계획(일정/마일스톤 포함) 2. 위험 요소 처리 회의록(고위 경영진) 3. 결과 교정 문서	조직은 내부 평가 결과의 위험 요소를 평가하는 프로그램 및 프로세스를 구비해야 하며 교정 활동 및 경영진 대상 보고 프로세스를 문서화해야 합니다.	AWS는 FISMA 표준과는 다른 차이점들로 인해, 필요한 교정 조치가 확인 및 계획된 시스템과 연간 보안 제어 평가 시 확인된 AWS 서비스 배포를 위한 실행 계획 및 마일스톤(POA&M) 프로그램을 실시하고 있습니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CA-5 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
위험 평가						
RA-1	위험 평가	여러 부서로 구성된 관리 팀이 정립된 방법론을 사용하여 주요 비즈니스 프로세스에 대한 철저한 검토를 요구하는 포괄적 위험 평가를 실시했습니까? 고객 정보의 위치, 시스템, 저장 방법, 처리 방법, 전송 방법 및 폐기 방법을 고려하고 고객 정보 및/또는 정보 시스템에 대한 합리적으로 예측 가능한 내부 및 외부 위협을 식별하고 가능성 및 영향 분석을 실시합니까? 보안 프로그램이 위험 평가를 기반으로 합니까? 위험 평가가 제대로 문서화되고 검토되며 주요 시스템 또는 프로세스 변경에 따라 필요할 경우 업데이트됩니까?	FFIEC IS Booklet(2006) Appendix A: Objective 3 p. A3-A4 FFIEC OPS Booklet(2004) Appendix A: Objective 3, Objective 5 p. A3, p. A4-A5	검사관은 고객이 AWS 서비스 사용을 조직 위험 평가에 통합하고 AWS에서 호스팅되는 주요 비즈니스 프로세스를 식별했는지 확인해야 합니다. 또한, 조직의 전체 위험 프로필 및 위험 허용치에 대한 AWS 배포의 중요성을 평가합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스가 범위에 포함되었는지 확인하기 위해, 최근 위험 평가 2. 식별된 교정 조치가 식별된 결함을 교정하기 위해 지정된 마일스톤 프로세스 포함 일정을 따르는지 확인하기 위해, 위험 요소 처리 계획	AWS 사용을 위험 평가에 통합합니다. 조직 위험 평가 프로세스에 AWS 서비스 요소를 수행 및/또는 통합합니다. 주요 위험에는 다음이 포함될 수 있습니다. • AWS 사용과 관련된 기업 위험을 식별하고 기업 소유자 및 주요 이해관계자를 파악합니다. • 기밀성, 무결성 및 가용성 보호를 위한 AWS 서비스 사용 및 조직의 보안 기준 내에서 기업 위험이 정렬되고 등급이 매겨지거나 분류되었는지 확인합니다. • AWS 서비스(SOC, PCI, NIST 800-53 관련 감사 등)와 관련된 이전 감사를 검토합니다. • 이전에 식별된 위험이 적절하게 처리되었는지 확인합니다. • AWS 검토를 수행하기 위해 전체 위험을 평가합니다.	이 정책에 따라, 모든 AWS 리전 및 회사를 포함하는 연간 위험 평가가 AWS 규정 준수 팀과 AWS 고위 경영진(AWS CISO, 재무 담당 VP 및 서비스 오퍼레이션 담당 VP 포함)에 의해 실시됩니다. 외부 감사자가 실시하는 보안 평가에 추가되는 평가입니다. 위험 평가의 목적은 회사가 보안 정책 및 표준을 준수하는지 확인하고(AWS를 포함하여), AWS의 위협과 취약성을 식별하고, 위협과 취약성에 위험 등급을 배정하며, 평가를 공식적으로 문서화하고 문제 해결을 위한 위험 처리 계획을 작성하는 것입니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: RA-1 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12
RA-2	위험 평가	정보 자산(예: 데이터 시스템, 물리적 위치)을 식별하고 순위를 결정하기 위해 위험 평가의 일환으로 시스템 특성 분석이 실시되었습니까?	FFIEC IS Booklet(2006) Appendix A: Objective 3 p. A3-A4	정보 자산(예: 애플리케이션 데이터 시스템 등)을 식별하고 순위를 결정하기 위해 위험 평가의 일환으로 AWS 서비스에 대해 시스템 특성 분석이 문서화되었습니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스가 특성 분석되고 순위가 결정되었는지 확인하기 위해, 최근 위험 평가	고객은 AWS 사용과 연결된 기업 위험을 식별하고 AWS 서비스 사용에 대한 전반적 위험 요소를 평가하는 노력에서 기업 소유자 및 주요 이해관계자를 식별해야 합니다.	보안 범주화는 AWS 규정 준수 팀이 연간 위험 평가 내에서 또한 서비스 온보딩 시 AWS 서비스 소유자와 공동으로 실시하는 범조직적 활동입니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: RA-2 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
RA-3	위험 평가	기관 및 고객 개인정보보호에 위험 평가가 고려되었습니까?	FFIEC IS Booklet(2006) Appendix A: Objective 3 p. A3-A4	검사관은 위험 평가가 기관 및 고객 개인정보보호와 관련하여 AWS 서비스 사용을 고려했는지 확인해야 합니다. 검사관은 다음 항목을 요청 및 검토해야 합니다. 1. AWS 서비스 사용에 대한 고려를 포함하는 개인정보보호 영향 평가가 완료되었는지 확인하기 위해, 최근 위험 평가	고객은 데이터 취급 및 저장에 관한 개인정보보호 문제를 관리하고 개인정보보호와 관련하여 AWS 서비스 사용에 대한 위험 평가를 실시할 책임이 있습니다.	AWS는 미연방 규정 준수 활동의 일환으로 매년 개인정보보호 영향 평가(PIA)를 실시합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: PL-5 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12 자세한 내용은 다음을 참조하십시오. AWS 개인정보보호 안내문
RA-4	위험 평가	위험 평가가 아웃소싱 관계로 인한 타사 서비스 공급자 및 위험을 고려합니까?	FFIEC IS Booklet(2006) Appendix A: Objective 3, Objective 5 p. A3-A4, A5-A6	검사관은 위험 평가가 AWS를 포함하여 아웃소싱 관계로 인한 타사 서비스 공급자 및 위험을 고려하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 타사 공급업체 관리 정책 및 절차 2. 타사 사전 계약 위험 평가 및/또는 보안 검토	조직은 타사 서비스 공급자와 관련된 위험 평가 프로세스를 관리하는 프로세스를 개발하고 AWS를 포함하여 아웃소싱 관계와 관련된 위험을 문서화해야 합니다.	AWS의 안전한 소프트웨어 개발 프로세스는 외부 당사자 검토를 위한 보안 검토 프로세스와 타사 소프트웨어 검토 프로세스를 규정합니다. AWS는 승인된 공급자 및 미승인된 타사 공급자의 목록을 관리하고 있습니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SA-2 SOC 2 – Section III PCI DSS v3.0 Requirement 12
RA-5	위험 평가	이사회 또는 지명된 감독 위원회가 정기적으로 위험 평가 프로세스를 검토합니까?	FFIEC IS Booklet(2006) Appendix A: Objective 3 p. A3-A4 FFIEC MGT Booklet(2004) Appendix A: Objective 5 p. A6-A7	검사관은 이사회 또는 지명된 감독 위원회가 정기적으로 평가 프로세스를 검토하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다**. 1. 위험 평가 및 처리 활동과 관련된 정기적 이사회 안건 상정, 의사록 및 브리핑	조직은 위험 평가 프로세스가 감독 조직(예: 경영진 및 이사회)에 대한 검토 및 승인을 포함하도록 확인하여야 하는데 이에는 조직 내에서 사용되는 AWS 서비스도 포함됩니다.	이 정책에 따라, 모든 AWS 리전 및 영업망을 포함하는 연간 위험 평가가 AWS 규정 준수 팀과 AWS 고위 경영진(AWS CISO, 재무 담당 VP 및 서비스 오퍼레이션 담당 VP 포함)에 의해 실시됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: RA-1 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
인시던트 대응						
IR-1	인시던트 대응	공식 인시던트 대응 계획 및 정책이 제대로 문서화되어 있고 규제 및 집행 기관으로 적절하게 보고되고 있습니까? 인시던트 대응 계획이 인시던트 처리 프로세스를 규정하는 세부 인시던트 대응 절차를 포함해야 합니다. - 역할 및 책임 - 초기 대응 - 억제 - 시스템 복원 - 보고	FFIEC IS Booklet(2006) Appendix A: Objective 6 p. A6-A7 FFIEC OPS Booklet(2004) Appendix A: Objective 10 p. A8-A9	검사관은 인시던트 대응 계획 및 정책이 적절한 AWS 보고 프로세스는 물론 조직과 AWS 간 커뮤니케이션 절차를 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 인시던트 대응 정책, 계획 및 절차 2. 인시던트 대응 계획 조정 문서 및 조직과 AWS 간 약정	AWS 책임 분담 모델은 고객이 자신의 환경을 운영 체제와 상위 계층에서 모니터링 및 관리하도록 요구합니다. 조직은 AWS 서비스 사용에 기초하여 기존의 인시던트 대응 정책, 프로세스, 도구 및 방법론을 조정해야 합니다.	AWS는 "AWS 인시던트 대응 계획"이라고 하는 공식적이고 문서화된 인시던트 대응 정책을 마련했으며, 이 정책은 매년 업데이트 및 검토됩니다. 인시던트 대응 정책은 내부 Amazon 포털을 통해 모든 직원 및 계약업체로 전파됩니다. AWS 규정 준수 팀은 AWS 최고 정보 보안 책임자의 승인을 얻어 매년 이 정책을 검토합니다. 이 정책은 목적, 범위, 역할, 책임 및 경영진의 책임감을 규정합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IR-1 SOC 2 – Appendix 1, Security Policy Criteria 1.2 Mapping PCI DSS v3.0 Requirement 12
IR-2	인시던트 대응	평가 로깅, 네트워크 및 호스트 기반 IDS와 같은 적절한 인시던트 모니터링 도구가 배포되었습니까?	FFIEC IS Booklet(2006) Appendix A: Objective 6 p. A6-A7	검사관은 조직이 기존의 인시던트 모니터링 도구는 물론 AWS 사용을 모니터링하기 위해 AWS가 제공하는 도구를 적절히 업데이트 및 활용했는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 내부 인시던트 대응 및 모니터링 도구의 사용 2. AWS 서비스 환경에서 사용되는 도구 **예:** • AWS CloudWatch • EC2 Describe API • Amazon Simple Notification Service • AWS 상태 대시보드 • AWS CloudTrail 로그 • AWS Config	고객은 AWS 서비스 및 도구를 자체 인시던트 대응 계획에 통합해야 합니다. **예:** • AWS CloudWatch • EC2 Describe API • Amazon Simple Notification Service • AWS 상태 대시보드 • AWS CloudTrail 로그 • AWS Config 이러한 AWS 서비스는 AWS 서비스를 모니터링하는 데 유용할 수 있습니다.	Amazon 사고 관리 팀은 비즈니스에 영향을 미치는 이벤트 발생 시 해결책을 모색하기 위해 업계 표준의 진단 절차를 사용합니다. 관리 직원은 상시 사고를 감지하고 이들이 미치는 영향과 해결방안을 관리합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IR-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
IR-3	인시던트 대응	이벤트를 인시던트로 에스컬레이션하는 임계값이 정의되어 있습니까?	FFIEC IS Booklet(2006) Appendix A: Objective 6 p. A6-A7 FFIEC OPS Booklet(2004) Appendix A: Objective 10 p. A8-A9	검사관은 조직의 AWS 서비스 사용이 내부에서 정의된 임계값과 부합하고 임계값을 지원할 수 있는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 임계값 및 에스컬레이션 절차를 지정하는 문서 2. 문서화된 임계값을 내부 도구 및 AWS 도구와 비교하여 해당 도구가 명시된 값을 지원하고 부합하는지 확인	고객은 내부적으로 정의된 임계값 및 에스컬레이션 프로세스를 준수하도록 AWS 모니터링 서비스를 구성해야 합니다.	AWS는 준비 활동, 탐지 및 분석 기능뿐만 아니라 억제, 원인 제거 및 복구 절차 등 보안 인시던트를 처리하는 데 필요한 다양한 프로세스를 실시하고 있습니다. AWS는 다양한 AWS 서비스에 걸쳐 다중 이벤트에 대응합니다. 따라서 AWS 내에서는 특별히 정의된 임계값이 없습니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IR-4 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 12
IR-4	인시던트 대응	인시던트 대응 계획이 매년 검토되고 필요에 따라 변경됩니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC OPS Booklet(2004) Appendix A: Objective 3 p. A3	검사관은 인시던트 대응 계획이 매년 검토되고 AWS와 관련하여 필요시마다 변경되는지 확인합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 인시던트 대응 계획 검토와 관련된 문서	조직은 연습으로부터의 교훈, 실제 인시던트 및 사용 중 AWS 서비스를 포함시키기 위한 서비스 환경 변화를 포함하는 연간 인시던트 대응 프로세스 검토를 지정해야 합니다.	AWS는 "AWS 인시던트 대응 계획"이라고 하는 공식적이고 문서화된 인시던트 대응 정책을 수립했으며 이 정책은 매년 업데이트 및 검토됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IR-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 12
IR-5	인시던트 대응	고객 정보가 부적절하게 노출될 경우, 인스던트 대응 계획은 고객에게 통지를 할 것을 요구하고 있습니까?	FFIEC IS Booklet(2006) Appendix A: Objective 6 p. A6-A7	검사관은 인시던트 대응 계획이 고객 영향 알림 절차를 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 에스컬레이션 및 알림 절차와 관련된 문서	조직은 정보 공개 시 에스컬레이션 및 고객 알림을 문서화해야 합니다.	AWS는 고객에게 영향을 미치는 인시던트를 AWS 인시던트 대응 계획에 따라 보고합니다. AWS 시스템, 호스트, 로그, 레코드와 관련된 모든 조사는 AWS 보안 팀이 실시합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IR-6 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
인력 제어						
PE-1	인력 제어	고객 정보에 액세스할 수 있는 중요한 또는 신뢰할 수 있는 직책에 있는 모든 IT 운영 직원이 고용 시 배경 조회를 포함해 포괄적 적격 심사 프로세스를 거칩니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: F p. A16 FFIEC OPS Booklet(2004) Appendix A: Objective 5 p. A4-A5	검사관은 조직 인력 보안(PS) 프로그램이 AWS 서비스 지원 인력 지명을 참조하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직 배경 조회 프로세스 2. 신뢰할 수 있는 직책 지명과 관련된 정책 및 절차	조직은 내부 적격 심사 프로세스에서 신뢰할 수 있는 직책을 정의하고 내부 및 외부 서비스(예: AWS)에 대한 액세스 레벨 배정과 부합하도록 해야 합니다.	AWS 내 시스템 및 장치를 지원하는 모든 AWS 직원은 AWS 모기업인 Amazon.com 내에서 고위험직으로 분류되고 있습니다. 이러한 직원은 민감한 AWS 영업비밀, 기밀 또는 독점 정보 또는 기타 소중한 기업 자산에 액세스 가능한 직책을 가진 것으로 간주됩니다. 철저한 배경 조회가 고용 전 프로세스의 일환으로 모든 AWS 직원에 대해 실시됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: PS-1 SOC 2 – Security Procedures Criteria 3.11 description PCI DSS v3.0 Requirement 12
PE-2	인력 제어	업무가 적절히 분담되고, 데이터 보안 작업을 수행하는 IT 직원이 시스템 및 프로그래밍, 컴퓨터 운영, 데이터 입출력 및 평가 활동으로부터 독립적이고, 가능할 경우 사기 및 부정을 방지하기 위해 경영진이 IT 직원 사이에서 직무 분리 및 로테이션을 실시합니까?	FFIEC IS Booklet(2006) Appendix A: Objective 7 p. A7 FFIEC MGT Booklet(2004) Appendix A: Objective 2 p. A2-A3 FFIEC OPS Booklet(2004) Appendix A: Objective 5 p. A4-A5	검사관은 조직이 업무 분담 프로세스를 확대하여 AWS 서비스 관리 및 운영까지 포함시켰는지 확인해야 합니다. 또한, 검사관은 조직 데이터 분류 및 모든 시스템에 대한 액세스 관리 정책, 절차 및 구현이 AWS 서비스를 포함하도록 검토 및 교차 참조해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직 데이터 분류 표준 2. 액세스 관리 정책 및 절차 3. AWS 관리자 및 사용자 그룹 구성	조직은 적절한 업무 분담이 정의되고 내부 데이터 분류 표준과 내부 시스템 및 AWS 서비스 내에서의 액세스 관리 표준 및 구성과 부합하도록 해야 합니다.	AWS는 필요에 따라 개인의 업무를 분담하여 악의적 행위의 공모를 예방합니다. 업무 분담은 액세스 제어, 그룹 권한, 논리적 액세스 및 변경 관리 프로세스를 통해 관리됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-5 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 7

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
PE-3	인력 제어	이중 관리 제어, 업무 분담, 고객 정보에 액세스 가능한 직원에 대한 배경 조회를 규정하는 문서화된 정책 및 절차가 있습니까?	FFIEC OPS Booklet(2004) Appendix A: Objective 5 p. A4-A5	검사관은 조직이 관리 구성 및 이중 제어 구현과 관련된 정책 및 절차에 AWS 서비스를 포함시켰는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 내부 시스템 및 AWS 서비스의 IT 관리와 관련된 정책 및 절차	조직은 내부 시스템 및 AWS 서비스의 이중 관리 제어를 지원하는 정책 및 절차를 문서화하고 실시해야 합니다.	AWS는 필요에 따라 개인의 업무를 분담하여 악의적 행위의 공모를 예방합니다. 업무 분담은 액세스 제어, 그룹 권한, 논리적 액세스 및 변경 관리 프로세스를 통해 관리됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-5 SOC 2 – Section III, Area A PCI DSS v3.0 Requirement 7
PE-4	인력 제어	조직은 직원 교육 프로그램을 통해 보안 문제 및 책임에 대한 인식을 제고해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Objective 4.2 p. A5 FFIEC IS Booklet(2006) Appendix A: Tier II: F p. A16	검사관은 조직의 직원 교육 프로그램을 점검하고 해당 프로그램이 내부 시스템 및 AWS 서비스에 대한 보안 문제 및 책임을 정의하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 직원 보안 교육 정책 및 절차	조직은 내부 보안 의식 고취 프로그램이 AWS 서비스의 사용, 구성 및 지원과 관련된 요소를 포함하도록 해야 합니다.	AWS는 "AWS 인식 및 교육 정책"이라고 하는 공식적이고 문서화된 인식 및 교육 정책을 마련했으며, 이 정책은 적어도 매년 검토 및 업데이트됩니다. AWS 인식 및 교육 정책은 내부 AWS 규정 준수 웹 포털을 통해 모든 직원, 공급업체 및 계약업체로 전파됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AT-1 SOC 2 – Section III, Area B PCI DSS v3.0 Requirement 12
PE-5	인력 제어	모든 직원이 회사 정책을 읽고 이해했음을 인정하는 양해 문서에 서명합니까? 직원은 정보 기밀성, 비밀 유지 및 정보 리소스의 허가된 사용에 관한 규칙을 이해 및 준수해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Objective 4.2 p. A5 FFIEC IS Booklet(2006) Appendix A: Tier II: F p. A16	검사관은 모든 직원이 정보 유출자, 비밀 유지, 그리고 AWS 와 같은 외부 서비스를 망라하는 정보 자원의 허가된 사용과 관한 양해 문서에 서명하는지 여부를 점검해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 정보 공개와 IT 서비스 및 AWS 서비스의 허가된 사용과 관련된 정책 및 절차	조직은 내부 시스템과 AWS 서비스의 사용 및 관리와 관련하여 직원의 책임을 규정하는 비밀 유지 계약을 문서화해야 합니다.	직무 적응 프로세스의 일부로서 AWS 내 시스템 및 장치를 지원하는 모든 개인은 액세스 권한이 부여되기에 앞서 비밀 유지 계약서에 서명합니다. 또한, 오리엔테이션 교육의 일부로서 개인은 Amazon 기업 행동강령 및 윤리강령(행동강령) 정책을 읽고 수락해야 합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: PS-6 SOC 2 – Section III, Area B PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
변경 관리 제어						
CM-1	변경 관리 제어	적절한 변경 관리 프로세스가 배포되었습니까? 다음 사항이 포함되어야 합니다. - 변경 관리 프로세스, 정책, 절차 및 양식 - 전체 변경 제어 프로세스를 관리하기 위한 변경 제어 감독 기능 또한, 경영진은 무엇이 "변경"을 구성하는지, 변경 프로세스를 통제하기 위해 어떤 표준을 따를지 공식적으로 규정해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 5 p. A4-A5 FFIEC D&A Booklet (2004) Appendix A: Objective 2, Objective 5, Objective 6, Objective 7 p. A2, A3-A6	검사관은 변경 관리 프로세스가 실시 중이고 AWS 서비스 관련 변경 사항을 포함하여 내부 변경 프로세스와 동일하게 추적 및 승인하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 변경 관리 관련 정책 및 절차 2. AWS 서비스의 변경 관련 변경 요청 샘플	조직은 모든 AWS 서비스 구성 요소에 대한 변경 관리 프로세스 및 실행을 기존의 변경 관리 승인 프로세스 및 정책에 통합하고 경영진이 AWS 서비스 사용 내에서의 변화를 확인할 수 있도록 해야 합니다.	AWS는 "AWS 구성 관리 정책"이라고 하는, AWS에 적용되는 공식적이고 문서화된 구성 관리 정책을 마련했습니다. AWS 구성 관리 정책은 내부 AWS 규정 준수 웹 포털을 통해 모든 직원, 공급업체 및 계약업체로 전파됩니다. AWS 규정 준수 팀은 AWS 최고 정보 보안 책임자의 승인을 얻어 매년 이 정책을 검토합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
CM-2	변경 관리 제어	변경 관리 절차가 다음 사항을 고려합니까? - 변경 요청 승인 - 테스트 - 철회 절차 - 변경 로그 - 사용자 교육	FFIEC D&A Booklet (2004) Appendix A: Objective 10 p. A7-A8	검사관은 변경 관리 프로세스가 AWS 서비스 및 AWS 서비스 변경 사항의 관리를 포함하고 변경과 관련된 테스트, 철회 절차, 교육 및 로그를 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스 변경 사항에 관한 테스트, 철회 프로세스 및 교육과 관련된 문서화된 프로세스 요소	AWS 서비스 사용이 내부 시리즈와 동일한 변경 제어 프로세스를 따라야 합니다. 자세한 내용은 다음을 참조하십시오. AWS 설명서	AWS 서비스 소유자가 시스템 및 장치에서 변경 사항을 구현하기 전에 AWS 내 시스템 및 장치에 대한 변경을 테스트, 검증, 문서화합니다. AWS 구성 관리 계획에 따라 서비스 소유자는 각 변경 사항과 관련된 테스트 / 검증 절차를 모두 포함하여 CM 도구 변경의 모든 측면을 문서화합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6
CM-3	변경 관리 제어	패치 업데이트로 인한 변경 사항을 승인 및 기록하는 패치 관리 프로세스가 배포되었습니까? 모든 패치 배포가 수립된 변경 제어 절차를 따릅니까? 모든 패치 배포는 기록되어야 합니다. 경영진은 시스템용으로 개발된 모든 패치를 책임지고 파악하고 있어야 합니다. 패치는 격리된 환경에서 설치 및 테스트한 후 적절한 시점에 설치해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 5 p. A4-A5 FFIEC D&A Booklet (2004) Appendix A: Objective 11 p. A8	검사관은 조직의 내부 패치 관리 프로세스에 AWS 서비스가 포함되는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. Amazon EC2 인스턴스의 구성 및 패치 적용에 대해 문서화된 프로세스: • Amazon 머신 이미지(AMI) • 운영 체제 • 애플리케이션	조직은 사용 중인 AWS 서비스가 설정된 내부 표준 및 절차를 기반으로 패치 및 구성되도록 해야 합니다. AWS 고객이 패치 배포 프로세스에 포함되도록 기여하는 항목 예: • Amazon 머신 이미지(AMI) • 운영 체제 • 애플리케이션	Amazon 스튜어드가 적절한 보안 픽스를 위해 실시하는 패치 배포는 네트워크 및 서비스 결함 수정 유지 관리를 제어합니다. Amazon 스튜어드는 서비스 그룹 릴리스를 배포하기 전에 보안 픽스의 적용성, 유효성 및 심각성을 검토할 책임이 있습니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: MA-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
CM-4	변경 관리 제어	패치 관리 전략은 모든 운영 체제 및 애플리케이션 소프트웨어의 버전 관리를 포함해야 합니다. 모든 소프트웨어 및 OS 버전은 기록해야 하고 최신 릴리스와 비교해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 5 p. A4-A5 FFIEC OPS Booklet(2004) Appendix A: Tier II: A p. A11-A12	검사관은 패치 관리 전략이 AWS 서비스 환경에서 사용되는 모든 운영 체제, Amazon 머신 이미지 및 애플리케이션 소프트웨어의 버전 관리를 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS EC2 인스턴스의 문서화된 구성 표준(골드 이미지): • Amazon 머신 이미지(AMI) • 운영 체제 • 애플리케이션	조직은 AWS에서 실행되는 Amazon 머신 이미지, 운영 체제 및 애플리케이션과 같은 AWS 시스템 및 서비스에 대해 승인된 구성 또는 기준을 개발해야 합니다. 맞춤화된 Amazon 머신 이미지를 생성하는 방법에 대한 자세한 내용은 다음을 참조하십시오. AWS AMI 사용 설명서	모든 AWS 시스템은 전체 네트워크 장치에서 구성 동질성을 유지하기 위해 장치에서 기준 구성을 유지합니다. 프로덕션 장치 또는 환경을 변경하거나 추가 장치를 배포하려면 CM 도구에 CM을 입력하여 승인을 받아야 합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6
CM-5	변경 관리 제어	고객 정보 시스템의 수정이 서비스 공급자의 정보 보안 프로그램과 일관되도록 정책 및 절차를 개발하고 문서화합니다.	FFIEC OT Booklet (2004) Appendix A: Tier II: D p. A10-A11	검사관은 AWS 내 고객 정보와 관련된 정책 및 절차가 조직의 IT 보안 정책에 따라 확보되었는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS에서 호스팅되는 정보 및 데이터 보호 정책과 절차	조직은 AWS 서비스에서 호스팅되는 고객 정보의 취급을 위한 기존 절차를 일관적으로 준수하고 기존 IT 보안 정책과 부합하도록 해야 합니다.	AWS 직원은 전반적인 회사 표준 및 정보 보안에 대한 책임을 확인하는 고용 계약서에 서명해야 합니다. 여기에 고객 정보 공개 프로세스가 포함됩니다. 모든 Amazon 직원은 정보 보호 요건을 포함하는 비밀 유지 계약에 서명합니다. **참조**: ISO/IEC 27001:2005 Control: A.6.1.5 & A.7.1.3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
시스템 개발 수명 주기						
SD-1	시스템 개발 수명 주기	다음과 같이 시스템 취득, 구성 및 유지 보수를 위해 문서화된 정책 및 절차가 있습니까? - 위험 평가 - 적합성 분석 - 테스트 - 시스템 개발 - 시스템 취득 프로세스(소프트웨어 및 하드웨어) - 변경 관리 개요 - 정보 시스템 유지 관리 관행	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC OPS Booklet(2004) Appendix A: Objective 5 p. A4-A5 FFIEC D&A Booklet (2004) Appendix A: Objective 5, Objective 6, Objective 7 p. A3-A6	검사관은 AWS 서비스가 조직의 SDLC 프로세스에 통합되었는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. SDLC 정책 및 절차에 포함되었는지 확인하기 위해, 조직에 의한 AWS 개발 도구의 사용	AWS 개발 도구(예: EC2Config, API 도구 및 명령줄 도구)의 사용을 기록하고 내부에서 개발된 시스템과 동일한 SDLC 프로세스를 따라야 합니다.	AWS 정보 보안 팀은 AWS의 정보 보안을 담당하며 보안 소프트웨어 개발 프로세스의 소유자입니다. 보안 검토를 위한 개발 팀의 역할 및 책임은 InfoSec 보안 검토 정책에 규정되어 있으며 애플리케이션 등록, 애플리케이션 위험 분류 시작, 보안 검토 시작, 아키텍처 검토 및 위협 모델링 참여 및 코드 검토 수행을 포함합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SA-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6
SD-2	시스템 개발 수명 주기	시스템 개발 또는 취득 전에 보안 요구 사항을 평가하기 위한 잘 정의된 절차 및 기준이 있습니까? 시스템 보안 요구 사항이 업계 모범 사례 및 표준과 부합해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: B, C, D, H p. A12-A16, A17-A19	검사관은 개발 시스템이 AWS에서 호스팅되기 전에 보안 요구 사항을 검토하기 위한 절차 및 기준이 잘 정의되어 있는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직의 SDLC 정책 및 절차 2. AWS 서비스의 평가와 관련된 절차 및 다음과의 부합성: AWS 설명서	조직은 다음에 수록된 모범 사례 및 권장 사항을 기반으로 AWS 서비스 사용 및 구성을 위한 절차와 문서화 표준을 정의해야 합니다. AWS 설명서	AWS 정보 보안 팀은 AWS의 정보 보안을 담당하며 보안 소프트웨어 개발 프로세스의 소유자입니다. 보안 검토를 위한 개발 팀의 역할 및 책임은 InfoSec 보안 검토 정책에 규정되어 있으며 애플리케이션 등록, 애플리케이션 위험 분류 시작, 보안 검토 시작, 아키텍처 검토 및 위협 모델링 참여 및 코드 검토 수행을 포함합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SA-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
SD-3	시스템 개발 수명 주기	공식적인 구성 관리 프로그램이 실시 중입니까? 모든 시스템이 프로덕션 환경으로 릴리스되기 전에 충분히 강화됩니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5	검사관은 공식적인 구성 관리 프로그램이 실시 중이고 모든 시스템이 프로덕션 환경으로 릴리스되기 전에 충분히 강화되는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직 내에서 사용 중인 Amazon 머신 이미지(AMI)의 구성 예 2. 로깅, 모니터링, 권한 및 암호화 키 관리를 포함하여 AWS 보안 지침에 따른 AWS 서비스의 구성	조직은 AWS 내에서 사용되는 서비스를 위해 정의된 Amazon 머신 이미지(AMI)를 개발해야 합니다. 맞춤화된 Amazon 머신 이미지를 생성하는 방법에 대한 자세한 내용은 다음을 참조하십시오. AWS AMI 사용 설명서	AWS는 "AWS 구성 관리 정책"이라고 하는, AWS에 적용되는 공식적이고 문서화된 구성 관리 정책을 마련했습니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 6
서비스 공급자 감독						
SPO-1	서비스 공급자 감독	고객 정보를 적절히 보호할 수 있는 서비스 공급자를 선택 및 유지하기 위해 합리적인 절차가 취해집니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: J p. A20 FFIEC OT Booklet (2004) Appendix A: Objective 3 p. A3-A7 FFIEC OT Booklet (2004) Appendix A: Tier II: B, D p. A8-A9, A10-A11	검사관은 고객 정보에 대한 적절한 보호 조치를 유지할 수 있는 서비스 공급자를 선택 및 유지하기 위해 합리적인 절차가 취해지는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 충분한 보안 검토가 실시되는지 확인하기 위해, 조직의 공급업체 관리 및 구매 프로세스 2. 외부 서비스 공급자를 처리하는 IT 위험 관리 정책 및 절차 3. AWS 서비스를 온보딩하는 데 사용되는 평가 문서	조직은 AWS와 같은 외부 서비스 공급자의 사용 시 보안 보호 조치를 평가, 온보딩 및 유지하기 위해 정의된 프로세스를 문서화하고 준수해야 합니다.	AWS는 "AWS 시스템 및 서비스 취득 정책"이라고 하는 공식적이고 문서화된 시스템 취득 계획 정책을 마련했으며 이 정책은 매년 업데이트 및 검토됩니다. AWS 시스템 및 서비스 취득 정책은 내부 AWS 규정 준수 웹 포털을 통해 모든 직원, 공급업체 및 계약업체로 전파됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SA-1 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
SPO-2	서비스 공급자 감독	공급업체/서비스 공급자 관리를 위한 정책 및 절차가 제대로 문서화되어 있습니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4, Objective 5 p. A4-A6 FFIEC OT Booklet (2004) Appendix A: Tier II: D p. A10-A11	검사관은 AWS 서비스 사용이 공급업체/서비스 공급자 관리를 위한 정책 및 절차에서 문서화되어 있는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 공급업체 및 서비스 공급자를 관리하기 위한 조직의 공급업체 관리 정책 및 절차	조직은 AWS와 같은 외부 서비스 공급자를 관리하기 위한 정책 및 절차를 문서화하고 실시해야 합니다. 절차는 조직과 서비스 공급자 간 온보딩, 책임 분담 보안 및 커뮤니케이션을 규정해야 합니다. (예: 인시던트 대응, 재해 복구, 보안 알림 등)	AWS를 위한 취득은 하드웨어 구성 요소 및 COTS(상용 기성품) 소프트웨어입니다. COTS 제품 및/또는 서비스 구매의 경우, 공급업체의 보안 요구 사항 준수 클레임은 문서화하여 기술 평가 단계에서 고려하고 실제로 테스트해야 합니다. 일단 선택된 AWS 구매는 기술/시스템에 대한 공급업체 계약 협상이 다이어그램, 도면 및 설명서는 물론 제품 기술에 고유한 기술, 보안 및 비즈니스 요구 사항을 포함하도록 요구합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SA-4 (1) SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12
SPO-3	서비스 공급자 감독	서비스 공급자가 고객 정보를 임의의 서비스 공급자에게 제공하거나 임의의 서비스 공급자에게 고객 정보에 대한 액세스 권한을 부여하는 경우: a) 서비스 공급자를 선택 시 적절한 실사를 수행합니다. b) 모든 서비스 공급자에게 적절한 정보 보안 프로그램 및 조치를 실시하도록 요구합니다. c) 정기적으로 서비스 공급자를 모니터링하여 고객 정보를 보호하기 위해 적절한 보안 조치를 유지하는지 확인합니다.	FFIEC IS Booklet(2006) Appendix A: Objective 5 p. A5-A6 FFIEC IS Booklet(2006) Appendix A: Tier II: J, M p. A20, A22-A25	검사관은 서비스 공급자가 적절한 실사 표준, 보안 프로그램 관리, 서비스 기능 및 안정성의 모니터링을 준수하도록 요구하는 프로세스가 있는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직의 공급업체 관리 정책 및 절차 2. 서비스 수준 계약 및 실사, 보안 및 모니터링에 대해 정의된 핵심 성능 지표(KPI)	조직은 공급업체 관리 정책 및 절차가 AWS와 같은 외부 서비스 공급자에 대해 적절한 실사 표준, 보안 및 모니터링 프로세스를 정의하도록 해야 합니다. 조직은 서비스 공급자가 준수해야 할 핵심 성능 지표(KPI)와 함께 서비스 수준 계약을 정의해야 하며 서비스 공급자가 정의된 보안 및 모니터링 기대치와 부합한다는 사실을 전파해야 합니다.	AWS는 특정 보안 및 정당한 주의 기준 및/또는 구현 중인 제안된 구성 요소에 적합한 기타 요구 사항을 충족하는 것으로 검증된 구성 요소를 선택하기 위해 합리적 노력을 기울이고 있습니다. 제안된 구성 요소 또는 시스템 향상은 정보 시스템 보안 책임자의 승인하에 정보 보안 팀, 개발 팀 관리자, 해당 서비스 소유자 및 규정 준수 팀에 의해 기술/비즈니스 요구 사항 충족 및 보안 고려 사항이 검토 및 조율됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SA-4 (7) SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
SPO-4	서비스 공급자 감독	조직이 현재 공급업체/서비스 공급자 및 아웃소싱 관계의 인벤토리를 유지합니까?	FFIEC IS Booklet(2006) Appendix A: Objective 1.3, Objective 2.1 p. A1-A2	검사관은 현재 공급업체/서비스 공급자 및 아웃소싱 관계의 인벤토리가 있는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 현재 서비스에 대한 외부 서비스 공급자 및 서비스 수준 계약의 목록	조직은 현재 공급업체/서비스 공급자 및 아웃소싱 관계의 인벤토리를 유지해야 합니다. 특히, AWS 서비스 내에서 서비스 상호작용을 커뮤니케이션 채널과 함께 규정해야 합니다.	AWS는 외부 구성 요소, 서비스 공급자 및 COTS 소프트웨어에 대한 공급업체 및 제조업체 문서 목록을 유지합니다. AWS 기술 담당자는 분석 및 테스트가 가능하도록 충분히 상세하게 시스템 내에서 사용된 보안 제어의 구현 세부 사항 및 하위 시스템 측면에서 정보 시스템의 상위 수준 설계를 설명하는 AWS 고유 문서로 공급업체 및 제조업체 문서를 보완합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SA-5 (3) SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12
SPO-5	서비스 공급자 감독	서비스 공급자에게 다음과 같은 개인정보보호 및 보안 보호 조치를 구현하고 유지하도록 계약을 통해 요구합니까? a) 보안 책임, 제어 및 보고. b) 영향을 받는 시스템 및 데이터와 관련하여 모든 서비스 공급자와 비밀 유지 계약. c) 적절한 평가 및 테스트를 통한 서비스 공급업체 보안에 대한 타사 검토 조항. d) 인시던트 대응 절차.	FFIEC IS Booklet(2006) Appendix A: Objective 5 p. A5-A6 FFIEC OT Booklet (2004) Appendix A: Objective 3 p. A3-A7	검사관은 서비스 공급자가 계약을 통해 다음과 같은 개인정보보호 및 보안 보호 조치를 구현하고 유지해야 하는지 확인해야 합니다. 1. 보안 책임, 제어 및 보고 **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 서비스 공급자 SOC, ISO 및 기타 규정 준수 보고서의 사본 2. 서비스 공급자의 SLA 계약서, NDA 및 기타 데이터 보호 책임 관련 공시	조직은 보안 및 데이터에 대한 책임 분담을 규정하는 서비스 공급자 감독 프로그램을 수립 및/또는 유지해야 합니다.	AWS는 민첩한 취득, 소규모 계약, 잘 알려지고 인정받는 다양한 공급자, 복수의 공급업체, 탄탄한 공급자, 제조업체 또는 제조업체 인증 및 승인 배포 파트너로부터 직접 주문 등 다수의 정의된 원칙을 따르는 확립된 서비스 공급자 프로그램을 준수하고 있습니다. 또한, AWS는 최대한으로 기술을 활용하는 한편 표준 사용 정보 시스템 구성도 따릅니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SA-12 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
비즈니스 연속성 계획						
BCP-1	비즈니스 연속성 계획	목표 및 책임을 명확하게 규정하는 비즈니스 연속성 계획(BCP)이 문서화되어 있습니까? BCP는 엔터프라이즈 수준에서 이루어져야 합니다. BCP는 단지 기술의 복구만이 아니라 비즈니스의 유지, 재개 및 복구에 관한 것이어야 합니다. BCP 사본이 적절한 담당자 및 복구 위치에 배포되었습니까?	FFIEC BCP Booklet(2008) Appendix A: Objective 4.6, Objective 5 p. A6-A7 FFIEC OPS Booklet(2004) Appendix A: Objective 3 p. A3	검사관은 AWS 서비스가 조직 BCP에 포함되어 있는지 점검 및 검토해야 합니다. BCP는 AWS 서비스와 관련하여 다음 영역을 다루어야 합니다. 1. 오프사이트 백업을 위한 AWS 서비스 사용 2. 중간 작업을 위한 AWS 사용 3. AWS BCP 프로세스 지원의 사용(BCP 문서 저장, 통신 등) 4. AWS 서비스를 위한 중간 작업으로 AWS 가용 영역을 사용 5. AWS 중단의 영향 및 대응 전략 **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직 BC 계획의 사본. 2. 사용 중인 AWS 서비스가 제대로 식별 및 포함되었는지 확인 3. 적절한 담당자 및 복구 위치에 배포된 BCP	조직은 조직에서 사용 중인 AWS 서비스를 포함하는 비즈니스 연속성 계획을 수립 및 문서화해야 합니다. 적어도 BCP가 AWS 서비스와 관련하여 다음 영역을 다루어야 합니다. 1. 오프사이트 백업을 위한 AWS 서비스 사용. 2. 중간 작업을 위한 AWS 사용. 3. AWS BCP 프로세스 지원의 사용(BCP 문서 저장, 통신 등). 4. AWS 서비스를 위한 중간 작업으로 AWS 가용 영역을 사용. 5. AWS 중단의 영향 및 대응 전략. 참조: 재해 복구를 위한 Amazon Web Services 사용	AWS는 "AWS 사고 관리 계획 정책"이라고 하는 AWS에 적용되는 공식적이고 문서화된 사고 관리 계획 정책을 마련했습니다. AWS 사고 관리 계획 정책은 내부 AWS 규정 준수 웹 포털을 통해 모든 직원, 공급업체 및 계약업체로 전파됩니다. AWS 규정 준수 팀은 AWS 최고 정보 보안 책임자의 승인을 얻어 매년 이 정책을 검토합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-1 SOC 2 – Section V

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
BCP-2	비즈니스 연속성 계획	사고 관리 계획을 실증하기 위한 비즈니스 영향 분석(BIA) 및 위험 평가가 이루어졌습니까?	FFIEC BCP Booklet(2008) Appendix A: Objective 3 p. A3-A4	검사관은 비즈니스 영향 분석(BIA) 및 위험 평가가 실시되었는지 확인하는 한편 AWS 서비스가 BIA에 포함되었는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. BIA 및/또는 위험 평가 프로세스 및 문서 2. BIA의 결과로 생성되는 위험 요소 처리 계획 3. AWS 서비스와 관련된 BIA에서 파생되는 프로젝트 계획	조직은 적어도 12~18개월 단위로 비즈니스 영향 평가(BIA) 또는 위험 평가를 실시해야 합니다. BIA는 모든 AWS 서비스 사용을 포함해야 합니다. 또한, 식별된 위험을 해결하는 데 필요한 일정, 마일스톤, 리소스와 함께 위험 요소 처리 계획을 수립하고 유지해야 합니다.	Amazon Web Services 사고 관리 계획(CP)은 AWS에서 심각한 서비스 중단 및 저하에 대응하기 위해 사용되는 프로세스 및 절차를 제시합니다. AWS CP는 AWS에 적용됩니다. AWS는 특수화된 AWS 리전으로 구현되기 때문입니다. 또한, AWS는 AWS에 매주 열리는 용량 관리 회의에서 영향 평가를 실시합니다. 이 회의는 IT 서비스 팀의 대표자가 참석하며, 지속적인 운영 및 유지 보수 활동을 포함한 시스템 요구 사항을 충족하기 위한 리소스를 확보하고 할당하도록 보장합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-2 (2) SOC 2 – Section V
BCP-3	비즈니스 연속성 계획	BCP가 다음 요소를 고려합니까? - 인력 - 시설 - 기술(하드웨어, 소프트웨어, 운영 장비) - 통신/네트워크 - 공급업체 및 서비스 공급자 - 유틸리티 - 데이터 및 레코드 - 법률 집행 - 미디어 및 주주 - BCP에서 보안의 역할, 즉 복구 사이트와 컴퓨터 시스템에 대한 물리적 및 논리적 액세스	FFIEC BCP Booklet(2008) Appendix A: Objective 5 p. A6-A7	검사관은 BCP가 조직 운영 및 BC 능력을 지원하는 데 사용되는 AWS 서비스, 인력 및 기술을 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스, 기술 및 책임 분담이 문서화되어 있는지 확인하기 위한 BCP	조직은 현재 사용 중인 AWS 서비스, 기술 및 리전을 BCP에 포함시켜야 합니다. 또한, 조직은 AWS와의 책임 분담과 BCP와 관련된 조직 역할을 문서화해야 합니다.	Amazon Web Services 사고 관리 계획(CP)은 AWS에서 심각한 서비스 중단 및 저하에 대응하기 위해 사용되는 프로세스 및 절차를 제시합니다. 빠르게 성장하는 고객 베이스의 수요를 충족하기 위해 새로운 리소스가 계속해서 온라인으로 투입되므로 AWS는 N+1 중복성 모델을 채택합니다. N+1 중복성은 구성 요소 장애 시 시스템 가용성을 촉진하는 일종의 복원성입니다. 구성 요소(N)는 적어도 하나의 독립적인 백업 구성 요소(+1)를 가집니다. AWS는 액티브-액티브 구성 요소 방식의 N+1 중복성을 채택하므로, 다른 모든 구성 요소가 정상 작동하더라도 백업 구성 요소가 활성 상태를 유지합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-2 (2) SOC 2 – Section V

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
BCP-4	비즈니스 연속성 계획	BCP가 다음과 같은 긴급 준비 및 위기 관리 측면을 포함합니까? - 직원/관리자 비상 연락망 - 특정 긴급 상황에서 취할 조치를 설명 - 백업 사이트를 사용하는 조건을 정의하고 백업 사이트 통보 절차를 지정 - 필요한 사무 공간 및 장비의 소스와 주요 공급업체 목록을 식별(하드웨어/소프트웨어/통신 등). - PR 대변인을 지명	FFIEC BCP Booklet(2008) Appendix A: Objective 5 p. A6-A7	검사관은 BCP가 제어 내에서 규정된 대로 긴급 준비 및 위기 관리 요소를 포함하는지, 이러한 요소가 사용 중인 AWS 서비스를 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 긴급 및 위기 관리 계획 2. 외부 서비스(즉 AWS) 시작을 포함하는 긴급 통신 계획	조직은 인시던트 및/또는 중단에 대응하기 위한 긴급 및 위기 조치 계획을 문서화하고 사용해야 합니다. 계획은 일상적으로 사용하는 AWS 서비스는 물론 백업 복구 프로세스의 일환으로 사용될 수 있는 AWS 서비스도 포함해야 합니다.	Amazon Web Services 사고 관리 계획(CP)은 AWS에서 심각한 서비스 중단 및 저하에 대응하기 위해 사용되는 프로세스 및 절차를 제시합니다. 중단이 기준을 충족하면 TOS 엔지니어가 개입을 시작하고, 그러면 ISCP가 활성화됩니다. TOS 엔지니어는 이벤트 관리 도구(EMT) 시스템을 사용하여 개입을 시작하고 문제 해결 담당자를 호출합니다. TOS 엔지니어가 모든 해결 담당자가 참여하는 컨퍼런스 콜을 시작합니다. TOS 엔지니어가 통화 리더의 역할을 담당합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-2 (2) SOC 2 – Section V
BCP-5	비즈니스 연속성 계획	BCP가 최신 방식으로 유지되고 정기적으로 업데이트되도록 보장하는 적절한 절차가 실시됩니까? 고위 관리자에게 BCP의 개발, 구현, 테스트 및 유지 관리를 감독할 책임이 할당되었습니까?	FFIEC BCP Booklet(2008) Appendix A: Objective 2 p. A3 FFIEC OPS Booklet(2004) Appendix A: Objective 3 p. A3	검사관은 BCP가 유지되도록 보장하는 절차가 실시 중인지, 고위 관리자에게 감독 책임이 할당되었는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. BC 계획 및 BC 계획이 업데이트되었는지, 고위 관리자에게 감독 책임이 할당되었는지 확인 2. BC 계획이 AWS 서비스 사용을 반영하도록 업데이트되었는지 확인	조직은 BC 계획이 최신 상태로 AWS 서비스를 포함하며 정기적으로 업데이트되도록 해야 합니다. 또한, 고위 관리자에게 감독 책임을 할당해야 합니다.	AWS는 "AWS 사고 관리 계획 정책"이라고 하는 AWS에 적용되는 공식적이고 문서화된 사고 관리 계획 정책을 마련했습니다. AWS 사고 관리 계획 정책은 내부 AWS 규정 준수 웹 포털을 통해 모든 직원, 공급업체 및 계약업체로 전파됩니다. AWS 규정 준수 팀은 AWS 최고 정보 보안 책임자의 승인을 얻어 매년 이 정책을 검토합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-1 SOC 2 – Section V

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
BCP-6	비즈니스 연속성 계획	복구 사이트 및 오프사이트 백업 선택 시 지리적 다양성이 고려되었습니까?	FFIEC BCP Booklet(2008) Appendix A: Objective 4 p. A4-A6	검사관은 오프사이트 복구 및 스토리지 기능이 식별되었는지 확인해야 합니다. AWS 서비스의 경우, 검사관은 AWS 가용 영역의 사용을 검토해야 하며 조직이 복구 책임을 이해하는지 확인해야 합니다. 참고: AZ는 다른 AZ에서 장애가 발생할 경우 격리되도록 설계된 개별적인 위치입니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직 AWS 아키텍처 설명서 및 DR 계획	조직은 현재 AWS 리전 및 대응되는 가용 영역(AZ)을 식별해야 합니다. 조직의 자산에 대해 다중 AZ 배포 전략이 사용되었는지 확인합니다. AWS는 고객이 복수의 AZ에서 인스턴스를 구동하여, 단일 AZ 전체에 장애가 발생하더라도 서비스 가용성을 확보할 것을 권장합니다. 또한, 조직의 AWS 아키텍처 문서, DR 계획 및 주요 DR 담당자와의 논의를 검토하여 제안된 재해 시 DR 접근법을 식별하십시오.	AWS는 백업 데이프, 오프사이트 데이터 스토리지, 대체 처리 사이트라는 전통적 모델과는 전혀 다릅니다. AWS는 중복 아키텍처와 결합된 고가용성 컴퓨팅 및 데이터 스토리지를 제공하여 중단의 영향을 축소하도록 새롭게 구축된 서비스입니다. AWS 서비스는 가용 스토리지 및 컴퓨팅 파워를 활용하도록 설계되었습니다. AWS는 복구 모델에 고전적 의미의 대체 스토리지 사이트를 사용하지 않습니다. AWS 내 데이터는 EBS 및 S3 서비스에 의해 자동으로 복수 위치에 저장됩니다. 그러므로 오프사이트 데이터 스토리지는 온라인 스토리지로 구현되고 오프사이트 위치는 단지 또 하나의 활성 AWS 데이터 센터인 것입니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-6 SOC 2 – Section V

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
BCP-7	비즈니스 연속성 계획	BCP 테스트 계획이 연간 테스트 시 모든 중요 사업 부문/부서/기능이 포함되는지 확인합니까? 조직의 규모 및 복잡성을 기준으로 테스트 레벨이 적절한지 결정합니다.	FFIEC BCP Booklet(2008) Appendix A: Objective 10 p. A11-A15	검사관은 BCP 테스트 계획이 모든 서비스를 망라하여 조직 내에서 사용되는 AWS 서비스를 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. BCP 테스트 계획 2. 테스트 결과 보고서 3. AWS 서비스가 계획 및 테스트 보고서에 포함되는지 확인	조직은 테스트 프로세스에 BCP 테스트 계획 및 AWS 서비스가 포함되도록 해야 합니다. 또한, 조직은 단일 또는 다중 AZ 배포 접근법을 사용할지 결정해야 합니다.	AWS BCP 테스트는 두 유형의 실습으로 구성됩니다. 개입 훈련 및 실전 연습. 개입 훈련은 시뮬레이션된 심각도 1 또는 2 이벤트를 선택하여 BCP 절차를 테스트하고 개입을 시작하여 BCP를 활성화합니다. 실전 연습은 매년 실시하는 전체 규모로 작동하는 BCP 테스트입니다. 개입 훈련과 실전 연습의 차이는 후자의 경우 실제 장애를 유발시켜 운영계 부하를 변화시킨다는 점입니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-4 SOC 2 – Section V
BCP-8	비즈니스 연속성 계획	DRP/BCP를 매년 테스트할지 결정합니다.	FFIEC BCP Booklet(2008) Appendix A: Objective 10 p. A11-A15	검사관은 BCP가 적어도 매년 한 번 테스트되는지, AWS 서비스 사용을 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. BCP 테스트 계획 2. 테스트 결과 보고서	조직은 테스트 프로세스에 BCP 테스트 계획 및 AWS 서비스가 포함되도록 해야 합니다. 테스트는 적어도 매년 한 번 실시하고 문서화해야 합니다.	AWS BCP 테스트는 두 유형의 실습으로 구성됩니다. 개입 훈련 및 실전 연습. 개입 훈련은 시뮬레이션된 심각도 1 또는 2 이벤트를 선택하여 BCP 절차를 테스트하고 개입을 시작하여 BCP를 활성화합니다. 실전 연습은 매년 실시하는 전체 규모로 작동하는 BCP 테스트입니다. 개입 훈련과 실전 연습의 차이는 후자의 경우 실제 장애를 유발시켜 프로덕션 부하를 변화시킨다는 점입니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-4 SOC 2 – Section V

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
액세스 관리, 인증 및 권한 부여						
AAA-1	액세스 관리, 인증 및 권한 부여	운영 체제, 네트워크 장치 및 애플리케이션에 대한 액세스를 관리하는 공식 프로세스가 있습니까? 다음의 절차를 포함해야 합니다. a) 새 사용자 만들기 b) 액세스 권한 부여 및 취소 c) 각 사용자에게 부여된 액세스 권한을 모니터링 d) 각 시스템 또는 담당자 변경 시 액세스 권한 업데이트를 실행	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: A p. A8-A12	검사관은 AWS 서비스 및 Amazon EC2 인스턴스에 대한 액세스를 관리하는 내부 정책 및 절차를 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** AWS 액세스 관리 프로세스 1. 고유 AWS 인증 방법 2. 인증 연동 및 기업 Active Directory 연결, 또는 3. LDAP 구현 4. IAM 구성 – IAM 설정 내보내기	조직은 AWS 액세스 제어의 사용 및 구성을 문서화해야 합니다. 예제 및 옵션은 아래에 요약되어 있습니다. 1. Amazon IAM이 액세스 관리에 사용되는 방법 설명 2. Amazon IAM이 관리에 사용되는 제어 목록 - 리소스 관리, 보안 그룹, VPN, 객체 권한 등 3. 고유 AWS 액세스 제어 사용 또는 액세스가 조직의 LDAP 통합을 사용하여 연동된 인증을 통해 관리되는지 여부. 4. AWS 계정 및 역할의 목록. 5. Amazon IAM 계정, 역할 및 모니터링 방식에 대한 설명을 제공. 6. EC2 내 시스템의 설명 및 구성을 제공. 구현 및 모범 사례는 Amazon IAM 설명서를 참조하십시오.	AWS는"AWS 액세스 제어 정책"이라고 하는 공식적이고 문서화된 액세스 제어 정책을 마련했으며, 이 정책은 매년(또는 시스템에 정책에 영향을 주는 대규모 변화가 발생할 때마다) 업데이트 및 검토됩니다. AWS 액세스 제어 정책은 내부 AWS 규정 준수 웹 포털을 통해 모든 직원, 공급업체 및 계약업체로 전파됩니다. AWS 규정 준수 팀은 AWS 최고 정보 보안 책임자의 승인을 얻어 매년 이 정책을 검토합니다. 이 정책은 목적, 범위, 역할, 책임 및 경영진의 책임감을 규정합니다. AWS 액세스 관리와 관련된 추가 리소스 및 보고서는 다음 링크를 참조하십시오. AWS 규정 준수 요청 **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AC-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
AAA-2	액세스 관리, 인증 및 권한 부여	사용자 및 시스템 리소스에는 최소 권한 원칙과 필요한 업무에 따라 '알아야 할 정보' 원칙에 따라 권한이 부여됩니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: A p. A8-A12	검사관은 AWS 서비스와 관련하여 조직 내에서 사용되는 액세스 제어 유형을 검토해야 합니다. **연동된 액세스 제어:** 연동 인증이 사용되는 경우 검사관은 메커니즘이 내부 역할 할당을 적절한 AWS 권한으로 적용하는지 확인해야 하며 액세스 레벨을 부여하는 프로세스와 방식을 이해하여, 최소 권한 모델이 구현되었는지 확인해야 합니다. **고유 AWS 액세스 제어:** 검사관은 Amazon IAM 역할 및 사용자 할당을 기능적인 역할 및 책임과 비교해야 합니다. 이러한 자격 증명이 제한적 권한만 배정하도록 임시 자격 증명도 고려해야 합니다. **인스턴스 액세스 제어:** Amazon EC2 인스턴스의 경우, 검사관은 조직이 EC2 가상 머신에 대한 액세스를 관리하기 위해 설정한 연동 및/또는 로컬 운영 체제 액세스 제어 메커니즘을 기반으로 구현된 역할 및 할당을 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. Amazon IAM 계정 계획 2. Amazon IAM 설정	조직은 사용되는 액세스 관리, 역할 및 그룹의 유형을 문서화해야 합니다. 3. Amazon IAM을 사용하여 관리하는 제어 목록 – 리소스 관리, 4. AWS 계정 및 역할의 목록. 5. 최소 권한을 설정 및 유지하는 프로세스를 제공. 6. EC2 환경 애플리케이션 제어로부터 정보를 제공. Amazon IAM 계정은 직접 또는 연동을 통해 권한 관리 프로세스와 통합되어야 합니다. Amazon IAM 설명서를 참조하십시오.	AWS는"AWS 액세스 제어 정책"이라고 하는 공식적이고 문서화된 액세스 제어 정책을 마련했으며, 이 정책은 매년(또는 시스템에 정책에 영향을 주는 대규모 변화가 발생할 때마다) 업데이트 및 검토됩니다. 모든 AWS 시스템 계정은 최소 권한 원칙에 따라 최소 액세스가 제공됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AC-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
AAA-3	액세스 관리, 인증 및 권한 부여	부여된 액세스 권한의 레코드가 중앙 위치에 보관됩니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: M p. A22-A25	검사관은 AWS 서비스 및 Amazon EC2 인스턴스에 대한 액세스를 부여한 레코드를 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스 프로비저닝과 관련된 액세스 요청 2. 요청이 기록된 AWS API 이벤트와 일치해야 함 – AWS CloudTrail	Amazon IAM 계정은 직접 또는 연동 및 EC2 상주 제어를 통해 권한 관리 프로세스와 통합되어야 합니다. 조직은 사용자에게 부여된 모든 액세스를 적절히 문서화하고 보존하도록 프로세스를 개발 또는 확장해야 합니다.	사용자 계정은 Amazon 인사 관리 시스템(HRMS) 내 온보딩 워크플로 프로세스의 일부로 설정됩니다. 사용자 계정이 필요한 모든 직원, 공급업체 및 계약업체는 반드시 Amazon HRMS를 통해 온보딩되어야 합니다. 온보딩 워크플로의 일부로, 직원의 직속 관리자, 공급업체 또는 계약업체가 사용자 계정의 설정을 요청합니다. 승인된 요청은 사용자 계정 설정을 승인하는 역할을 합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AC-6 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7 & 10
AAA-4	액세스 관리, 인증 및 권한 부여	사용자 이름, 암호와 같은 적절한 인증 프로세스가 네트워크, 운영 체제, 네트워크 장치 및 애플리케이션에 대한 액세스를 제한하고 있습니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: A p. A8-A12 FFIEC AUD Booklet(2012) Appendix A: Tier	검사관은 AWS 서비스와 관련하여 조직 내에서 사용되는 액세스 제어 유형을 검토해야 합니다. 또한, 사용자 계정 정책 및 암호 복잡성을 검토하고 이들이 AWS 서비스까지 확장되는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 액세스 관리 정책 및 절차 2. Amazon IAM 설정	조직은 EC2 인스턴스와 EC2 환경 내 서비스(예: RDS)에 대한 액세스 제어를 구현 및 유지해야 합니다. 독립형 시스템과 마찬가지로, 이러한 가상 시스템도 로컬 계정을 사용하여 또는 액세스 제어 관리를 위한 디렉터리 서비스와 연결하는 방식으로 액세스 제어를 구현 및 유지해야 합니다.	AWS는 "AWS 액세스 제어 정책"이라고 하는 공식적이고 문서화된 액세스 제어 정책을 마련했습니다. 시스템 계정은 Amazon의 셀프 서비스 계정 생성 도구를 사용하여 요청을 제출하는 것으로 설정됩니다. 이 도구를 사용하여, 고유 계정 이름, 계정 설명, 계정 소유자, 계정 생성 근거를 포함한 필수 필드. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AC-6 PCI DSS v3.0 Requirement 8

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
AAA-5	액세스 관리, 인증 및 권한 부여	조직이 코어 시스템 등에 대한 원격 액세스, 비콘솔 액세스, 관리자 액세스와 같이 위험이 그 필요성을 입증하는 모든 중요 시스템, 서비스 및 애플리케이션에서 멀티 팩터 인증을 구현했습니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5	검사관은 AWS 서비스와 관련하여 조직 내에서 사용되는 액세스 제어 유형을 검토해야 합니다. **참고: 고유 AWS 액세스 제어:** 금융 기관이 AWS 고유 보안 기능을 사용하는 경우 검사관은 다음 단계를 수행해야 합니다. 경영진 승인 및 새 사용자 액세스 부여 프로세스와 관련된 문서를 식별합니다. 1. AWS 관리 또는 명령줄 액세스 사용자의 샘플을 선택 2. 할당된 액세스에 대한 공식적 경영진 승인의 증거를 검토 **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 관리 콘솔에 액세스하는 사용자를 관찰하여 멀티 팩터 인증이 활성화된 사용자의 샘플 및 토큰(가상 또는 물리적)이 요청되었는지 여부를 확인 2. Amazon EC2 인스턴스의 경우 검사관은 물리적 시스템의 경우와 비슷한 방식으로 멀티 팩터 인증 메커니즘을 검토	AWS 서비스를 관리하기 위해 새 사용자에게 액세스를 할당하는 공식 프로세스를 개발해야 합니다. 여기에는 요청, 경영진 승인 및 경영진 합의 액세스에 따라 부여된 액세스의 증거가 포함되어야 합니다. 고객은 각 사용자에게 고유한 암호를 할당해야 하며 멀티 팩터 인증 디바이스를 활성화해야 합니다. 이 작업은 IAM 서비스를 사용하여 다음 단계를 따라 수행할 수 있습니다. 1. IAM 서비스를 엽니다. 2. 각 사용자에 대해 사용자 계정을 선택하고 “보안 자격 증명”을 선택합니다. 1. 각 사용자에 대해 암호 및 멀티 팩터 인증 디바이스가 활성화되어 있는지 확인합니다. 명령줄 및 API 액세스의 경우, 활성 액세스 키 및 로그인 인증서가 활성화되어 있어야 합니다. AWS Management Console, API 및 명령줄 도구는 작업을 수행하기 위해 암호화된 연결을 필요로 하며 변경이 불가합니다. MFA에 대한 자세한 내용은 다음을 참조하십시오. 멀티 팩터 인증	AWS 관리자는 RSA 개인키 및 암호를 사용하여 네트워크 중계 호스트와의 SSH 연결을 인증한 후 TACACS를 사용하여 LDAP 사용자 ID 및 암호로 사용자를 인증하는 네트워크 장치로 로그인합니다. 권한 있는(루트) 명령의 경우, 사용자가 인증된 암호를 사용하여 권한을 에스컬레이션해야 합니다. 권한 명령 에스컬레이션은 모두 감시됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IA-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 8

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
AAA-6	액세스 관리, 인증 및 권한 부여	조직이 공유 IT 리소스 액세스에 고유한 사용자 ID를 적용합니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: A p. A8-A12	검사관은 IAM 내 계정 목록을 검토해야 하며 모든 사용자가 고유한 사용자 계정을 사용해야 하는지, AWS 환경에 액세스하는 공유 계정이 없는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 구성된 사용자 ID 및 액세스 구성의 목록	AWS 관리 콘솔 기능, AWS 서비스, 그리고 EC2, RDS, S3 또는 기타 서비스 안에 저장된 인스턴스 및 데이터에 액세스하려면 고유한 사용자 계정을 사용해야 합니다. 연동 환경에서는, 조직의 LDAP 구현에서 고유한 계정을 할당하고, 오직 개별적으로 할당된 그 계정에만 AWS 권한을 부여함으로써 이를 달성할 수 있습니다. IAM 내에서는 조직이 액세스가 필요한 각 개인에게 고유한 사용자 계정을 생성하고 각 계정에 적절한 권한을 부여할 수 있습니다.	AWS는 "AWS 액세스 제어 정책"이라고 하는 공식적이고 문서화된 액세스 제어 정책을 마련했습니다. 시스템 계정은 Amazon의 셀프 서비스 계정 생성 도구를 사용하여 요청을 제출하는 것으로 설정됩니다. 이 도구를 사용하여, 고유 계정 이름, 계정 설명, 계정 소유자, 계정 생성 근거를 포함한 필수 필드. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AC-6 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7
AAA-7	액세스 관리, 인증 및 권한 부여	조직이 최소 8자, 암호 복잡성, 42일 주기 로테이션 등 강력한 암호 요건을 적용합니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: A p. A8-A12 FFIEC EB Booklet (2003) Appendix A: Objective 4.5 p. A11-A12	검사관은 AWS 서비스 및 Amazon EC2 인스턴스에 대한 강력한 암호를 적용하는 내부 정책 및 절차를 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 암호 정책을 적용하는 프로세스는 AWS 관리 기능 및 Amazon EC2 인스턴스에 대한 액세스를 포함	조직은 강력한 암호 요건을 정의하고 이 요건을 AWS 서비스까지 확장해야 합니다. Amazon IAM이 복잡성, 로테이션 또는 만료에 대한 암호 요건을 적용할 수 없는 고객은 추가 제어를 구현해야 하며, 이러한 계정에 대해서는 Amazon IAM 멀티 팩터 인증이 활성화되어야 합니다. EC2 인스턴스와 EC2 환경 내 서비스(예: RDS)에 대한 액세스 제어를 구현하고 유지합니다. 독립형 시스템과 마찬가지로, 이러한 가상 시스템에도 암호 제어를 적용하기 위한 액세스 제어를 구현하고 유지해야 합니다.	AWS는 사용자가 암호를 변경할 때 사용하는 AWS 암호 도구를 통해 AWS LDAP에 암호 복잡성을 적용하고 있습니다. 이 도구는 암호에서 다음을 요구합니다. 1. 대/소문자 구별 2. 길이가 8~30자이고 하나 이상의 대문자, 하나 이상의 소문자, 그리고 처음과 마지막을 제외한 자리에 하나 이상의 비영문자 문자를 포함해야 합니다. 3. 사용자가 이전에 사용한 암호를 다시 사용할 수 없음 **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IA-5 SOC 2 – 'Security Procedures' Criteria 3.2 PCI DSS v3.0 Requirement 8

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
네트워크 제어						
NW-1	네트워크 제어	통신 인프라가 중복성을 고려하여 설계되었습니까? 단일 장애 지점은 정밀 조사하여 제거해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 8 p. A6-A7	검사관은 AWS 서비스 연결 및 사용을 포함하여 전체 인프라를 검토해야 합니다. AWS는 가용 영역, 중복 Direct Connect 또는 Amazon EC2 VPN과 같은 중복성 기능을 제공합니다. 검사관은 단일 장애 지점을 제거하기 위한 이들 기능의 구현을 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. ECS 내 Amazon EC2 인스턴스 및 서비스(예: Amazon RDS)의 구성에서 중복성 여부	조직은 인프라 중복성 요구 사항을 검토해야 하며 단일 장애 지점을 방지하도록 AWS 서비스 사용을 검토해야 합니다. 대부분의 AWS 서비스는 가용 영역을 사용한 가용성 옵션을 제공합니다. 각 서비스는 포괄적 중복성 설계를 제공하는 것으로 간주되어야 합니다. 또한, AWS 서비스는 시스템의 기본 사이트로 현재 사용 중인 다른 인프라를 위한 중복성도 제공합니다.	AWS는 n+1 중복성 모델을 채택합니다. N+1 중복성은 구성 요소 장애 시 시스템 가용성을 보장하는 일종의 복원성입니다. 구성 요소(N)는 적어도 하나의 독립적인 백업 구성 요소(+1)를 가집니다. AWS는 액티브-액티브 구성 요소 방식의 N+1 중복성을 채택하므로, 다른 모든 구성 요소가 정상 작동하더라도 백업 구성 요소가 활성 상태를 유지합니다. 이는 네트워크 및 데이터 센터 구현을 비롯해 AWS 전반에 걸쳐 적용됩니다. 데이터 센터 네트워크 인바운드/아웃바운드는 대체 서비스 공급자를 사용한 다양한 경로로 설계됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-2 SOC 2 – Section III, Area C
NW-2	네트워크 제어	논리적 도메인 및 네트워크 세그먼트 구분이 사용자, 네트워크 서버, 애플리케이션 및 데이터를 별도의 보안 도메인으로 그룹화하는 데 사용됩니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14 FFIEC AUD Booklet(2012) Appendix A: Tier II: D A13-A14	검사관은 AWS 보안 그룹 구현, AWS Direct Connect 및 Amazon VPN 구성을 검토해야 합니다. AWS는 인스턴스 격리를 위한 내부 제어 기능을 제공하며, 이 제어 기능은 AWS 보안 그룹 사용을 통해 유지됩니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. Amazon EC2 및 기타 AWS 서비스와 연결하는 물리적 장치 및 시스템에 대한 세그먼트 구분 제어	AWS는 고객이 네트워크 세그먼트 구분을 설명하고 구현할 수 있도록 구성 가능한 보안 그룹을 제공합니다. VPC와 같은 추가 옵션을 사용하여 시스템 영역을 더 확실하게 지정하여 민감한 고객 정보를 관리할 수 있는 프라이빗 클라우드 환경을 제공할 수 있습니다.	AWS 액세스 제어 정책은 AWS가 액세스 제어 정책(예: 자격 증명 기반 정책, 역할 기반 정책, 규칙 기반 정책) 및 관련 액세스 적용 메커니즘(예: 액세스 제어 목록, 엑세스 제어 매트릭스, 암호화 기법)을 사용하여 정보 시스템에서 사용자(또는 사용자를 대리하는 프로세스)와 객체(예: 장치, 파일, 레코드, 프로세스, 프로그램, 도메인) 간 액세스를 제어하도록 규정하고 있습니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
NW-3	네트워크 제어	각 보안 도메인 내부 또는 보안 도메인 사이에서 작업을 제한하기 위해 ACL, 방화벽과 같은 액세스 제어가 사용됩니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14	검사관은 AWS 보안 그룹 규칙, AWS Direct Connect 및 Amazon VPN 구성을 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스를 위한 ACL 및 방화벽 설정	조직은 AWS 보안 그룹을 사용하여 네트워크 세그먼트 구분 및 ACL을 설명하고 구현해야 합니다. AWS Direct Connect 또는 VPC VPN을 사용하는 경우 온프레미스 장치에 대해 세그먼트 구분이 적절히 구성되었는지 확인하십시오. 참조: AWS 보안 그룹	시스템 경계 내부의 시스템과 장치는 필요에 따라 별도의 보관실로 분할됩니다. 서버와 네트워크 장치는 시스템 경계 내부의 시스템 및 장치에 대해 전원, HVAC 및 기타 환경 지원을 제공하는 장치를 포함하는 보관실로부터 물리적으로 분할된 서버 및 네트워킹 보관실에 설치됩니다. 또한, AWS는 내부 네트워크를 2개의 구별되는 네트워크 패브릭, PROD 및 EC2로 분할했습니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SC-32 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
NW-4	네트워크 제어	IT 관리는 로컬 보안 제어에 대해 (최소한) 예방, 탐지 및 교정 전략을 포함하는 계층화된 접근법을 구현해야 합니다. 이는 액세스 제어, 기록 및 모니터링 제어, 인시던트 대응 제어를 포함할 수 있습니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 5 A4-A5 FFIEC AUD Booklet(2012) Appendix A: Tier II: D A13-A14	검사관은 AWS Direct Connect 및 Amazon VPN 구성을 검토해야 합니다. AWS는 또한 AWS CloudWatch, Describe API 등의 모니터링 서비스도 제공합니다. 이러한 서비스가 사용되는 경우 검사관이 논리적 보안을 위한 이들 서비스의 사용을 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. Amazon EC2 및 기타 AWS 서비스와 연결하는 조직 및 시스템에서 호스팅하는 물리적 장치를 위한 기록, 모니터링 및 알림 2. 기록된 AWS API 이벤트 – AWS CloudTrail	조직이 모든 보안 관련 이벤트를 식별하기 위해서는 EC2 인스턴스에 대해 적절한 기록 및 모니터링을 설정해야 합니다. AWS가 AWS 관리 환경을 위해 다양한 계층화된 보안 제어를 관리하지만 조직은 계층화된 접근법이 올바로 구현되도록 구성, 할당된 액세스, AWS 보안 그룹 및 EC2 인스턴스에서 적절한 제어를 구현해야 합니다. 참조: • 서비스 액세스 로깅 • AWS CloudTrail • AWS Config	AWS는 AWS 모니터링 도구가 AWS 서비스 및 보안 팀에서 결정한 임계값 경보 메커니즘을 기초로 위반 또는 잠재적 위반 발생의 징후를 표시하면 거의 실시간으로 알림을 제공합니다. AWS 모니터링은 방화벽, 게이트웨이, 라우터 같은 장치를 포함합니다. 모니터링 도구는 모두 실시간에 가까운 알림을 제공합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SI-4 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1, 10, & 11

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
NW-5	네트워크 제어	네트워크 및 시스템을 유지 관리하는 담당자의 일상 활동은 서면 절차로 관리됩니다.	FFIEC AUD Booklet(2012) Appendix A: Tier II: D A13-A14	검사관은 작업자의 일상 활동을 관리하는 절차가 AWS 관리 기능 및 Amazon EC2 인스턴스를 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스를 포함하기 위해, 일상적 네트워크 및 시스템 작업을 위한 절차	조직은 작업자의 일상 활동을 관리하는 절차에 AWS 관리 기능과 Amazon EC2 인스턴스를 포함시켜야 합니다.	AWS는 "AWS 유지 관리 계획"이라고 하는 공식적이고 문서화된 시스템 유지 관리 정책을 마련했으며, 이 정책은 매년 업데이트 및 검토됩니다. AWS 유지 관리 정책은 내부 AWS 규정 준수 웹 포털을 통해 모든 직원, 공급업체 및 계약업체로 전파됩니다. 이 정책은 목적, 범위, 역할, 책임 및 경영진의 책임감을 규정합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: MA-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
NW-6	네트워크 제어	직원, 공급업체 또는 기타 사용자를 위해 네트워크에 대한 원격, 인터넷 또는 VPN 액세스를 배포하려면 적절한 승인이 필요합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14 FFIEC AUD Booklet(2012) Appendix A: Tier II: D A13-A14	검사관은 조직 내부에서 서비스를 배포하기 위한 절차를 실시 중인지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 직원, 공급업체 또는 기타 사용자에게 원격 액세스를 승인하는 절차, 그리고 AWS 서비스 및 Amazon EC2 인스턴스에 대한 액세스를 포함하는지 확인	조직은 직원에게 원격, 인터넷 또는 VPN 액세스를 부여하기 위한 절차를 개발해야 하며, EC2 네트워크 및 시스템에 대한 AWS 콘솔 액세스 및 원격 액세스를 포함하도록 절차를 확장해야 합니다.	시스템 경계 내부의 시스템 및 장치에 대한 구성 제어 액세스는 승인이 필요합니다. 시스템 경계 내부의 시스템 및 장치에 배포된 모든 변경은 적어도 두 번의 승인이 필요합니다. 이러한 승인에는 승인자의 보안 영향 분석에 대한 명시적 고려가 내재되어 있습니다. 승인자는 변경과 관련된 CM 티켓 안에 승인을 표시합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1 & 6

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
운영 체제 액세스						
OS-1	운영 체제 액세스	조직이 모든 운영 체제 유틸리티 및 구성 관리에 대한 액세스를 지정된 시스템 관리자로 제한합니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: C p. A15-A16 FFIEC AUD Booklet(2012) Appendix A: Tier II: D A13-A14	검사관은 AWS 서비스 및 Amazon EC2 인스턴스에 대한 액세스를 지정된 관리자로 제한하는 내부 정책 및 절차를 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 운영 체제 유틸리티 및 구성 관리에 대한 액세스를 제한하는 절차가 AWS 관리 기능 및 Amazon EC2 인스턴스에 대한 액세스를 포함	조직은 AWS 콘솔 및 관리 액세스를 관리자 액세스로 간주해야 하며, 관리 콘솔의 다양한 기능에 대한 액세스는 지정된 시스템 관리자로 제한해야 합니다. EC2 인스턴스는 현재 조직에서 관리하는 다른 모든 운영 체제와 동일하게 취급해야 합니다. 운영 체제가 EC2 인스턴스의 시스템 유틸리티 및 구성 관리에 대한 액세스를 관리자로 제한해야 합니다.	AWS는 인프라 구성 요소 전체에 걸쳐 최소 권한을 구현합니다. 네트워크 장치 및 서버는 최소 기능으로 구현되어 있으며, 서비스 팀이 장치가 기능을 발휘하는 데 필요한 소프트웨어 패키지와 서비스만 추가합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7
OS-2	운영 체제 액세스	조직이 모든 권한 있는 또는 관리자 액세스를 제한하고 모니터링합니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: A p. A8-A12 FFIEC AUD Booklet(2012) Appendix A: Tier II: D A13-A14	검사관은 AWS 서비스 및 Amazon EC2 인스턴스에 대한 권한 있는 액세스를 지정된 관리자로 제한 및 모니터링하는 내부 정책 및 절차를 검토해야 합니다. AWS는 또한 AWS CloudWatch, Describe API 등의 모니터링 서비스도 제공합니다. 이러한 서비스가 사용되는 경우 검사관이 논리적 보안을 위한 이들 서비스의 사용을 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 액세스 관리 관련 정책 및 절차 2. Amazon EC2 인스턴스에 대한 기록, 모니터링 및 알림	조직은 Amazon IAM을 사용하여 AWS 서비스 구성에 대해 권한을 가진 액세스를 제한해야 합니다. AWS는 AWS 콘솔에 대한 액세스를 기록 및 모니터링하지만 관리자 활동을 모니터링하기 위한 관리자 로그에 액세스하기 위한 인터페이스는 제공하지 않습니다. 서비스 구성 변경을 주기적으로 모니터링하기 위한 프로세스가 수립되어야 합니다.	액세스 및 권한 있는 명령 감사 로그(authpriv): AWS Linux 시스템에 의해 생성되는 authpriv 로그는, 자동화 및 대화식 로그인과 그리고 실행한 권한 있는 모든 명령을 모두 시스템에 기록합니다. 적어도 매주 한 번, AWS 보안 팀이 이러한 액세스에 관련된 모든 로그 메시지를 추출하여 호스트 클래스별로 AWS CISO 및 VP에 보고합니다. 프로덕션 서버와 상호작용은 업무상 필요가 있는 직원이 업무를 수행할 때만 그렇게 해야 합니다. 특히 로그 분석이 이벤트를 검색합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AU-6 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7, 10, & 11

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
OS-3	운영 체제 액세스	조직은 모든 운영 체제 파라미터에 대한 액세스를 제한해야 합니다. 즉, 업무상 필요가 없는 한 일반 사용자에게 로컬 관리자 권한을 부여하면 안 됩니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: A p. A8-A12	검사관은 내부 정책 및 절차에서 AWS 서비스 및 Amazon EC2 인스턴스 접근이 지정된 관리자로 제한하고 있는지를 검토해야 합니다. AWS 콘솔 및 관리 API는 물리적 시스템, 운영 체제 및 애플리케이션과 동일한 기능 및 민감도를 가집니다. Amazon EC2 인스턴스는 물리적 서버와 동일한 것으로 간주해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 운영 체제 파라미터에 대한 액세스를 제한하는 절차가 AWS 관리 기능 및 Amazon EC2 인스턴스에 대한 액세스를 포함	조직은 모든 AWS 콘솔 및 관리 액세스를 관리자 액세스로 취급해야 하며, 관리 콘솔의 다양한 기능에 대한 액세스는 지정된 시스템 관리자로 제한해야 합니다.	AWS는 인프라 구성 요소 전체에 걸쳐 최소 권한을 구현합니다. 네트워크 장치 및 서버는 최소 기능으로 구현되어 있으며, 서비스 팀은 장치가 기능 수행에 필요한 소프트웨어 패키지와 서비스만 추가합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7
OS-4	운영 체제 액세스	운영 및 애플리케이션 시스템에 대해 비인가된 접근 시도가 독립된 담당자에 의해서 기록, 모니터링 및 대응됩니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: A, B p. A8-A14 FFIEC OPS Booklet(2004) Appendix A: Tier II: F p. A14-A15	검사관은 AWS 서비스에 대한 액세스 시도를 모니터링하는 내부 정책 및 절차를 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 비인가 접근 시도에 대한 기록 및 경고를 하도록 시스템이 구성되어 있는지 확인할 수 있는 EC2 인스턴스의 구성	조직은 Amazon IAM을 사용하여 AWS 서비스 구성에 대한 액세스를 제한해야 합니다. AWS는 AWS 콘솔에 대한 액세스를 기록 및 모니터링하지만 비인가 접근 시도를 모니터링하기 위한 로그에 액세스하기 위한 인터페이스는 제공하지 않습니다.	AWS 관리자가 시도하는 배스천 호스트에 대한 액세스는 모두 기록되며, 보안 팀이 이 로그에서 비인가된 시도 또는 의심스러운 활동을 검토합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 10 & 11
OS-5	운영 체제 액세스	모든 운영 체제에서 시스템 활동을 기록하도록 평가 이벤트가 활성화되어 있습니까?	FFIEC OPS Booklet(2004) Appendix A: Tier II: B, F p. A12, A14-A15 FFIEC AUD Booklet(2012) Appendix A: Tier II: D p. A13-A15	검사관은 조직에서 사용 중인 Amazon EC2 인스턴스를 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 운영 체제 구성 검토를 통해서 모든 운영 체계 파라메터에 대한 평가 이벤트의 기록이 구현되어 있는지 확인	조직은 Amazon IAM을 사용하여 AWS 서비스 구성에 대한 액세스를 제한해야 합니다. AWS는 AWS 콘솔에 대한 액세스를 기록 및 모니터링하지만 비인가 접근 시도를 모니터링하기 위한 로그에 액세스하기 위한 인터페이스는 제공하지 않습니다.	AWS는 인프라 구성 요소 전체에 걸쳐 최소 권한을 구현합니다. 네트워크 장치 및 서버는 최소 기능으로 구현되어 있으며, 서비스 팀은 장치가 기능 수행에 필요한 소프트웨어 패키지와 서비스만 추가합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 10

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
애플리케이션 액세스 제어						
AP-1	애플리케이션 액세스 제어	애플리케이션에 대한 인증 및 인증 방법은 애플리케이션의 위험에 따라 충분히 복잡해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Tier II: G p. A17	검사관은 물리적 시스템의 경우와 비슷한 방식으로 Amazon EC2 인스턴스에서 구현된 애플리케이션에 대한 인증 및 권한 방법을 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스에서 애플리케이션 수준 액세스를 포함하는 액세스 관리 정책 및 절차	조직은 API 및 AWS 소프트웨어 개발 키트를 통해 어느 애플리케이션 또는 시스템 프로세스가 AWS 서비스에 액세스할지 결정해야 합니다. 애플리케이션 또는 시스템 프로세스가 AWS 리소스에 액세스해야 할 경우 액세스가 정책에 따라서 안전하게 제공되고, 관련 사항을 문서화해야합니다. 세 유형의 액세스 자격 증명은 다음과 같습니다. 1. 대칭 암호키에 대한 서명 (REST/Query API 접근 및 타사 도구를 이용하는 경우) 2. X.509 인증서 및 해당 비밀키 (SOAP API 및 명령줄을 통해 액세스할 경우) 3. 멀티 팩터 인증(옵션)	애플리케이션 액세스 제어는 전적으로 고객의 책임입니다.
AP-2	애플리케이션 액세스 제어	애플리케이션 액세스 제어가 "최소 권한" 및 "알아야 할 정보"를 기반으로 합니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: A p. A8-A12	검사관은 물리적 시스템의 경우와 비슷한 방식으로 Amazon EC2 인스턴스에서 구현된 애플리케이션 액세스 제어를 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스에서 애플리케이션 수준 액세스를 포함하는 액세스 관리 정책 및 절차 2. RDS 데이터베이스에 대한 권한 구성	조직은 EC2 인스턴스에서 구현된 애플리케이션에 대해 해당 애플리케이션의 위험과 조직 사용자의 요구 사항에 적합한 액세스 제어를 구현하고 유지해야 합니다. 이러한 제어는 조직의 기존 액세스 제어 프로세스에 통합하여 관리해야 합니다.	애플리케이션 액세스 제어는 전적으로 고객의 책임입니다.

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
AP-3	애플리케이션 액세스 제어	모든 액세스 및 보안 이벤트를 기록할 수 있도록 애플리케이션에서 평가 이벤트가 활성화되어 있습니까?	FFIEC OPS Booklet(2004) Appendix A: Tier II: G p. A17 FFIEC OPS Booklet(2004) Appendix A: Tier II: B, F p. A12, A14-A15	검사관은 Amazon EC2 인스턴스에서 구현된 애플리케이션에 대한 평가 이벤트 로깅을 물리적 시스템의 경우와 비슷한 방식으로 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스 내부에서의 애플리케이션 수준 액세스를 포함시키기는 이벤트 로깅 정책 및 절차 2. RDS 데이터베이스 로깅	조직은 EC2 인스턴스에서 구현된 애플리케이션에 대한 애플리케이션 로깅에 대한 설명을 제공해야 합니다.	애플리케이션 액세스 제어는 전적으로 고객의 책임입니다.
AP-4	애플리케이션 액세스 제어	각 애플리케이션 프로세스에 할당된 기업 소유자/사업부 관리자가 해당 애플리케이션에 액세스할 수 있는 사용자 및 데이터 소비자에 대한 최종 결정권을 소유합니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: G p. A17	검사관은 애플리케이션 액세스를 관리하는 내부 정책 및 절차가 AWS 서비스 및 Amazon EC2 인스턴스를 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 및 RDS 데이터베이스 내에서 호스팅되는 애플리케이션 액세스에 대한 정책 및 절차	조직은 AWS 서비스 내에서 호스팅되는 애플리케이션의 애플리케이션 액세스 및 소유권을 문서화해야 합니다.	애플리케이션 액세스 제어는 전적으로 고객의 책임입니다.
AP-5	애플리케이션 액세스 제어	기업 소유자가 본인 소유의 모든 애플리케이션에 대한 액세스 권한을 정기적으로 검토합니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5	검사관은 애플리케이션 액세스를 관리하는 내부 정책 및 절차가 Amazon EC2 인스턴스 내에서 호스팅되는 AWS 서비스 및 애플리케이션을 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 내에서 호스팅되는 애플리케이션 액세스에 대한 정책 및 절차	조직은 EC2 인스턴스에서 애플리케이션에 대한 사용자 및 권한을 보장해야 하고 일반 액세스 제어 프로세스와 통합해야 합니다.	애플리케이션 액세스 제어는 전적으로 고객의 책임입니다.

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
데이터베이스 보안 제어						
DC-1	데이터베이스 보안 제어	데이터베이스 관리 액세스 및 데이터 수정 활동이 기록되고 면밀히 모니터링됩니까? 이 로그들은 데이터베이스 관리 그룹의 어떤 멤버도 변경해서는 안 됩니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 10 p. A8-A9 FFIEC OPS Booklet(2004) Appendix A: Tier II: F p. A14-A15	검사관은 내부 시스템의 경우와 비슷한 방식으로 Amazon RDS 또는 클라이언트 데이터베이스에 대한 액세스 및 데이터 수정 활동을 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스 사용까지 확장될 수 있는 데이터베이스 관리 정책 및 절차	조직은 Amazon IAM을 사용하여 AWS 데이터베이스 구성에 대한 액세스를 제한해야 합니다. 물리적 시스템과 마찬가지로, 시스템이 특정 활동을 기록하고 알리도록 구성하여 AWS 환경 내의 데이터베이스에 대한 관리 액세스를 모니터링하기 위한 제어를 구현하고 유지해야 합니다.	AWS 관리자는 암호 도구를 사용하여 RSA 퍼블릭 키와 시스템 계정을 연결합니다. 이 퍼블릭 키는 사용자가 관리 권한이 있는 호스트 클래스의 모든 호스트에 전파됩니다. 이를 통해서 관리자는 자신의 사용자 ID와 프라이빗 키를 이용해서 호스트에 SSH 접속을 할 수 있습니다. 프라이빗 키는 사용자가 passphrase를 이용해서 보호합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AC-17 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 3
DC-2	데이터베이스 보안 제어	프로덕션 데이터가 테스트 환경에서 사용되는 경우 데이터 보안 제어가 프로덕션 환경과 동일한 강도여야 합니다. 그렇지 않을 경우, 관리자가 프로덕션 데이터를 테스트 환경에서 암호화하여 데이터 민감도를 보호해야 합니다.	FFIEC D&A Booklet (2004) Appendix A: Objective 9 p. A6-A7	검사관은 AWS 데이터베이스 서비스를 사용하는 테스트 환경에서 프로덕션 데이터가 사용되는지 여부를 확인해야 하며, 테스트 데이터베이스에 대한 보안 제어를 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스 내에서 사용되는 테스트 데이터베이스에 대한 보안 정책, 절차 및 제어	AWS에 의해 구현된 테스트 환경에서 프로덕션 데이터가 사용되는 경우 보안 정책, 절차 및 제어를 프로덕션 제어와 일치하도록 구성해야 합니다.	이 제어는 전적으로 고객의 책임입니다.

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
원격 액세스						
RA-1	원격 액세스	경영진이 승인한 원격 액세스가 업무상 충분한 근거가 있습니까? 원격 액세스, 지원 및 관리는 금지되지 않았다면 신중하게 고려해야 합니다. 최소한 관리자가 강력한 인증 및 암호화된 세션을 요구해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14 FFIEC AUD Booklet(2012) Appendix A: Tier II: D A13-A14	검사관은 AWS 서비스 및 Amazon EC2 인스턴스에 대한 액세스를 관리하는 내부 정책 및 절차를 검토해야 합니다. 조직이 Direct Connect를 사용하여 기존 네트워크와 AWS 간을 연결하는 경우, 검사관은 조직의 네트워크 상의 시스템에 액세스하는 데 사용되는 원격 액세스 모델도 검토해야 하며, 해당 원격 액세스가 AWS 내 시스템에 액세스하는 데 사용될 수 있는지 검토해야 합니다. 참고: AWS 및 Amazon EC2 인스턴스에 대한 모든 액세스는 Direct Connect가 구성되지 않는 경우 "원격 액세스"로 정의됩니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 직접 및 원격 액세스를 관리하는 정책 및 절차, 그리고 AWS 서비스가 이에 부합하는지 확인	조직은 AWS 서비스 및 인스턴스에 대한 원격 액세스를 구현 및 유지해야 합니다. 멀티 팩터 인증을 평가합니다. AWS 계정의 멀티 팩터 인증이 정책상 필요한지 결정합니다. 1. 필요할 경우, AWS Management Console을 통해 AWS 계정 및 개별 IAM 사용자 계정에서 MFA가 적용되어 있는지 확인합니다. 2. 독립형 시스템과 마찬가지로, 이러한 가상 시스템에도 액세스 제어를 구현하고 유지해야 합니다. 멀티 팩터 인증 구현도 포함될 수 있습니다. 참조: Multi-Factor Authentication	AWS 시스템에 AWS 원격 관리 연결은 SSH를 통해 이뤄진다. 원격 연결은 시스템을 관리 및 운영하기 위해 사용합니다. AWS 관리자는 암호 도구를 사용하여 RSA 퍼블릭 키와 시스템 계정을 연결합니다. 이 퍼블릭 키는 사용자가 관리 권한이 있는 호스트 클래스의 모든 호스트에 전파됩니다. 이를 통해서 관리자는 자신의 사용자 ID와 프라이빗 키를 이용해서 호스트에 SSH 접속을 할 수 있습니다. 프라이빗 키는 사용자가 passphrase를 이용해서 보호합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AC-17 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 8

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
RA-2	원격 액세스	모든 원격 액세스는 기록하고 모니터링해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14 FFIEC AUD Booklet(2012) Appendix A: Tier II: D A13-A14	검사관은 Amazon EC2 인스턴스 및 IAM 인증 구성의 원격 액세스 로깅을 검토해야 합니다. 네트워크 액세스를 위한 Amazon IAM 계정은 멀티 팩터 인증으로 구성해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 액세스 로깅 및 IAM 구성	AWS Management Console 액세스는 AWS에서 기록하고 모니터링합니다. 공통 관리 포트(Windows는 3389, Linux는 22)에 대한 액세스를 허용하여 EC2 인스턴스에 대한 직접 액세스를 구성한 경우 시스템에서 로깅 및 모니터링을 구성하여 운영 체제 구성에서 모든 원격 액세스를 기록해야 합니다.	AWS는 베스천 호스트에서 수행되는 syslog를 통해서 원격 제어 메소드을 모니터링하고 제어하는 자동화된 메커니즘을 이용합니다. sys.log 또는 auth.log 파일에 포함된 시스템 및 장치에서 감사가 이뤄지며, 이후의 검토 및 사고 조사를 위해 취합 및 저장됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AC-17 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 8
RA-3	원격 액세스	모든 원격 액세스 통신은 강력한 인증 제어 및 암호화 기술을 사용해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: B, K p. A12-A14, A20-A21	검사관은 Amazon 인스턴스에서 보안 그룹이 일반적인 관리 포트(Windows는 3389, Linux는 22)에 대한 직접 액세스를 허용하도록 구성되었는지 검토해야 합니다. 또한, 검사관은 시스템에 구현되어 있을 수도 있는 멀티 팩터 인증 메커니즘 및 암호화 구성을 물리적 시스템의 경우와 비슷한 방식으로 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 보안 그룹을 구성	AWS 콘솔 및 관리에 대한 액세스는 모두 강력한 암호화의 HTTPS를 사용합니다. 전송 중 데이터의 암호화가 필요할 경우 모든 적용 가능한 AWS 서비스에 대한 연결이 HTTPS 전송용 보안 엔드포인트를 경유하는지 확인해야 합니다. 1. 또한, Windows X.509 인증서, SSH, 기본 데이터베이스 프로토콜용 SSL/TLS 래퍼 및/또는 VPN 솔루션의 사용도 확인해야 합니다. 2. AWS 서비스를 관리할 경우 전송 중 데이터의 보호와 관련된 문서를 이해 및 확인해야 합니다.	호스트에 대한 원격 액세스는 인증서 기반 SSH v2를 경유합니다. 이 방식은 암호화 해시와 암호를 사용하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AC-17 (2) SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 4

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
인력 제어와 업무 분리						
PCS-1	인력 제어와 업무 분리	시스템, 네트워크 및 보안 관리자가 최소한의 트랜잭션 기능을 가집니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: A p. A8-A12	검사관은 AWS 서비스와 관련하여 조직 내에서 사용되는 액세스 제어 유형을 검토해야 합니다. **연동된 액세스 제어:** 연동 인증을 사용하는 경우 AWS 권한에 대한 내부 역할 할당을 검토하고 권한 부여를 위한 프로세스 및 방식을 이해합니다. **고유 AWS 액세스 제어:** 기능 역할 및 책임에 할당된 Amazon IAM 역할 및 사용자 **인스턴스 액세스 제어:** Amazon EC2 인스턴스의 경우에는 로컬 운영체계 엑세스 제어 메커니즘 기반으로 구현된 역할과 할당을 검토하고, EC2 가상 메신에 접근을 관리하기 위해서 조직이 사용하는 연동 방식도 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. Amazon IAM 계정 계획 2. Amazon IAM 설정 내보내기.	조직은 다음을 관리하기 위해 실시하는 제어를 문서화하고 목록을 작성해야 합니다. 3. 리소스 관리, 보안 그룹, VPN, 객체 권한 등을 관리하는데 사용되는 Amazon IAM 4. AWS 계정 및 역할의 목록. 5. 자격 증명 연동 또는 임시 자격 증명을 사용하는 경우 구현에 대한 설명을 제공합니다. 6. 최소 권한을 설정 및 유지하는 프로세스를 제공. 7. EC2 환경 애플리케이션 제어로부터 정보를 제공. EC2 인스턴스와 EC2 환경 내 서비스(예: RDS)에 대한 액세스 제어를 구현하고 유지합니다. 독립형 시스템과 마찬가지로, 이러한 가상 시스템에도 액세스 제어를 구현하고 유지해야 합니다.	시스템 경계 내부의 시스템 및 장치를 지원하는 모든 AWS 직원은 AWS 모기업인 Amazon.com 내에서 고위험직으로 분류되고 있습니다. 이러한 직원은 민감한 AWS 영업비밀, 기밀 또는 독점 정보 또는 기타 소중한 기업 자산에 액세스 가능한 직책을 가진 것으로 간주됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: PS-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 7

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
PCS-2	인력 제어와 업무 분리	IT 직원은 정보 보안 프로그램과 이 프로그램이 본인 업무와 어떻게 연결되는지 잘 알고 있어야 합니다. 여기에는 보안 교육 프로그램과 보안 문제 및 목표의 전달이 포함됩니다.	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC OPS Booklet(2004) Appendix A: Tier II: F p. A14-A15	검사관은 정보 보안 인식 교육 기록을 검토하고 교육이 Amazon IAM 사용, EC2 보안 그룹, EC2 인스턴스에 대한 원격 액세스 등 AWS 보안을 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 보안 인식 정책 및 절차	조직은 정보 보안 인식 교육에 Amazon IAM 사용, EC2 보안 그룹, Amazon EC2 인스턴스에 대한 원격 액세스 등 AWS 보안을 포함시켜야 합니다.	AWS는 "AWS 인식 및 교육 정책"이라고 하는 공식적이고 문서화된 인식 및 교육 정책을 마련했으며, 이 정책은 적어도 매년 검토 및 업데이트됩니다. AWS 인식 및 교육 정책은 내부 AWS 규정 준수 웹 포털을 통해 모든 직원, 공급업체 및 계약업체로 전파됩니다. AWS 규정 준수 팀은 AWS 최고 정보 보안 책임자의 승인을 얻어 매년 이 정책을 검토합니다. 이 정책은 목적, 범위, 역할, 책임 및 경영진의 책임감을 규정합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AT-1 SOC 2 – 'Security Communications' Criteria 2.2 description PCI DSS v3.0 Requirement 12
PCS-3	인력 제어와 업무 분리	시스템 및 보안 관리자 로그를 모니터링하는 IT 보안 담당자는 IT 운영과 독립적으로 근무하거나 적절한 보상 제어(예: 외주 보안 모니터링)를 구현해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 5 p. A4-A5 FFIEC AUD Booklet(2012) Appendix A: Tier II: D A13-A14	검사관은 AWS 서비스 및 Amazon EC2 인스턴스에 대한 액세스를 관리하는 내부 정책 및 절차를 확인해야 합니다. 보안 관리자 로그를 모니터링하는 직원은 운영 관리자를 담당하는 직원과 독립적으로 근무해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 액세스 관리 정책 및 절차 2. 로깅 및 모니터링 정책 및 절차	조직은 직접 또는 연동 액세스의 사용이 관리자 로그에 대한 적절한 업무 분리을 통해 구현되는지 평가해야 합니다. EC2 인스턴스에 대한 액세스 제어를 구현하고 유지합니다. 로그 관리 구성은 보안 관리 로그에 대한 적절한 업무 분리을 적용해야 합니다.	AWS 업무 분리는 정보 시스템 계정, 그룹 멤버십 및 그룹 권한의 관리를 통해 구현되고 제어됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AC-5 SOC 2 – 'Security Communications' Criteria 2.2 description PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
방화벽 제어						
FC-1	방화벽 제어	모든 방화벽 규칙이 ISO/운영 위원회 또는 고위 경영진의 승인을 받았습니까? 모든 승인 기록이 유지됩니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14	검사관은 방화벽 규칙을 승인하는 내부 정책 및 절차가 AWS 보안 그룹 및 VPN 구성을 포함하는지 확인해야 합니다. AWS 보안그룹이 적절한 승인이 이루어졌는지 확인하기 위해서 변경 샘플링은 통해서 검토하고 검증해야한다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 방화벽, 보안 그룹 및 VPN 구성에 대한 정책 및 절차	조직은 AWS에서 방화벽 규칙 관리를 위한 프로세스를 정의해야 하며, 여기에는 보안 그룹 구성 변경 사항, 경영진 승인, 승인 문서의 관리가 포함되어야 합니다. EC2 환경에서 호스트 기반 또는 어플라이언스 기반 방화벽과 같은 추가 방화벽 기술이 구현된 경우 이러한 방화벽의 변경도 승인 및 보존이 필요하며 보안 그룹 문서도 마찬가지입니다.	모든 컴퓨팅 인스턴스는 호스트 기반 방화벽을 사용하여 의도치 않은 또는 승인되지 않은 연결 및 통신으로부터 보호합니다. AWS는 자동화된 메커니즘을 사용하여 논리적 및 물리적 액세스 제한을 모두 적용합니다. 이러한 메커니즘은 적용 작업의 감사를 지원합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SC-7 (12); CM-5 (1) SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
FC-2	방화벽 제어	방화벽 구성이 강화되어 불필요한 서비스를 모두 제거하고 최신 보안 패치 및 펌웨어 업데이트로 최신 상태를 유지합니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14	검사관은 호스트 기반 또는 기타 방화벽 구성을 검토하여 충분히 강화되었는지 확인해야 하며, 조직과 공동으로 방화벽 강화 기술에 관한 공급업체 또는 업계 문서를 식별해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 방화벽, 보안 그룹 및 VPN 구성에 대한 정책 및 절차	조직은 AWS 보안 그룹을 내부 경계 보호 정책과 부합하도록 구성해야 합니다. 호스트 기반 또는 기타 방화벽 기술과 같은 다른 기술이 구현된 경우, 조직은 NIST, CIS 또는 SANS와 같은 공급업체 또는 업계 표준을 사용하여 방화벽 구성을 강화시켜야 합니다.	AWS는 인프라 구성 요소 전체에 걸쳐 최소 권한을 구현합니다. 모든 네트워크 장치, 방화벽 및 서버는 최소 기능으로 구현되어 있으며, 서비스 팀이 장치가 기능을 발휘하는 데 필요한 소프트웨어 패키지, 패치 및 서비스만 추가합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1 & 2

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
FC-3	방화벽 제어	방화벽 제어를 실행 중입니까? a) 기본값. 특정하여 허용되지 않은 모든 트래픽을 제한 b) NAT를 사용하여 내부 주소를 숨김 c) 악성 코드를 차단 d) 로깅이 활성화됨	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14	검사관은 AWS 보안 그룹이 기본 방화벽 솔루션인지 확인해야 합니다. AWS 방화벽: a) 기본적으로 모든 트랙픽을 제한 b) NAT 사용 c) 네트워크 연결 상태 검사 구현 d) ACL 및 특권 사용을 기록 다른 방화벽 기술이 사용되는 경우 검사관은 해당 기술을 검토하여 내부 주소를 숨기고 악성 코드를 차단하고 로깅을 활성화하도록 올바로 구성되었는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 방화벽, 보안 그룹 및 VPN 구성에 대한 정책 및 절차	조직은 AWS 보안 그룹을 내부 경계 보호 정책과 부합하도록 구성해야 합니다. AWS ECS는 완벽한 방화벽 솔루션을 제공합니다. 이 필수 인바운드 방화벽은 기본 거부 모드로 구성되며 인바운드 트래픽을 허용하려면 EC2 클라이언트는 명시적으로 포트를 개방해야 합니다. 트래픽은 프로토콜, 서비스 포트, 소스 IP 주소(개별 IP 또는 CIDR 블록)를 기준으로 제한될 수 있습니다. 방화벽은 호스트/인스턴스 자체에 의해 제어될 수는 없고, 클라이언트의 X.509 인증서 및 키를 사용하여 변경을 인가하므로 추가 보안 계층이 추가합니다. EC2 내에서는 고객 호스트 관리자와 고객 클라우드 관리자가 별개 인물일 수 있으므로 2인 규칙 보안 정책을 적용할 수 있습니다.	AWS 방화벽은 모두 기본 거부 정책을 사용하므로 인스턴스 소유자가 액세스를 특정하여 정의해야 합니다. AWS는 VPC 내 고객별로 VLAN을 구현합니다. 즉 고객이 자체 VPC에서 VLAN 구성을 제어합니다. AWS는 모든 트래픽이 NAT를 통하고, 특별한 비즈니스 목적이 없는 모든 포트와 프로토콜을 금지합니다. AWS는 감사 기능을 제공하는 모든 보안 장치 및 호스트의 감사 가능한 이벤트에 대해 감사 레코드 생성 기능을 제공합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-5 & CM-7 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
FC-4	방화벽 제어	방화벽 원격 관리가 보안이 확실한 장치에서만 신뢰할 수 있는 네트워크 경로를 통해 암호화된 통신으로 수행됩니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14	검사관은 AWS 보안 그룹 관리가 보안이 확실한 워크스테이션으로부터 AWS 콘솔 또는 커멘드라인 API을 HTTPS를 통해 이루어지는지 확인해야 합니다. 또한, 검사관은 일반 관리 권한이 할당되었거나 AWS 콘솔 내에서 또는 커맨드라인 API를 통해 보안 그룹을 관리할 권한이 할당된 모든 사용자에 대해 멀티 팩터 인증이 활성화되었는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 원격 액세스를 관리하는 정책 및 절차	조직은 방화벽 관리를 위해 AWS Management Console 또는 커맨드라인 API용 HTTPS를 구현해야 합니다. 또한, 조직은 멀티 팩터 인증을 구현하여 일반 관리 권한이 할당되었거나 AWS 콘솔 내에서 또는 커맨드라인 API를 통해 보안 그룹을 관리할 권한이 할당된 모든 사용자에 대해 활성화해야 합니다.	AWS 시스템과의 AWS 원격 관리 연결은 SSH v2를 사용하여 이루어집니다. AWS 관리자는 암호 도구를 사용하여 RSA 퍼블릭 키와 시스템 계정을 연결합니다. 이 퍼블릭 키는 사용자가 관리 권한이 있는 호스트 클래스의 모든 호스트에 전파됩니다. 이를 통해서 관리자는 자신의 사용자 ID와 프라이빗 키를 이용해서 호스트에 SSH 접속을 할 수 있습니다. 프라이빗 키는 사용자가 passphrase를 이용해서 보호합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AC-17 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
FC-5	방화벽 제어	방화벽에 대한 관리 액세스가 일부 IT 직원으로 제한됩니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14	검사관은 AWS 보안 그룹 관리를 일부 IT 직원으로 제한하는 내부 정책 및 절차를 확인해야 합니다. 내부 정책 및 절차가 AWS 보안 그룹 관리를 일부 IT 직원으로 제한해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 방화벽, 보안 그룹 및 VPN 구성에 대한 정책 및 절차	AWS 서비스가 고객 데이터용으로 사용되는 경우 보안 그룹 구성 또는 AWS 권한의 VPN 방화벽 규칙의 변경을 허용하는 AWS 계정은 중요 계정으로 간주되어야 합니다. 이러한 계정에 대해서는 Amazon IAM 멀티 팩터 인증이 활성화되어야 합니다. 또한, 영구 특권있는 계정을 유지하지 않으려면 임시 보안 자격 증명(토큰)을 사용할 수 있습니다.	AWS는 인프라 구성 요소 전체에 걸쳐 최소 권한을 구현합니다. 모든 네트워크 장치, 방화벽 및 서버는 최소 기능으로 구현되어 있으며, 서비스 팀이 장치가 기능을 발휘하는 데 필요한 소프트웨어 패키지, 패치 및 서비스만 추가합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-7 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
FC-6	방화벽 제어	방화벽 구성 변경은 잘 구성되고 문서화된 변경 제어 절차를 통해 이루어져야 합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14	검사관은 방화벽 구성 변경에 대한 내부 정책 및 절차가 AWS 보안 그룹 및 VPN 구성을 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 방화벽, 보안 그룹 및 VPN 구성에 대한 정책 및 절차	조직은 변경 프로세스를 새로 설정하거나 기존 프로세스를 확장하여 모든 방화벽 변경이 적절한 변경 관리 프로세스 및 문서화를 요구하도록 해야 합니다.	시스템 경계 내부에서 네트워크 장치의 기본 구성은 네트워킹 팀이 유지 관리하고 업데이트합니다. 구성을 업데이트하는 경우 네트워킹 팀이 위에 나열된 구성 관리 도구를 사용하여 다음을 제공합니다. 1. 버전 관리 - 모든 업데이트가 버전 관리되며 필요에 따라 이전 버전도 사용 가능합니다. 2. 액세스 제어 - 변경을 실시하는 사용자가 해당 권한이 있으며 변경이 특정 사용자와 연결됩니다. 3. 문서화 - 변경 목적이 담겨있어야합니다. 새로운 기본 구성은 전체 네트워크 장치에 동일하게 관리되기 위히새 장치들이 적용됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-2 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1 & 2

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
FC-7	방화벽 제어	조직이 전체 조직의 보안 정책을 구현하는 데 방화벽의 역할을 설명하는 방화벽 정책을 문서화합니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14	검사관은 내부 방화벽 정책이 AWS 보안 그룹과 VPN 구현 및 관리를 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 방화벽, 보안 그룹 및 VPN 관리가 정의되었는지 확인하기 위한 보안 정책	조직은 기존 보안 정책을 검토하여 AWS 보안 그룹과 VPC 방화벽 관리를 포함하도록 기존 정책을 개정해야 합니다.	AWS는 "AWS 구성 관리 정책"이라고 하는, AWS에 적용되는 공식적이고 문서화된 구성 관리 정책을 마련했습니다. 이 정책은 네트워크 및 방화벽의 역할과 구성을 포함합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CM-1 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1
FC-8	방화벽 제어	조직이 방화벽 정책을 올바르게 구현할 수 있도록 IT 직원을 교육하거나, 서비스를 아웃소싱하는 경우 방화벽 관리가 조직 정책을 준수합니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5	검사관은 교육 기록을 검토하고 교육이 Amazon IAM 사용, EC2 보안 그룹, EC2 인스턴스에 대한 원격 액세스 등 AWS 보안을 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 서비스 지원 및 보안이 포함되는지 확인하기 위한 보안 교육 프로그램	조직은 절차 문서 및 교육 자료를 새로 작성하거나 기존 문서를 개정하여 AWS 방화벽이 IT 직원을 대상으로 하는 인식 및 교육 프로그램에 포함되도록 해야 합니다.	시스템 설계/아키텍처 또는 주요 시스템 기능을 상당히 변경했거나 대폭적인 조직 변경이 있은 경우 역할 기반 보안 교육이 필요합니다. 또한, 역할 기반 교육이 일상적 상호 작용을 통해 또는 팀 wiki를 검토하여 지속적으로 제공되고 있습니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AT-3 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 1

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
로깅, 평가 추적 및 모니터링						
LAM-1	로깅, 평가 추적 및 모니터링	조직이 시스템과 연관된 위험에 따라 로깅해야 하는 시스템 구성 요소, 서비스 또는 이벤트를 식별했으며 다음 시스템에서 활성화했습니까? - 운영 체제 - 네트워크 장치 - 애플리케이션 - 방화벽 - VPN	FFIEC IS Booklet(2006) Appendix A: Objective 6 p. A6-A7 FFIEC IS Booklet(2006) Appendix A: Tier II: B, C, G, M p. A12-A15, A17, A22-A25 FFIEC AUD Booklet(2012) Appendix A: Tier II: D p. A13-A14	검사관은 물리적 시스템과 비슷한 방식으로 로깅 메커니즘을 검토해야 합니다. AWS 관리 활동의 경우, 검사관은 서비스 구성 변경을 모니터링하기 위해 구현된 프로세스의 레코드를 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직의 로깅 및 모니터링 정책/절차 및 AWS 서비스 부합/포함 여부	조직은 서비스 구성 변경을 주기적으로 모니터링하는 프로세스를 정의해야 합니다. 물리적 시스템과 마찬가지로, EC2 인스턴스, EC2 인스턴스에 배포된 애플리케이션, Amazon RDS 데이터베이스, 고객 EC2 환경의 다른 서비스 부분의 로깅 및 모니터링을 구현하고 유지해야 합니다.	AWS 감사 및 책임 계획은 Amazon Web Services(AWS) 로그 데이터의 획득, 보존 및 관리에 대한 공식적으로 문서화된 구현 계획 및 지침을 제공합니다. 이는 서비스 디버깅, 보안 사고 조사, 규정 준수 활동 등 다수의 중요 비즈니스 프로세스를 지원하는 데 필요합니다. 이 계획은 또한 AWS 감사 및 책임 정책의 요구 사항을 해석하는 기초가 되는데, AWS 서비스별 로그 관리 절차를 개발할 때 이 요구 사항을 사용해야 합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AU-1 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 10
LAM-2	로깅, 평가 추적 및 모니터링	조직이 운영 체제, 서버 및 네트워크장치 로그를 중앙 리포지토리에 일정 기간(약 90일) 저장하여 평가 추적을 유지하는 중앙 집중식 로깅 솔루션을 구현했습니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: M p. A22-A25	검사관은 로깅 메커니즘을 검토하여 이들 메커니즘이 물리적 시스템과 비슷한 방식으로 로그를 중앙 서버로 전송하도록 구성되었는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직의 로깅 및 모니터링 정책/절차 및 AWS 서비스 부합/포함 여부: 2. AWS CloudTrail 3. AWS Config 4. S3 서버 로그	AWS가 AWS 콘솔에 대한 액세스를 기록하고 모니터링하지만 고객이 활동을 모니터링할 인터페이스는 제공하지 않습니다. 물리적 시스템과 마찬가지로, 조직은 EC2 인스턴스, EC2 인스턴스에 구현된 애플리케이션, Amazon RDS 데이터베이스, 고객 EC2 환경의 다른 서비스 부분의 로깅 및 모니터링을 구현하고 유지해야 합니다. 로그는 검토 및 보존을 위해 중앙 집중식 로깅 솔루션이 수집해야 합니다.	AWS 감사 및 책임 계획은 Amazon Web Services(AWS) 로그 데이터의 획득, 보존 및 관리에 대한 공식적으로 문서화된 구현 계획 및 지침을 제공합니다. 이는 서비스 디버깅, 보안 사고 조사, 규정 준수 활동 등 다수의 중요 비즈니스 프로세스를 지원하는 데 필요합니다. 이 계획은 또한 AWS 감사 및 책임 정책의 요구 사항을 해석하는 기초가 됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AU-1 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 10

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
LAM-3	로깅, 평가 추적 및 모니터링	조직이 보존할 로그의 유형 및 형식을 지정했습니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: M p. A22-A25	Amazon EC2 인스턴스의 경우, 검사관이 로깅 메커니즘을 검토하여 올바른 유형 및 형식의 로그가 물리적 시스템과 비슷한 방식으로 유지되고 있는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. AWS 로그 요소가 포함될 수 있는지 확인하기 위해, 로깅 형식과 관련된 조직의 로깅 및 모니터링 문서	AWS가 AWS 콘솔에 대한 액세스를 기록하고 모니터링하지만 고객이 활동을 모니터링할 인터페이스는 제공하지 않습니다. 물리적 시스템과 마찬가지로, 조직은 EC2 인스턴스, EC2 인스턴스에 구현된 애플리케이션, Amazon RDS 데이터베이스, 고객 EC2 환경의 다른 서비스 부분의 로깅 및 모니터링을 구현하고 유지해야 합니다. 조직은 보존할 로그의 유형 및 형식을 결정해야 합니다.	AWS 감사 및 책임 계획은 Amazon Web Services(AWS) 로그 데이터의 획득, 보존 및 관리에 대한 공식적으로 문서화된 구현 계획 및 지침을 제공합니다. 이는 서비스 디버깅, 보안 사고 조사, 규정 준수 활동 등 다수의 중요 비즈니스 프로세스를 지원하는 데 필요합니다. 이 계획은 또한 AWS 감사 및 책임 정책의 요구 사항을 해석하는 기초가 됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AU-1 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 10
LAM-4	로깅, 평가 추적 및 모니터링	조직이 로그 파일 보안을 위한 정책 및 절차를 수립하고 있습니까? 여기에는 다음 항목이 포함됩니다. - 업무 분담 및 부인 방지 인정(시스템 관리자가 로그 내용을 수정할 수 없어야 함) - 로그 파일의 물리적 및 논리적 운반을 보호 - 로그 분석에 공식 권위를 부여	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: M p. A22-A25 FFIEC AUD Booklet(2012) Appendix A: Tier II: D p. A13-A15	검사관은 내부 정책이 AWS 로그 관리 기능의 감독 및 모니터링과 관련하여 AWS 서비스 및 Amazon EC2 인스턴스를 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. SoD, 보안 및 액세스 권한을 다루고 있는지 확인하기 위해, 조직의 로깅 및 모니터링 정책/절차	AWS가 AWS 콘솔에 대한 액세스를 기록하고 모니터링하지만 고객이 활동을 모니터링할 인터페이스는 제공하지 않습니다. 물리적 시스템과 마찬가지로, 조직은 EC2 인스턴스, EC2 인스턴스에 구현된 애플리케이션, Amazon RDS 데이터베이스, 고객 EC2 환경의 다른 서비스 부분의 로깅 및 모니터링을 구현하고 유지해야 합니다.	AWS 감사 및 책임 계획은 Amazon Web Services(AWS) 로그 데이터의 획득, 보존 및 관리에 대한 공식적으로 문서화된 구현 계획 및 지침을 제공합니다. 이는 서비스 디버깅, 보안 사고 조사, 규정 준수 활동 등 다수의 중요 비즈니스 프로세스를 지원하는 데 필요합니다. 이 계획은 또한 AWS 감사 및 책임 정책의 요구 사항을 해석하는 기초가 됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AU-1 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 10

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
LAM-5	로깅, 평가 추적 및 모니터링	조직의 네트워크는 네트워크 모니터링 도구를 사용하여 정기적으로 모니터링하여 문제 여부를 확인해야 합니다(예: 패킷 드롭, 간섭 또는 용량 문제).	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: B, M p. A12-A14, A22-A25	AWS는 또한 AWS CloudWatch, Describe API 등의 모니터링 서비스도 제공합니다. 이러한 서비스를 사용하는 경우 검사관은 고객이 네트워크 모니터링에 해당 서비스를 사용하는 프로세스 및 레코드를 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. Amazon EC2 인스턴스에서 구현된 네트워크 로깅 및 CloudWatch(AWS CloudTrail과 연동) 사용, 조직 내부에서 사용되는 경우	고객은 AWS 환경에서 어떤 네트워크 계층에도 액세스하지 않습니다. AWS가 서비스 성능 모니터링 서비스를 제공합니다. 조직은 AWS CloudWatch의 사용을 평가해야 합니다. Amazon CloudWatch를 통해 Amazon EC2 인스턴스, Amazon EBS 볼륨, Elastic Load Balancers, Amazon RDS DB 인스턴스를 비롯한 AWS 리소스를 실시간으로 모니터링할 수 있습니다. CPU 사용률, 지연 시간, 요청 횟수와 같은 측정치는 해당 AWS 리소스가 자동으로 제공합니다. 참조: CloudWatch	AWS 서비스 모니터링: 시계열 데이터(TSD)는 Amazon의 서비스 기반 모니터링 솔루션 및 파이프라인으로 성능 측정치를 수집하고 저장합니다. 시스템은 이러한 추가 요소를 기록하도록 구성되며, 각 이벤트는 시스템의 auth.log / authpriv 파일에 캡처됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: AU-2 & AU-3 SOC 2 – Section III, Area D PCI DSS v3.0 Requirement 11
백업 및 스토리지 제어						
BU-1	백업 및 스토리지 제어	조직이 기본 데이터 시설이 손상될 경우 데이터를 복구하기 위해 소산된 위치에 있는 데이터 스토리지를 사용합니까?	FFIEC OPS Booklet(2004) Appendix A: Objective 6 p. A5-A6 FFIEC OPS Booklet(2004) Appendix A: Tier II: C p. A12-A13	검사관은 오프사이트 백업을 위한 AWS 서비스 사용을 검토하고 본 문서 전체에서 AWS에 저장되는 데이터에 적합한 제어를 고려해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직의 백업 전략에서 AWS가 어떻게 활용되는지 평가하기 위해, 조직의 백업/스토리지 정책 및 절차	AWS 서비스는 데이터 백업 시설로 사용할 수 있습니다. 전 세계의 개발자 및 기업은 블록 스토리지, 파일 스토리지, 백업, 아카이브, 재해 복구에 Amazon Web Services(AWS)를 활용하고 있습니다. 조직은 백업 및 스토리지 전략에서 어떻게 AWS를 활용할지 평가하고 문서화해야 합니다. 참조: AWS 백업/스토리지	AWS는 AWS 내에서 사용 가능한 EBS 및 S3 스토리지 서비스를 통해 사용자 수준 정보를 저장합니다. 데이터가 EBS 또는 S3에 저장되어 있으면 데이터가 변경될 때마다 중복 사본이 자동으로 및 동기식으로 생성되고 사본이 원본 데이터와 동일한지 검증됩니다. AWS는 손실된 중복성을 자동으로 검색 및 복원하여 데이터의 내구성을 유지합니다. 손상이 감지된 경우 중복 데이터를 사용하여 자동으로 복원되므로 데이터 무결성이 보장됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-09 SOC 2 – Section III, Area C

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
BU-2	백업 및 스토리지 제어	경영진이 오프사이트 위치에 저장된 모든 백업 미디어의 인벤토리를 유지합니까? 모든 백업 미디어의 가용성을 보장하려면 인벤토리 검사를 자주 실행해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 6 p. A5-A6	검사관은 소산 백업으로 AWS 서비스에 백업한 데이터의 인벤토리를 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 오프사이트 스토리지 위치 및/또는 오프사이트 스토리지로 AWS 사용 여부를 식별하기 위해, 조직의 백업/스토리지 정책 및 절차	AWS 서비스는 데이터 백업 시설로 사용할 수 있습니다. 전 세계의 개발자 및 기업은 블록 스토리지, 파일 스토리지, 백업, 아카이브, 재해 복구에 Amazon Web Services(AWS)를 활용하고 있습니다. 조직은 백업 및 스토리지 전략에서 어떻게 AWS를 활용할지 평가하고 문서화해야 합니다.	선택된 지리적 리전 내에서 다중 장치 및 다중 시설에 걸쳐 데이터가 변경될 때마다 AWS는 자동으로 또한 동기식으로 데이터를 저장합니다. S3 스토리지는 AWS IaaS에서 최고 수준의 데이터 내구성과 가용성을 제공합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-09 SOC 2 – Section III, Area C
BU-3	백업 및 스토리지 제어	향후 성장을 대비해 백업 및 스토리지 제어가 확장 가능합니까?	FFIEC OPS Booklet(2004) Appendix A: Objective 6 p. A5-A6	검사관은 계획에서 추정 데이터 백업 요건과 현재의 AWS 서비스 사용을 검토하여 이러한 성장을 지원할 수 있을지 판단해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 확장 가능성 및 AWS 서비스 사용을 확인하기 위한 조직의 백업/스토리지 정책 및 절차	AWS 서비스는 데이터 백업 시설로 사용할 수 있습니다. AWS는 데이터가 감사되는 데이터 센터에 유지하고 이동식 미디어는 사용하지 않습니다. 고객은 향후 AWS 사용 계획 및 예산을 수립할 책임이 있습니다. AWS를 사용하면 확장 가능한 솔루션을 구축하여 향후 성장에 대비할 수 있습니다.	데이터는 AWS에 저장되고 중복 사본이 자동으로 생성되며 원본 데이터와 동일한지 검증됩니다. AWS는 손실된 중복성을 자동으로 검색 및 복원하여 데이터의 내구성을 유지합니다. 손상이 감지된 경우 중복 데이터를 사용하여 자동으로 복원되므로 데이터 무결성이 보장됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-09 SOC 2 – Section III, Area C
BU-4	백업 및 스토리지 제어	중요 데이터에 대한 무단 액세스를 방지하도록 백업 미디어가 보호됩니까(물리적 및 암호화)?	FFIEC OPS Booklet(2004) Appendix A: Objective 6 p. A5-A6	검사관은 소산 백업으로 AWS 서비스에 백업한 데이터의 인벤토리를 검토해야 합니다. AWS는 이동식 미디어를 사용하지 않습니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 내부적으로 또한 AWS 내에서 데이터를 보호하기 위해 실시 중인 보호 조치를 보다 잘 이해하기 위한 조직의 백업/스토리지 정책 및 절차	AWS 서비스는 데이터 백업 시설로 사용할 수 있습니다. AWS는 데이터가 감사되는 데이터 센터에 유지하고 이동식 미디어는 사용하지 않습니다. AWS는 어떤 이동식 미디어도 사용하지 않지만 데이터를 추가로 보호하기 위해 지원되는 경우 서버 측 암호화를 사용하거나 AWS 서비스를 사용하여 저장하기 전에 데이터를 암호화할 수 있으므로 데이터 보호에 도움이 되도록 키를 안전하게 보관하십시오.	AWS는 데이터를 전송하는 과정에서 메시지 내용을 읽을 수 없도록 데이터 전송 전에 대칭 암호화를 사용하여 전송된 데이터의 기밀성을 보호합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SC—09 SOC 2 – Section III, Area C

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
BU-5	백업 및 스토리지 제어	필요시 미디어가 제대로 작동할 수 있도록 정기적으로 오프사이트 데이터 미디어를 테스트합니까?	FFIEC BCP Booklet(2008) Appendix A: Objective 6 p. A8 FFIEC OPS Booklet(2004) Appendix A: Objective 6 p. A5-A6	검사관은 AWS 서비스에 저장된 백업 데이터를 테스트한 기록을 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직의 테스트 프로세스를 검증하기 위한 조직의 백업/스토리지 정책 및 절차	AWS 서비스는 데이터 백업 시설로 사용할 수 있습니다. AWS는 데이터가 감사되는 데이터 센터에 유지하고 이동식 미디어는 사용하지 않습니다. 조직은 다른 백업 서비스 공급자와 마찬가지로 정기적으로 복원 테스트를 실시해야 합니다.	데이터는 AWS에 저장되고 중복 사본이 자동으로 생성되며 원본 데이터와 동일한지 검증됩니다. AWS는 손실된 중복성을 자동으로 검색 및 복원하여 데이터의 내구성을 유지합니다. 손상이 감지된 경우 중복 데이터를 사용하여 자동으로 복원되므로 데이터 무결성이 보장됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: CP-09
암호화 제어						
ENC-1	암호화 제어	전송 및 저장 중 고객의 기밀 정보를 보호하기 위해 적절한 제어가 적용되고 있습니까(예: 전송 암호화, 인증서, Secure File Share)?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: L p. A21-A22 FFIEC OPS Booklet(2004) Appendix A: Objective 5 p. A4-A5	검사관은 AWS 콘솔, 관리 API, S3, RDS 및 Amazon EC2 VPN에 연결하는 방식을 검토해야 합니다. 검사관은 관리 액세스를 위해 구현된 제어를 검토하고 AWS에서 호스팅된 시스템에 배포될 수 있는 애플리케이션 제어도 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 내부적으로 또한 AWS 서비스 내에서 저장, 전송 및 사용 시 데이터 보호와 관련된 정책 및 절차	AWS는 콘솔 및 웹 서비스 인터페이스를 위한 HTTPS, 스토리지를 위한 서버 측 암호화를 비롯해 전송 및 저장 암호화 기능을 제공합니다. EC2 인스턴스는 고객이 완벽하게 통제할 수 있습니다. 고객은 EC2 리소스에서 구현 및 사용될 수 있는 암호화를 구현 및 관리할 책임이 있습니다. 조직은 AWS 내 보안 기능을 이해하고 평가해야 합니다. 참조: AWS 보안 리소스	스토리지의 경우, AWS Acceptable Encryption Standard는 자격 증명 및 키 저장을 위해 승인된 방법을 지정합니다. 이 인증 및 보고서에는 다음 항목이 포함됩니다. ▪ AWS Key Management Service ▪ Window DPAPI ▪ MAC OS X Keychain ▪ Password Safe ▪ AWS CloudHSM 하드웨어 보안 모듈 **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IA-05 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 4

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
ENC-2	암호화 제어	데이터를 보호하기 위해 사용되는 암호화 알고리즘은 공개가 중대한 위험을 초래하지 않을 때까지 데이터를 보호할 수 있을 정도로 강력해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: K, L p. A20-A22	검사관은 암호화를 적용하기 위해 AWS 콘솔, 관리 API 및 Amazon EC2 VPN에 연결하는 방식을 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. Amazon EC2 인스턴스에서 데이터를 보호하기 위해 사용되는 암호화 프로세스(물리적 시스템과 비슷함) 2. Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift 및 Amazon Elastic Transcoder와 통합을 포함하여 AWS Key Management Service의 구성 3. AWS CloudHSM의 구성	AWS는 콘솔 및 웹 서비스 인터페이스를 위한 HTTPS, 스토리지를 위한 서버 측 암호화를 비롯해 전송 및 저장 암호화 기능을 제공합니다. EC2 인스턴스는 고객이 완벽하게 통제할 수 있습니다. 고객은 EC2 리소스에 의한 암호화를 구현 및 관리할 책임이 있습니다.	AWS는 다수의 알고리즘 및 암호화 기법을 사용합니다. 예를 들어 Open SSL를 활용한 SSL/TLS, 전송 데이터의 암호화를 위해 AES 및 3DES 방식의 암호화, 서버 신뢰성을 위해 RSA 키를 포함하는 x.509 서버 인증서, 메시지 무결성을 위해 SHA-1 등의 암호화 방식을 사용합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IA-07 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 3 & 4
ENC-3	암호화 제어	조직이 모든 인증 자격 증명의 전송 및 저장 시 암호화를 구현합니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: K p. A20-A21	검사관은 암호화를 적용하기 위해 AWS 콘솔, 관리 API 및 Amazon EC2 VPN에 연결하는 방식을 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. Amazon EC2 인스턴스에서 데이터를 보호하기 위해 사용되는 암호화 프로세스(물리적 시스템과 비슷함)	AWS는 콘솔 및 웹 서비스 인터페이스를 위한 HTTPS, 스토리지를 위한 서버 측 암호화를 비롯해 전송 및 저장 암호화 기능을 제공합니다. EC2 인스턴스는 고객이 완벽하게 통제할 수 있습니다. 고객은 EC2 리소스에 의한 암호화를 구현 및 관리할 책임이 있습니다.	AWS는 다수의 알고리즘 및 암호화 기법을 사용합니다. 예를 들어 Open SSL를 활용한 SSL/TLS, 전송 데이터의 암호화를 위해 AES 및 3DES 방식의 암호화, 서버 신뢰성을 위해 RSA 키를 포함하는 x.509 서버 인증서, 메시지 무결성을 위해 SHA-1 등의 암호화 방식을 사용합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IA-07 SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 8

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
ENC-4	암호화 제어	조직이 키 관리 정책을 수립하고 있습니까? 암호화 키는 기밀 정보로 취급하고 계층화된 관리 및 기술 제어로 보호해야 합니다. 다음은 뛰어난 키 보안 관행입니다. 키 로테이션, 고유 키 생성, 키 배포 및 취소 문서화, 노출 가능성 있는 키 폐기, 키 활성화 및 비활성화 기간 예시.	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: K p. A20-A21	검사관은 내부 키 관리 정책 및 절차가 AWS 서비스 및 Amazon EC2 인스턴스를 포함하는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. Amazon EC2 인스턴스에서의 키 관리 프로세스(물리적 시스템과 비슷함)	AWS는 키 관리를 지원하는 기능을 제공합니다. 고객은 암호화 키 관리를 구현할 책임이 있습니다. EC2 인스턴스는 고객이 완벽하게 통제할 수 있습니다. 고객은 EC2 리소스에 의한 암호화 키를 구현 및 관리할 책임이 있습니다. 고객은 AWS에서 호스팅되는 시스템의 키를 관리하기 위해 CloudHSM과 같은 여러 기술을 사용할 수 있습니다. 이러한 하드웨어 기반 키 관리 솔루션을 사용하면 오로지 고객만 키를 통제할 수 있습니다.	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 관리자는 AWS에서 대칭적 키를 생성, 보호, 배포하는 데 사용하는 기본 시스템입니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SC-12 PCI DSS v3.0 Requirement 3
악성 코드 제어						
MC-1	악성 코드 제어	모든 중요 서버 및 워크스테이션에 안티바이러스 및 안티스파이웨어 소프트웨어가 배포되어 있습니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: B, C, D p. A12-A16	검사관은 Amazon EC2 인스턴스상의 맬웨어 방지 소프트웨어를 물리적 시스템과 비슷한 방식으로 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 안티바이러스 관련 정책 및 절차, 그리고 해당 정책/절차에 AWS 서비스가 포함되는지 확인	EC2 인스턴스는 고객이 완벽하게 통제할 수 있습니다. 고객은 EC2 리소스용 맬웨어 방지 소프트웨어를 구현 및 관리할 책임이 있습니다. 참조: • AWS & Symantec • AWS & Trend Micro	AWS 보안은 다음 유형의 서비스 거부 공격을 정의했지만 이에 대한 서비스 보호 기능을 제한하지는 않았습니다. • Flooding 공격 - 잘 구성되었지만 서명이 불량한 API 호출을 엄청나게 수신, 고속 패킷 Flooding • 소프트웨어 / 논리적 공격 - 애플리케이션 수준 공격 • 분산 공격 - 다중 위치로부터 홍수 공격 • 의도치 않은 서비스 거부 - 사용량이 엄청나게 증가 **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SC-05 SOC 2, Section IV PCI DSS v3.0 Requirement 5

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
MC-2	악성 코드 제어	안티바이러스/안티스파이웨어 서명 및 업데이트가 릴리스되는 즉시 배포됩니까? AV 패치 및 업데이트 로그가 유지됩니까?	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: B, C, D p. A12-A16	검사관은 Amazon EC2 인스턴스상의 맬웨어 방지 소프트웨어를 물리적 시스템과 비슷한 방식으로 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 안티바이러스 관련 정책 및 절차, 그리고 해당 정책/절차에 AWS 서비스가 포함되는지 확인	EC2 인스턴스는 고객이 완벽하게 통제할 수 있습니다. 고객은 EC2 리소스용 맬웨어 방지 소프트웨어를 구현 및 관리할 책임이 있습니다.	AWS 보안은 다음 유형의 서비스 거부 공격을 정의했지만 이에 대한 서비스 보호 기능을 제한하지는 않았습니다. • Flooding 공격 - 잘 구성되었지만 서명이 불량한 API 호출을 엄청나게 수신, 고속 패킷 Flooding • 소프트웨어 / 논리적 공격 - 애플리케이션 수준 공격 • 분산 공격 - 다중 위치로부터 Flooding 공격 • 의도치 않은 서비스 거부 - 사용량이 엄청나게 증가 **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SC-05 SOC 2 – Section IV PCI DSS v3.0 Requirement 5
MC-3	악성 코드 제어	주변 보안 도구(침입 탐지/방지 시스템 및 애플리케이션 방화벽 포함)는 내부 네트워크로 침입하기 전에 악성 코드를 차단해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14	검사관은 Amazon EC2 인스턴스상의 맬웨어 방지 소프트웨어를 물리적 시스템과 비슷한 방식으로 검토해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 침입 탐지 관련 정책 및 절차, 그리고 해당 정책/절차에 AWS 서비스가 포함되는지 확인	고객은 AWS 네트워크에 접근이 불가능하며, 물리적으로 해당 고객만을 위한 전용 네트웍 보안 장비 등을 구성해 주지 않습니다. 하지만 EC2 인스턴스를 고객의 EC2 환경 내에서 논리적 네트워크 세그먼트로 구현할 수 있습니다.	AWS 보안은 다음 유형의 서비스 거부 공격을 정의했지만 이에 대한 서비스 보호 기능을 제한하지는 않았습니다. • 홍수 공격 - 잘 구성되었지만 서명이 불량한 API 호출을 엄청나게 수신, 고속 패킷 홍수 • 소프트웨어 / 논리적 공격 - 애플리케이션 수준 공격 • 분산 공격 - 다중 위치로부터 홍수 공격 • 의도치 않은 서비스 거부 - 사용량이 엄청나게 증가 **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SC-05 SOC 2 – Section IV PCI DSS v3.0 Requirement 1 & 6

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
침입 탐지 및 대응						
IDS-1	침입 탐지 및 대응	조직이 고객 정보 시스템에 대한 무단 액세스를 모니터링하는 침입 탐지 시스템을 배포했습니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14	검사관은 Amazon EC2 인스턴스의 호스트 기반 IDS를 물리적 시스템에서와 비슷한 방식으로 검토해야 합니다. AWS가 네트워크에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디에서 검토할 수 있는지는 AWS 제공 증거를 참조하십시오. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직의 IDS 관련 정책 및 절차 및 AWS 서비스 내에서 IDS의 구현.	고객은 AWS 네트워크에 접근이 불가능하며, 물리적으로 해당 고객만을 위한 전용 네트웍 보안 장비 등을 구성해 주지 않습니다. 하지만 호스트 기반 침입 탐지를 EC2 인스턴스에서 구현할 수 있습니다. 참조: 보안 리소스	AWS는 성능 측정치 및 추세를 측정하기 위해 모니터링 도구를 사용합니다. 이때 보안 및 서비스 팀 소유자가 수집된 통계를 활용하여 시스템의 이상 거동을 평가합니다. 시스템에는 대상 호스트에서 실행되며 측정치를 수집하고 경보 사양을 기준으로 측정치를 평가하는 모니터링 에이전트가 통합되어 있습니다. 측정치는 온라인 콘솔을 통해 제공되며, 모든 Amazon 서비스 소유자가 현재 상태를 확인하고 향후 추세를 분석하기 위해 활용할 수 있습니다. 또한, 문제 티켓 또는 이메일 알림을 생성하도록 경보를 구성할 수도 있습니다. 호스트 기반 측정치는 1분 간격으로 제공됩니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IR-04 SOC 2 – Section IV PCI DSS v3.0 Requirement 11
IDS-2	침입 탐지 및 대응	침입 탐지 장치를 사용하여 방화벽에서 수행되는 모든 작업과 방화벽 통과가 허용되는 모든 트래픽을 모니터링해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: M p. A22-A25	AWS 서비스를 위한 모든 네트워크는 AWS가 관리합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거.	고객은 AWS 네트워크에 접근이 불가능하며, 물리적으로 해당 고객만을 위한 전용 네트웍 보안 장비 등을 구성해 주지 않습니다. AWS 보안 그룹 관리는 AWS API를 통해 모니터링할 수 있습니다.	AWS는 방화벽 및 기타 경계 장치를 포함한 모든 네트워크 장치를 모니터링합니다. 네트워크 장치는 시스템의 외부 경계 및 주요 내부 경계에서 통신을 모니터링하고 제어합니다. **참조**: NIST SP 800-53 rev.3 FedRAMP Control: SC-07 SOC 2 – Section IV PCI DSS v3.0 Requirement 11

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
IDS-3	침입 탐지 및 대응	침입 시도를 탐지하기 위해 IDS/IPS 로그를 저장하고 모니터링합니까?	FFIEC AUD Booklet(2012) Appendix A: Tier II: D p. A13-A15	Amazon CloudWatch를 통해 조직이 Amazon EC2 인스턴스, Amazon EBS 볼륨, Elastic Load Balancers, Amazon RDS DB 인스턴스를 비롯한 AWS 리소스를 실시간으로 모니터링할 수 있습니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** 1. 조직의 CloudWatch 사용 및 구성, 그리고 로그를 저장 및 보호하는 방식.	고객은 AWS 네트워크에 접근이 불가능하며, 물리적으로 해당 고객만을 위한 전용 네트웍 보안 장비 등을 구성해 주지 않습니다. 하지만 호스트 기반 침입 탐지를 EC2 인스턴스에서 구현할 수 있습니다. 마찬가지로 고객은 고객의 EC2 환경 내에서 로깅을 구현할 책임이 있습니다.	스토리지의 경우, AWS Acceptable Encryption Standard는 자격 증명 및 키 저장을 위해 승인된 방법을 지정합니다. 다음 항목이 포함됩니다. ▪ Odin - AWS에서 개발한 보안 키 및 자격 증명 관리자 ▪ Window DPAPI ▪ MAC OS X Keychain ▪ Password Safe ▪ Thales nShield 하드웨어 보안 모듈 **참조**: NIST SP 800-53 rev.3 FedRAMP Control: IA-05 SOC 2 – Section IV PCI DSS v3.0 Requirement 10
문서 및 인벤토리						
DI-1	문서 및 인벤토리	네트워크는 원격 및 퍼블릭 액세스를 포함하여 완전히 문서화되며, 승인된 담당자에게만 문서가 제공됩니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: B p. A12-A14 FFIEC OPS Booklet(2004) Appendix A: Objective 4 p. A3-A4	검사관은 인벤토리 문서에 AWS 서비스와 Direct Connect 및 VPN 연결이 포함되어 있는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** AWS Config는 AWS 리소스 인벤토리, 구성 기록 및 구성 변경 알림에 대해 보고합니다.	**감사 지침:** 모든 관련 시스템 및 AWS 서비스에 대한 시스템 인벤토리 및 문서를 제공합니다. **구현 지침:** 물리적 시스템의 인벤토리 및 문서 이외에 고객은 모든 AWS 리소스의 인벤토리 및 문서와 AWS 서비스 관리 프로세스에 대한 인벤토리 및 문서도 유지해야 합니다.	**참조:** SOC 2 – Section IV PCI DSS v3.0 Requirement 1
DI-2	문서 및 인벤토리	모든 중요 시스템의 인벤토리가 유지되고 필요시 업데이트됩니까?	FFIEC OPS Booklet(2004) Appendix A: Tier II: A p. A11-A12	검사관은 인벤토리 문서에 Amazon EC2 인스턴스가 포함되는지 확인해야 합니다. **검사관은 다음 항목을 요청 및 검토해야 합니다.** AWS Config는 AWS 리소스 인벤토리, 구성 기록 및 구성 변경 알림에 대해 보고합니다.	**감사 지침:** 모든 관련 시스템 및 AWS 서비스에 대한 시스템 인벤토리 및 문서를 제공합니다. **구현 지침:** 물리적 시스템의 인벤토리 및 문서 이외에 고객은 모든 AWS 리소스의 인벤토리 및 문서와 AWS 서비스 관리 프로세스에 대한 인벤토리 및 문서도 유지해야 합니다.	AWS는 구성 관리 도구를 사용하여 패키지, 패키지 그룹 및 환경에서 배포 가능한 소프트웨어를 관리합니다. 패키지 서비스란 서로 긴밀하게 결합된 소프트웨어, 콘텐츠 등 관련 파일의 모음입니다. 패키지 그룹이란 흔히 함께 배포되는 패키지 세트를 말합니다. **참조:** SOC 2 – Section IV PCI DSS v3.0 Requirement 2

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
DI-3	문서 및 인벤토리	비즈니스 목적을 달성하기 위한 중요도 및 민감도에 따라 정보를 분류하는, 시스템 복잡성에 적합한 정보 분류 프로그램이 있습니까? 민감도 및 중요도에 비례하는 제어는 이러한 분류를 기반으로 해야 합니다. 미디어 취급 및 폐기 정책은 전반적인 분류 전략을 반영해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: L p. A21-A22 FFIEC OPS Booklet(2004) Appendix A: Objective 5 p. A4-A5	검사관은 정보 분류 정책 및 프로세스가 AWS 서비스와 Amazon EC2 인스턴스를 포함하는지 확인해야 합니다.	**감사 지침:** 정보 분류 프로그램 설명을 제공합니다. **구현 지침:** AWS 서비스 및 관리가 정보 분류 정책 및 프로세스에서 관리하는 시스템 및 미디어의 범위에 포함되어야 합니다.	AWS 데이터 취급 표준에서는 AWS 고객 정보를 중요 정보로 정의하고 있습니다. 이 표준에서 규정된 AWS 데이터 취급 요건은 AWS 중요 정보를 전송 및 저장 상태에서 암호화하도록 요구하고 있으며 액세스, 액세스 제어, 액세스 로깅 및 물리적 제어 관련 요구 사항을 정의하고 있습니다. **참조:** SOC 2 – Appendix I PCI DSS v3.0 Requirement 12
물리적						
PS-1	물리적 보안 제어	조직이 정의된 물리적 보안 구역(시설, 데이터 센터, 민감 작업 구역 및 워크스테이션)을 운영하고 각 구역에서 적절한 예방 및 탐지 제어를 구현했습니까? 보안 구역에서 다음이 구현되어야 합니다. - 승인되지 않은 개인의 물리적 침입을 방지 - 환경 오염 물질로부터 보호 - Tempest 공격, 불법 무선 액세스 지점 및 전자기 간섭으로부터 보호	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5 FFIEC IS Booklet(2006) Appendix A: Tier II: E p. A16 FFIEC OPS Booklet(2004) Appendix A: Tier II: E p. A13-A14	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	AWS는 "AWS 물리적 및 환경 보호 정책"이라고 하는 공식적으로 문서화된 물리적 및 환경 보호 정책을 마련했습니다. 당사의 인증 및 보고서를 요청하면 추가적인 세부 정보를 검토할 수 있습니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
PS-2	물리적 보안 제어	데이터 센터가 다음과 같은 충분한 억지 제어에 의한 외부 침입으로부터 보호됩니까? - 데이터 센터 보안문 및 창 - 데이터 센터에 사이니지를 설치하거나 외부인이 용이하게 식별할 수 있는 지정을 하지 않아야 합니다. - 데이터 센터는 다음과 같은 충분한 탐지 제어로 보호해야 합니다. 물리적 침입 탐지 시스템, 경보, 동작 감지기, CCTV 및 기타 감시 시스템 - 네트워크 운영 센터는 민감한 위치로 간주해야 하며 물리적 접근을 승인된 개인으로만 제한해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: E p. A16 FFIEC OPS Booklet(2004) Appendix A: Tier II: E p. A13-A14	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	IT 인프라 구성 요소가 상주하는 모든 AWS 데이터 센터, 공동 건물 및 POP 시설에 대한 물리적 접근은 업무를 수행하기 위해 접근이 필요한 승인된 데이터 센터 직원, 공급업체 및 계약업체로 제한됩니다. 당사의 인증 및 보고서를 요청하면 추가적인 세부 정보를 검토할 수 있습니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-3	물리적 보안 제어	이중 바닥, 소화 시스템, 연기 탐지기, 정전기 방지 바닥 등이 환경 위험을 완화해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: E p. A16 FFIEC OPS Booklet(2004) Appendix A: Objective 7 p. A6 FFIEC OPS Booklet(2004) Appendix A: Tier II: D p. A13	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	AWS 데이터 센터는 Tier III 데이터 센터 시설이며, 구성 요소 장애 시 시스템 가용성을 보장하기 위해 N+1 중복성 아키텍처를 구현했습니다. 당사의 인증 및 보고서를 요청하면 추가적인 세부 정보를 검토할 수 있습니다. **참조:** SOC 2 – Section III, Area C

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
PS-4	물리적 보안 제어	보안 구역을 출입하는 직원은 적절한 ID를 패용하고 출입을 승인받아야 합니다.	FFIEC IS Booklet(2006) Appendix A: Tier II: E p. A16 FFIEC OPS Booklet(2004) Appendix A: Tier II: E p. A13-A14	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	데이터 센터 시설에 물리적으로 접근할 수 있도록 승인된 담당자에게 전자식 출입 배지(직원, 공급업체 또는 계약업체에 고유) 및 PIN을 포함한 권한 부여 자격 증명이 제공됩니다. 당사의 인증 및 보고서를 요청하면 추가적인 세부 정보를 검토할 수 있습니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-5	물리적 보안 제어	비공개 구역을 출입하는 모든 방문자는 적적한 ID를 패용해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Tier II: E p. A13-A14	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	AWS는 긴급 수리 또는 데이터 센터 투어(일부 제한적 상황)와 같은 합법적인 업무 목적으로 이러한 권한이 필요한 공급업체, 계약업체 및 방문자에게만 데이터 센터 접근 권한 및 정보를 제공합니다. 당사의 인증 및 보고서를 요청하면 추가적인 세부 정보를 검토할 수 있습니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-6	물리적 보안 제어	방문자 출입이 기록됩니까? 그렇다면 이 로그가 30일 이상 유지됩니까?	FFIEC AUD Booklet(2012) Appendix A: Tier II: D A13-A14	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	AWS Utility Computing Services 부사장이 모든 방문자 요청을 승인해야 합니다. 이 요청에는 투어 그룹 인원의 전체 목록, 투어 요청 사유, 투어 효과가 포함되어야 합니다. 이 승인된 요청서의 사본이 데이터 센터 출입 승인 전에 AWS Ticketing System 티켓에 첨부 문서로 포함됩니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
PS-7	물리적 보안 제어	조직 구내에서의 모든 하드웨어 및 소프트웨어 이전에 대해 공식 절차가 수립되어 있어야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Tier II: E p. A13-A14	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	데이터 센터로 배송되고 데이터 센터가 시스템 경계 내에서 수령하는 서버, 랙, 네트워크 장치, 하드 드라이브, 시스템 하드웨어 구성 요소, 건축 자재 등 모든 정보 시스템 구성 요소는 사전에 데이터 센터 관리자에게 알려 승인을 받아야 합니다. 서비스 소유자가 물리서버 클러스터, 하드웨어를 관리하고, 랙 입고 효율성과 같은 측정치를 제공하는 인프라 자동화 도구가 사용됩니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-8	물리적 보안 제어	네트워크 장치, 네트워크 케이블 및 배선과 같은 모든 통신 장비는 민감한 위치로 간주해야 하며 물리적 접근을 승인된 개인으로만 제한해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 8 p. A7-A8 FFIEC OPS Booklet(2004) Appendix A: Tier II: D p. A13	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	AWS에서는 데이터 센터 액세스를 위한 멀티 팩터 인증 메커니즘과 승인된 개인만 AWS 데이터 센터에 출입하도록 허용하는 추가 보안 메커니즘을 이용합니다. 승인된 직원/계약업체는 카드 리더에 자신의 배지를 사용하고 고유 PIN을 입력해야만 출입이 승인된 해당 시설 및 작업실에 접근할 수 있습니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-9	물리적 보안 제어	네트워크 케이블 및 배선은 유지 관리, 수리 및 업그레이드가 용이하도록 자세히 문서화하고 물리적으로 정리해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 8 p. A7-A8	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	옥내 전송 선로(노출 및 비노출)와 옥외 케이블은 보안 전선관을 사용하여 우발적 손상, 중단 및 물리적 훼손으로부터 보호해야 합니다. **참조:** SOC 2 – Section III, Area C

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
PS-10	물리적 보안 제어	조직은 운영 체제 액세스를 제공하는 모든 단말기가 물리적으로 안전하고 감시되는 환경에 위치하도록 해야 합니다.	FFIEC IS Booklet(2006) Appendix A: Objective 4 p. A4-A5	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	시스템들(서버에 연결될 수 있음)이 데이터 센터 내에서 사용되는 유일한 출력 장치입니다. 이러한 시스템은 물리적 출입 장치(배지 리더)로 보호되어 배지 및 PIN 인식이 성공해야 입실할 수 있는 데이터 센터 서버실 안에만 배치됩니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-11	물리적 보안 제어	PC 또는 워크스테이션이 화면보호기 암호 또는 자동 세션 종료 기능을 사용해 무단 사용을 방지합니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: D p. A15-A16	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	AWS는 "AWS 식별 및 인증 정책"이라고 하는 AWS에 적용되는 공식적이고 문서화된 식별 및 인증 정책을 마련했습니다. 여기에 자동 세션 종료 기능이 포함됩니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 8
PS-12	물리적 보안 제어	시설 주변은 충분한 조명, 펜스, 가드, 비디오 감시, 경보 등 적절한 억지 및 탐지 제어로 보호되어야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Tier II: E p. A13-A14	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	AWS 데이터 센터는 Tier III 데이터 센터 시설이며, 구성 요소 장애 시 시스템 가용성을 보장하기 위해 N+1 중복성 아키텍처를 구현했습니다. 따라서 구성 요소(N)는 적어도 하나의 독립적인 백업 구성 요소(+1)를 가집니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
PS-13	물리적 보안 제어	경영진은 고정 자산 추적 시스템을 사용하여 모든 중요 및 귀중 장비의 인벤토리를 관리해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Tier II: A p. A11-A12	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	데이터 센터로 배송되고 데이터 센터가 시스템 경계 내에서 수령하는 서버, 랙, 네트워크 장치, 하드 드라이브, 시스템 하드웨어 구성 요소 및 건축 자재를 포함하는(이에 제한되지 않음) 모든 정보 시스템 구성 요소는 사전에 데이터 센터 관리자에게 알려 승인을 받아야 합니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 2
PS-14	물리적 보안 제어	경영진이 기밀 문서 인쇄본 파괴 및 폐기 전 전자 미디어 복구 불능 삭제에 대해 규정하는 미디어 폐기 정책 및 절차를 수립했습니까?	FFIEC IS Booklet(2006) Appendix A: Tier II: D p. A15-A16 FFIEC OPS Booklet(2004) Appendix A: Objective 5 p. A4-A5	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	AWS는 이동식 스토리지 또는 고정식 스토리지를 불문하고 모든 형태의 디지털 미디어를 복구 불능 방식으로 삭제합니다. AWS 시스템은 출력된 인쇄물 형태로 서비스를 제공하지 않기 때문에 비디지털 미디어를 복구 불능 방식으로 삭제하고 있지 않습니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 9
PS-15	물리적 보안 제어	경영진이 중요 데이터의 이동을 방지하기 위한 모바일 컴퓨터 및 이동식 미디어 관련 정책을 유지합니까?	FFIEC OPS Booklet(2004) Appendix A: Tier II: E p. A13-A14	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	자기식, 비자기식 및 하드카피 미디어 유형은 데이터 저장에 사용되지 않으며, 따라서 AWS 서비스 경계 외부로 이동하지 않습니다. **참조:** SOC 2 – Section III, Area C PCI DSS v3.0 Requirement 12

제어	제어 영역	제어 목표	제어 참조	검사관 지침	고객 지침	AWS 증거
환경적						
EC-1	환경 제어	컴퓨팅 장비(특히 중요 시스템)는 무정전 전원 공급 장치(UPS)를 사용해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 7 p. A6 FFIEC OPS Booklet(2004) Appendix A: Tier II: D p. A13	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	AWS 데이터 센터는 Tier III 데이터 센터 시설이며, 구성 요소 장애 시 시스템 가용성을 보장하기 위해 N+1 중복성 아키텍처를 구현했습니다. 따라서 구성 요소(N)는 적어도 하나의 독립적인 백업 구성 요소(+1)를 가집니다. AWS는 액티브-액티브 구성 요소 방식의 N+1 중복성을 채택하므로, 다른 모든 구성 요소가 정상 작동하더라도 백업 구성 요소가 활성 상태를 유지합니다. **참조:** SOC 2 – Section III, Area C
EC-2	환경 제어	연료를 사용하는 백업 시스템은 적어도 2~3일간 전력을 공급할 수 있는 충분한 연료를 구비해야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 7 p. A6 FFIEC OPS Booklet(2004) Appendix A: Tier II: D p. A13	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	AWS 데이터 센터는 Tier III 데이터 센터 시설이며, 구성 요소 장애 시 시스템 가용성을 보장하기 위해 N+1 중복성 아키텍처를 구현했습니다. 따라서 구성 요소(N)는 적어도 하나의 독립적인 백업 구성 요소(+1)를 가집니다. AWS는 액티브-액티브 구성 요소 방식의 N+1 중복성을 채택하므로, 다른 모든 구성 요소가 정상 작동하더라도 백업 구성 요소가 활성 상태를 유지합니다. **참조:** SOC 2 – Section III, Area C
EC-3	환경 제어	운영 센터는 업무 및 장비 운전에 문제가 없도록 적절한 난방, 환기 및 냉방(HVAC) 솔루션을 갖춰야 합니다.	FFIEC OPS Booklet(2004) Appendix A: Objective 7 p. A6 FFIEC OPS Booklet(2004) Appendix A: Tier II: D p. A13	검사관은 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 어디서 검토할 수 있는지 자세히 보여주는 AWS 제공 증거를 검토해야 합니다.	AWS는 물리적 제어를 책임집니다.	데이터 센터 서버 및 네트워크실 내 온도 및 습도 수준은 ASHRAE(American Society of Heating, Refrigerating, and Air-Conditioning Engineers)에서 제정한 수준으로 유지 및 관리됩니다. **참조:** SOC 2 – Section III, Area C