Global Best Practices

클라우드 보안 감사 로드맵

조직이 하이브리드 및 멀티클라우드 환경으로 확장함에 따라, 도입 속도는 보안 프로그램의 성숙도를 앞지르는 경우가 많다. 이번 『Global Best Practices』에서는 AI 기반 워크로드와 복잡한 제3자 생태계로 정의되는 시대에 내부감사가 어떻게 검증 기능을 강화할 수 있는지를 살펴본다. 또한 통합 가시성 확보, 보다 강력한 ID(신원,접근권한) 거버넌스, 사전적 리스크 관리 등을 포함하여 클라우드 보안 격차를 해소하기 위한 실질적인 전략을 강조한다. 최고감사책임자(CAE)가 클라우드 시대의 민첩한 운영을 안전하게 보호하는 데 필요한 전문성과 프레임워크를 어떻게 구축할 수 있는지 알아본다.

클라우드 및 인공지능(AI) 기반 솔루션의 도입은 경쟁상 필수 요소이자 새로운 리스크의 원천이 되었다. 오늘날 대부분의 조직은 하이브리드 및 멀티클라우드 환경에서 운영되고 있으며, 혁신 기술과 제3자 제공업체를 통합하는 과정에서 복잡성이 더욱 가중되고 있다. 많은 조직은 끊임없이 진화하는 위협 환경에 발맞추는 데 어려움을 겪고 있다.

최근의 산업 연구와 실무자 설문조사는 클라우드 도입 속도와 보안 프로그램의 성숙도 사이의 격차가 점점 확대되고 있음을 보여준다. 이러한 과제를 더욱 심화시키는 것은 지속적인 역량 격차이다. 내부감사 기능과 사이버보안 전문가 모두 복잡한 멀티클라우드 아키텍처와 AI 기반 워크로드를 평가하고 관리하는 데 필요한 전문성을 개발하고 유지하는 데 어려움을 겪고 있다고 보고하고 있다.

이번 『Global Best Practices』는 현대적 클라우드 보안 내부감사 프로그램의 필수 요소를 살펴본다. 또한 최고감사책임자(CAE)를 위한 실질적인 권고사항을 제시하며, 클라우드 시대에 안전하고 민첩한 비즈니스 운영을 위한 기반으로서 통합된 가시성, 강력한 ID(신원,접근권한) 거버넌스, 사전적 리스크 관리를 강조하면서 전략을 재정비할 것을 제안한다.

클라우드 보안 감사를 수행할 때 내부감사는 회사의 클라우드 전략, 아키텍처 및 운영 환경을 평가해야 한다. 여기에는 조직

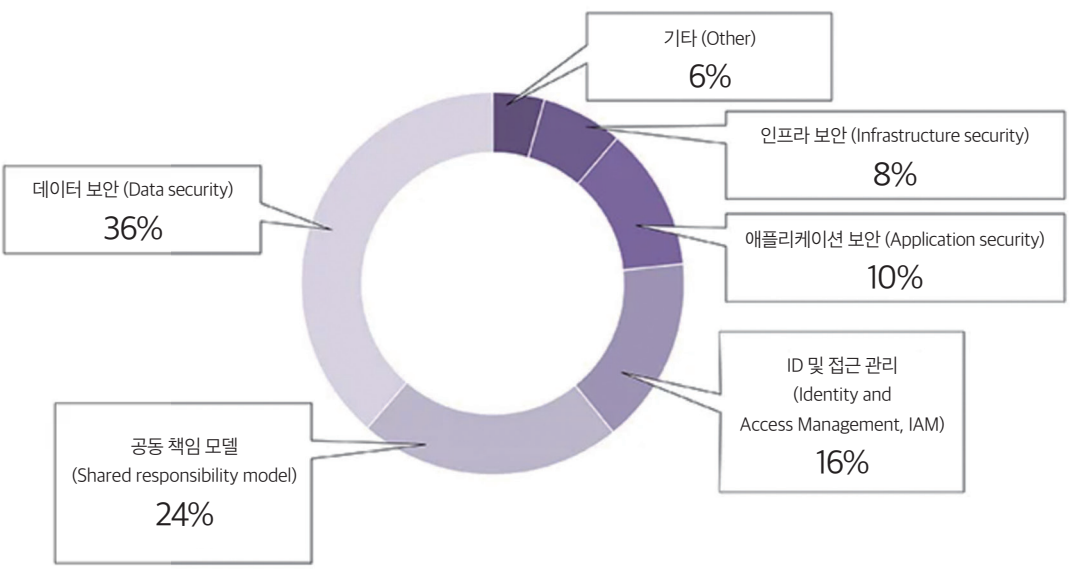
과 서비스 제공업체 간의 책임 구분뿐만 아니라 조직 내부의 책임 구분도 포함되며, 소프트웨어의 클라우드 마이그레이션과 프로비저닝 원칙, 그리고 진화하는 사이버보안 위협에 대응하는 제품·애플리케이션·데이터의 개발, 유지관리 및 보안도 이에 해당한다. 효과적인 클라우드 보안 내부감사 프로그램은 주요 기회와 과제를 식별하고, 클라우드 환경 내에서 내부감사의 역할을 정의하며, 민첩한 리스크 관리와 테스트를 적용하여 강력한 클라우드 보안 프로그램을 개발하고 유지한다.

클라우드 보안 감사의 과제

클라우드 환경은 막대한 기회를 제공하는 동시에 여러 리스크도 수반한다. Grant Thornton Advisors LLC의 리스크 자문 부문 전무이사인 Vikrant Rai는 내부감사인이 구성 관리를 포함하여 기능적 관점과 기술적 관점 모두에서 해당 환경을 이해해야 한다고 말한다.
일반적인 과제는 다음과 같다.

- 조직과 클라우드 서비스 제공자 간의 공유 책임 모델(Shared Responsibility Model)에 대한 거버넌스 및 이해가 제한적이거나 비공식적임.
- 이용 가능한 보안 도구와 구성의 최적화되지 않은 사용.
- 관리되지 않는 사용자 권한 및 자격 증명이 누적됨에 따라 발생하는 자격 증명 “확산(sprawl)”.
- 데이터 흐름에 대한 제한적인 가시성.
- 취약한 접근통제.
- 안전하지 않은 애플리케이션 프로그래밍 인터페이스(API) 통합.

최근 Grant Thornton Advisors LLC의 클라우드 보안 감사 웨비나에서 약 1,200명의 참석자를 대상으로 실시한 설문조사에 따르면, 데이터 보안과 공유 책임이 가장 큰 과제로 나타났다. 그림 A를 참조하기 바란다.



그림A

클라우드 환경의 복잡성을 이해하는 것은 어려울 수 있다. 조직이 기존 및 신규 기술, 솔루션, 그리고 제공업체를 통합함에 따라 내부감사는 역할, 역량 및 기타 요소의 보안성과 투명성을 보장해야 한다. Rai는 "현대 AI 워크로드의 막대한 연산 수요, 높은 데이터 처리량, 그리고 특수 하드웨어 요구사항으로 인해 전통적인 인프라나 단일 클라우드 환경만으로는 더 이상 요구사항을 충족할 수 없게 되었다. 이로 인해 복잡한 클라우드 컴퓨팅 환경의 도입이 더욱 가속화되었다"고 설명한다.

기술 발전과 빠르게 변화하는 서비스 자동화는 복잡성을 가중시키며, 내부감사가 클라우드 전략, 아키텍처 및 운영 환경을 포함한 클라우드 보안 프로그램을 감사하기 위해 고도화된 기술적 테스트 방법을 활용할 것을 요구한다. Grant Thornton Advisors LLC의 사이버 리스크 내부감사팀은 세 가지 감사 중점 영역과 그에 따른 과제를 식별하였다. 그림 B를 참조하기 바란다.

글로벌 클라우드 컴퓨팅 시장은 2024년 약 7,520억 달러 규모에서 성장하여 2030년까지 약 2조3천억 달러에 이를 것으로 전망된다. 2025년부터 2030년까지의 예상 연평균성장률(CAGR)은 20.4%이다.

출처: Grand View Research

클라우드 프로그램 거버넌스 (Cloud Program Governance)	데이터 보안 태세 관리 (Data Security Posture Management)	클라우드 보안 태세 관리 (Cloud Security Posture Management)
투명성과 책임소유 (Transparency & Ownership) - 성공적인 클라우드 기반 비즈니스 구현에 핵심적인 거버넌스가 제한적인 경우가 많다.	**데이터 자산에 대한 제한적인 가시성** (Limited visibility into data assets) - 클라우드 환경의 확장성은 조직이 데이터 자산(예: 섀도우 데이터 저장소, 방치된 데이터베이스)에 대한 가시성을 확보하는 데 어려움을 초래할 수 있다.	**기하급수적 성장에 따른 과제** (Challenges with exponential growth) - 클라우드 보안 관리는 지속적인 전투와 같으며, 이를 위해서는 강력한 기초 보안 아키텍처가 필요하다.
다중 환경과 섀도우 IT (Multiple environments and shadow IT) - 관리되지 않는 IT는 분산형 클라우드 모델로 인해 빠르게 통제 범위를 벗어날 수 있다.	**규제 미준수 리스크로 이어지는 부정확한 데이터 흐름** (Inaccurate data flows leading to risk of regulatory non-compliance) - 클라우드에 저장된 데이터 자산은 데이터가 이동함에 따라 노출 증가 위험에 처하게 되며, 이에 따라 규제 미준수 리스크가 발생한다.	**핵심 클라우드 보안 기능 감사** (Auditing key cloud security functions) - 접근 관리, 애플리케이션 보안, 암호화 및 키 관리와 같은 서비스와 기능을 감사하는 일은 기술적으로 어려울 수 있다.
공유 책임 모델 (Shared responsibility model) - 클라우드 서비스 제공업체(CSP)와 클라우드 서비스 고객(CSC) 간 역할과 책임이 명확히 정의되지 않으면 전체 클라우드 보안 태세에 공백이 발생할 수 있다.	**알려지지 않은 공격 경로** (Unknown attack paths) - 잘못된 ID 및 접근 구성, 구성 오류, 취약점이 발견되지 않은 채 존재하여 데이터 유출과 사이버 사고로 이어질 수 있는 상당한 리스크가 존재한다.	**클라우드 자원에 대한 제한적인 가시성** (Limited visibility of cloud resources) - 클라우드 자원에 대한 가시성과 통제가 제한적이어서, 구성 오류 예방 및 탐지 방식이 파편화되고, 그 결과 보안 사고가 증가하며 컴플라이언스를 유지하지 못하게 될 수 있다.

그림B

클라우드 보안 감사의 요소

내부감사는 조직이 강력한 클라우드 보안 태세 관리(CSPM)와 데이터 보안 태세 관리(DSPM)를 유지할 수 있도록 지원할 수 있다. Rai는 "변화하는 환경에서 보안 태세에 대한 통제를 유지할 수 있는 프로세스를 경영진이 구축하는 것이 매우 중요하다"고 말한다. 그는 이어 "포괄적인 평가를 위해 내부감사는 확립된 프레임워크를 활용하여 클라우드 전략, 아키텍처 및 운영 환경과 관련된 절차와 통제의 설계 및 운영 효과성을 평가해야 한다"고 설명한다. ("Cloud Security Frameworks" 참조.)

76%
의 조직은 측면 이동(lateral movement)을 가능하게 하는 최소 하나 이상의 외부 공개형 클라우드 자산을 보유하고 있으며, 이는 공격자가 고가치 목표에 도달할 수 있게 할 수 있다.

32%
의 클라우드 자산은 지원이 종료된 운영체제를 실행하거나 180일 이상 패치가 적용되지 않은 상태로 방치되어 있다. 공격자는 이를 이용해 공격 표면을 확대할 수 있다.

38%
의 조직은 민감한 데이터를 포함한 데이터베이스를 외부에 공개한 상태이다.

출처: 『Detect, Prioritize, Annihilate: Hunting Threats in the Age of Relentless Risk』, Orca Security, 「2025 State of Cloud Security Report」

클라우드 프로그램 거버넌스

클라우드 보안 감사 프로그램은 적용 가능한 연방, 주 및 지방 규제를 고려하는 동시에, 거버넌스와 전략, 즉 경영진의 접근방식, 역할과 책임, 정책 및 제3자 감독에 대한 이해와 평가에서 시작되어야 한다. 전기 장비 제조업체인 ChargePoint의 최고정보보호책임자(CISO) 겸 IT 총괄인 Rohan Singla는 "부적절한 거버넌스가 존재하거나 일관된 전략이 부족한 경우 보안팀은 클라우드 환경을 보호할 수 없다"고 말한다. 이러한 노력의 일환으로 내부감사는 조직이 확립된 클라우드 보안 전략과 구현 로드맵을 보유하고 있는지, 그리고 그것이 얼마나 자주 업데이트되는지를 판단해야 한다.

클라우드 보안의 또 다른 중요한 측면은 그것이 조직의 전반적인 보안 및 개인정보보호 전략과 태세에 어떻게 부합하는지를 이해하는 것이다. 클라우드 보안이 조직의 목표와 목적 달성을 어떻게 지원하는지를 판단하는 것도 고려되어야 한다.

책임의 결정

공유 책임 모델(shared responsibility model)은 하드웨어, 인프라, 데이터, 애플리케이션, 운영체제, 네트워크 통제 및 접근관리 등을 포함할 수 있는 영역에서 클라우드 서비스 제공업체와 고객이 보유하는 책임을 규정하며, 여기에는 조직 내부에서 공유 책임에 접근하는 고객의 방식도 포함된다. 클라우드 보안 감사는 각자의 책임이 문서화되어 있고, 이해되고 있으며, 수행되고 있는지를 판단해야 한다.

리스크 관리와 컴플라이언스에 대한 최종 책임은 클라우드 서비스 고객에게 있다. 내부감사는 조직이 통제 환경을 평가하기 위해 클라우드 서비스 제공업체의 시스템 및 조직 통제(SOC) 보고서를 확보하고 평가하는지를 판단해야 한다.

클라우드 보안 태세 관리(CSPM)

Rai는 "조직은 적절한 구현과 관리가 가능하도록 우수한 보안 관행이 클라우드 소프트웨어에 내재되어 있는지를 보장해야 한다"고 말한다. 클라우드 기술 플랫폼은 취약점 식별 및 해결을 포함하여 클라우드 보안 태세를 관리하는 데 도움이 되는 도구와 서비스를 제공하는 경우가 많지만, 해당 서비스와 도구가 적절하게 구성되고 활용되도록 보장하는 책임은 여전히 고객에게 있다. 내부감사인은 조직이 클라우드 서비스 제공업체와 협력하여 클라우드 배포 모델(SaaS, IaaS, PaaS)과 관련된 클라우

드 보안 리스크를 어떻게 모니터링하고 관리하는지를 이해해야 한다.
CSPM을 평가할 때의 초기 단계는 클라우드 환경에 대해 클라우드 고객과 서비스 제공업체가 수행하는 모니터링 활동을 평가하여, 그 범위와 경계가 현재의 클라우드 구현을 다루고 있는지를 판단하는 것이다. 잠재적 리스크가 중요도에 따라 적시에 적절하게 식별 • 보고 • 대응될 수 있도록, 모니터링 책임자의 역량과 능력을 고려해야 한다. Rai는 감사 프로그램의 후속 단계에서 내부감사인이 보안 프로세스와 구성, 그리고 클라우드 환경 내 데이터 보호 및 관리를 평가할 수 있다고 말한다.

데이터 보안 태세 관리(DSPM)

금융시장 참여자에게 청산, 결제 및 거래 보고 서비스를 제공하는 DTCC의 전무이사 겸 총괄 감사인인 Aadesh Gandhre는 "적절한 데이터 거버넌스를 갖추지 못하고 정의된 프레임워크를 도입하지 않는다면, 무결성, 무단 접근 및 가용성과 같은 여러 데이터 보안 문제에 노출될 수 있다"고 말한다. 그 결과, 클라우드 및 데이터 보안은 "조직의 대응 태세에 필수적인 요소가 되어야 한다."

클라우드 보안 프레임워크

내부감사인은 클라우드 보안 감사를 수행할 때 적용할 최적의 프레임워크를 고려함에 있어 다음과 같은 여러 선택지를 가질 수 있다.

- CSA(Cloud Security Alliance) 클라우드 통제 매트릭스(Cloud Controls Matrix).
- 미국 국립표준기술연구소(NIST) 사이버보안 프레임워크(Cybersecurity Framework).
- Amazon Web Services 클라우드 도입 프레임워크(Cloud Adoption Framework).
- 클라우드 서비스 제공업체 아웃소싱 가이드라인에 관한 유럽증권시장감독청(European Securities and Markets Authority) 최종 보고서.
- 정보보안 관리에 관한 ISO/IEC 27000 계열 표준.

기업이 자체 데이터센터에서 클라우드로, 또는 하나의 클라우드 플랫폼에서 다른 플랫폼으로 데이터를 이전할 때 데이터 보안이 간과될 수 있다고 Rai는 말한다. 기업은 관련된 정형 및 비정형 데이터세트를 식별할 수 있어야 하며, 저장 중(at rest) 및 전송 중(in motion) 데이터의 개인정보보호와 기밀성을 보호할 통제를 평가해야 한다. 데이터는 다음과 같아야 한다.

- 필요 시 권한이 부여된 사용자가 접근할 수 있어야 한다.
- 데이터 무결성이 보장될 수 있도록 보호되어야 한다.
- 적용 가능한 법률 및 규정을 준수하는 방식으로 관리되어야 한다.

클라우드 보안 감사에서 고려해야 할 기타 필수 사항은 다음과 같다.

- **ID 및 접근관리**. 여기에는 암호화와 키 관리 등의 이슈가 포함된다. Singla는 일부 조직이 여러 클라우드 환경을 사용하고 있다고 지적하며, 따라서 내부감사인은 조직이 사용자 인증에 대한 정의된 전략을 보유하고 있는지와 관련 가이드라인이 무엇인지를 고려해야 한다고 말한다.

- **위협 탐지 이벤트 모니터링**. Gandhre는 필요한 로그 분석을 강화하기 위해 AI 도구를 활용할 수 있다고 말한다.
- **제3자 리스크 관리**. 여기에는 공유 책임 모델과 관련된 리스크 대응이 포함된다.
- **로깅 및 모니터링**. 여기에서의 핵심 고려사항은 위협 또는 클라우드 환경 내 의심스러운 활동에 대한 알림인 중요 경고가 기록되고 있는지, 그리고 그것이 어떻게 처리되고 있는지 라고 Singla는 말한다.

Gandhre는 클라우드 보안 평가가 내부감사 계획의 핵심 구성요소가 되어야 한다고 강조하며, 그의 회사는 새로운 보안 이슈를 식별하기 위해 월 단위까지 포함한 지속적 모니터링을 수행하고 있다고 설명한다.

세계내부감사인협회(The IIA)의 Global Technology Audit Guide (GTAG), Auditing Identity and Access Management, 2nd Edition은 주요 용어와 함께 조직의 ID 및 접근관리 프로토콜이 잠재적인 보안 리스크를 완화할 수 있도록 감사 업무를 어떻게 수행해야 하는지를 설명한다. 이 지침서는 내부감사인이 IT 자원에 대한 접근관리를 위한 통제가 적절하게 설계되고 효과적으로 구현되었는지에 대한 보증을 제공할 수 있도록 지원한다.

일관성과 비교가능성

비즈니스 애플리케이션을 이해하고 이를 클라우드 제공업체, 배포 방식 및 서비스 모델(예: SaaS, IaaS, PaaS)별로 분류하는 것은, 통제 테스트에 활용할 수 있는 관련 프레임워크의 적절한 보안 통제를 식별하는 데 도움이 된다. 이러한 접근방식은 이후 클라우드 내 애플리케이션 전반의 보안 통제를 평가할 때 일관성과 비교가능성을 확보하는 데 활용될 수 있다. 그림 C를 참조하기 바란다.

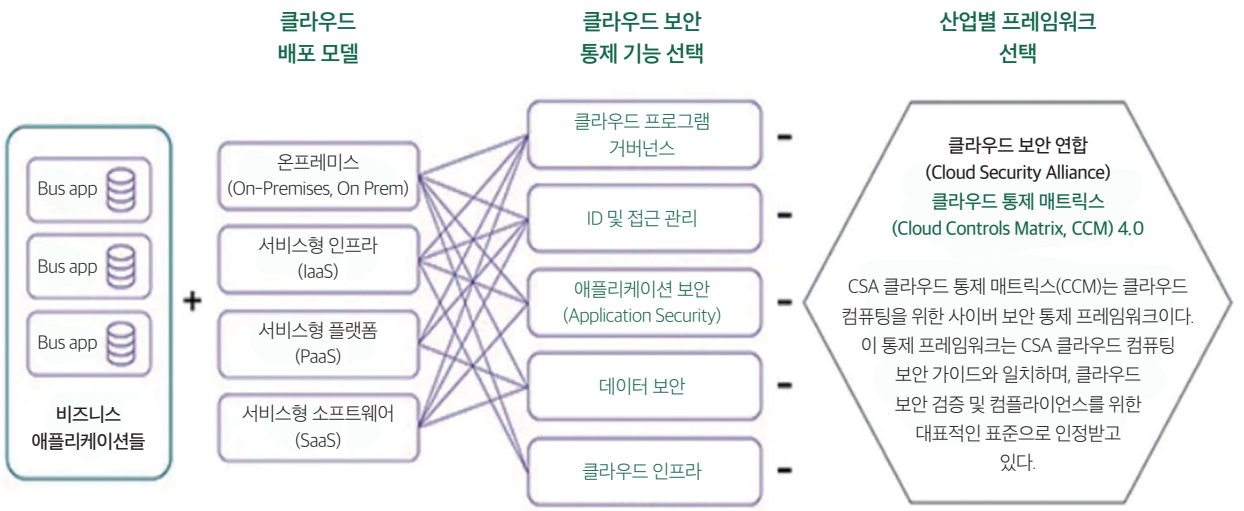


그림 C-1

CIS 벤치마크 / 선택된 프레임워크에 대해 통제를 평가

- 동종 조직 벤치마킹(peer benchmarking)과 함께 상세한 현재 및 목표 성숙도 모델을 제공한다.
- 식별된 개선 기회를 기반으로 클라우드 보안 평가를 수행한다.

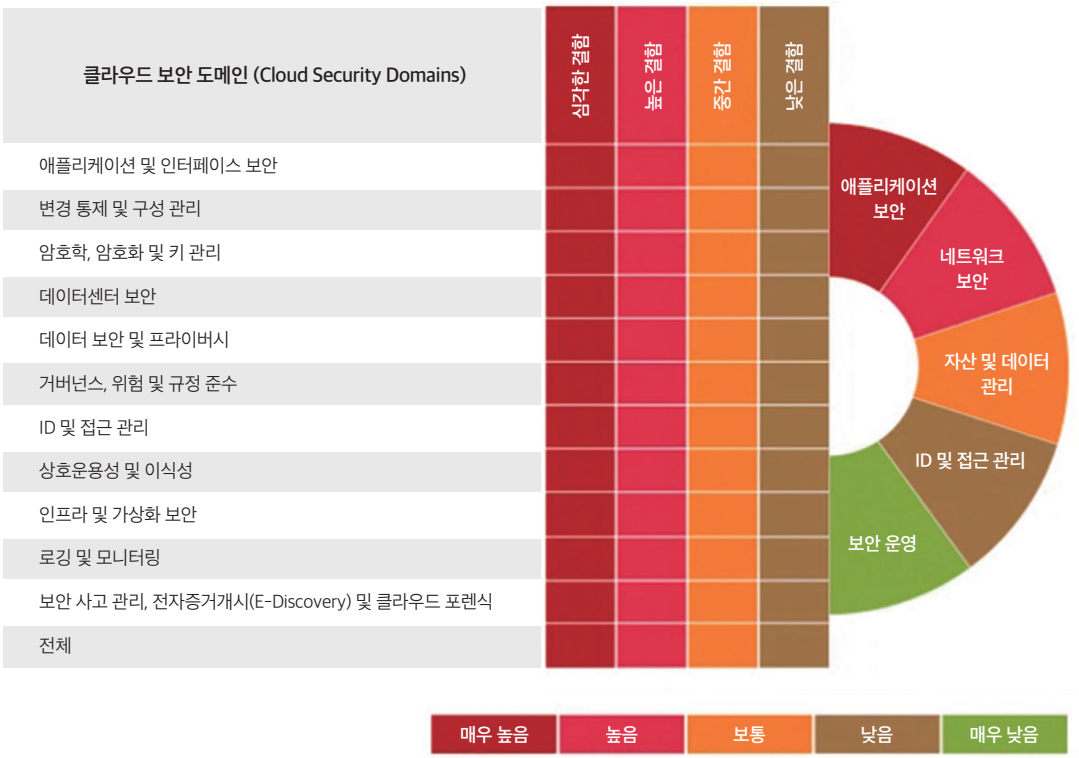


그림 C-2

다년간의 클라우드 보안 감사 프로그램을 수립하는 것은 핵심 비즈니스 환경을 이해하는 것에서 시작된다. 내부감사인은 먼저 비즈니스 우선순위와 함께, 클라우드 환경으로 이전될 것으로 예상되는 기존 및 미래의 비즈니스 애플리케이션을 평가해야 한다. 안전하고 지속적인 비즈니스 운영을 가능하게 하기 위해 클라우드 이전 전·후 전략이 고려되어야 한다. 그림 D를 참조하기 바란다.

다년도 클라우드 보안 감사 계획(예시)

		감사연도			클라우드 감사 중점 영역						
# 클라우드 보안 감사	리스크	1	2	3	CPG	IAM	APS	DSP	IVS	CSPM	DSPM
1 비즈니스 애플리케이션 1 (PII/PHI) (AWS)	C (Critical)	X		X	X	X	X	X	-	X	X
2 비즈니스 애플리케이션 2 (Azure)	C (Critical)	X		X	X	X	X	X	X	-	-
3 비즈니스 애플리케이션 3 (AWS)	H (High)	X			X	X	-	X	X	X	X
4 비즈니스 애플리케이션 4 (Azure)	M (Medium)		X		X	X	-	-	-	-	-
5 비즈니스 애플리케이션 5 (AWS)	M (Medium)		X		X	X	X	-	-	X	X
6 비즈니스 애플리케이션 6 (GCP)	L (Low)			-	X					-	

그림 D

Rai는 "클라우드 보안 감사 프로그램을 정의하는 데에는 많은 요소가 포함되며, 이를 성숙시키는 데에는 시간이 걸릴 수 있다"고 말한다. 그는 조직이 거버넌스 구성요소 평가부터 시작하는 단계적 접근방식을 취할 것을 권고한다. 이러한 신중한 접근방식은 내부감사가 거버넌스, 운영 모델, 그리고 공유 책임 모델을 신속하게 이해하고 평가할 수 있도록 해준다.

그는 이어 "클라우드 보안 감사 프로그램을 구축할 때는 클라우드 환경별, 주제 영역별 또는 이 둘의 교차 영역별로 클라우드 보안이라는 큰 주제를 적절한 규모로 나누는 것이 중요하다"며, "이를 통해 감사 범위를 관리 가능하게 하고 경영진이 통제를 구현·강화·집행할 시간을 확보할 수 있다"고 말한다. 감사인은 거버넌스, 구성 또는 데이터 보호 요소를 다루는 경우에도 확립된 프레임워크를 활용하여 적용 가능한 성숙도 요소와 통제를 평가할 수 있다.

내부감사의 역할

내부감사는 클라우드 보안 리스크를 완화하고 그 성숙도를 향상시키는 데 필요한 거버넌스, 리스크 관리 및 통제를 평가할 책임이 있으며, 이사회와 최고경영진에 투명성과 지원을 제공한다.
내부감사가 중요한 역할을 수행할 수 있는 여러 영역의 예시는 다음과 같다.

- 조직의 CSPM 및 DSPM 보안 솔루션 구현 현황, 관련 정책, 그리고 그것들이 조직의 필요와 선도적 관행(leading practice)에 부합하는지를 평가한다.
- 보안 전략, 아키텍처 또는 운영 환경의 주요 업데이트와 같은 이슈에 대해 경영진을 인터뷰한다.
- 경영진이 강력한 보안 기준선과 가이드라인을 개발하기 위해 구현할 수 있는 내부통제를 식별하도록 지원한다.
- 제3자의 통제, 정책 및 절차가 회사의 기대 수준에 부합하는지를 평가한다.
- 경영진이 적절한 인력이 계약 검토 및 협상에 참여하도록 보장할 것을 권고한다. 조직을 보호하고 제공업체와 생산적으로 협력하기 위해 중요한 계약상 고려사항에는 다음이 포함되며, 이에 한정되지 않는다.
  - 정의된 기간 내에 SOC 보고서를 발행하겠다는 약속.
  - 심각도에 따라 합의된 기간 내에 위협을 식별·보고·대응하기 위한 공식적인 서비스 수준 협약(SLA).
  - 서비스 제공업체와 고객 간 책임에 대한 명확한 규정.
  - 데이터 소유권 및 접근권, 감사 권한 등에 관한 서비스 제공업체의 규정을 이해하는 것.
- 널리 채택된 프레임워크를 기반으로 한 선도적 관행을 경영진에 제공하기 위해 자문 업무를 수행한다.

통합적 접근방식

Rai는 기술 환경의 상당 부분이 클라우드로 전환되고 있으며, 많은 AI 및 머신러닝 솔루션이 클라우드를 기반으로 구축되고 있다고 지적한다. 그는 "이러한 과제는 계속해서 증가할 것"이라고 말한다.
Gandhre에 따르면, 클라우드 보안 감사는 하나의 여정이며 협업이 중요하다. 그는 "단지 클라우드 보안을 위한 별도의 프로그램만 보유하는 것으로는 충분하지 않다"고 말한다. 클라우드 보안은 내부감사의 리스크평가 및 조직의 전사적 리스크 관리(ERM) 프레임워크와 연계되어야 한다.
Gandhre는 내부감사가 의사결정이 이루어지기 전에 질문을 제기하고 조언을 제공할 수 있도록, 리스크가 어떻게 평가되는지를 포함하여 초기 단계부터 클라우드 보안 관련 사항에 참여해야 한다고 말한다. 그는 "독립성이 고립을 의미하는 것은 아니다"고 강조한다.

면책조항

IIA는 본 문서를 정보 제공 및 교육 목적에 한해 발행한다. 본 자료는 특정 개별 상황에 대한 확정적인 해답을 제공하기 위한 것이 아니며, 동료 기반의 인사이트를 반영한 사고 리더십 자료로서 활용되는 것을 목적으로 한다. 이는 IIA의 공식 지침이 아니다. IIA는 특정 상황과 직접적으로 관련된 사항에 대해서는 독립적인 전문가의 자문을 구할 것을 권고한다. 본 자료에 전적으로 의존하여 발생하는 어떠한 결과에 대해서도 IIA는 책임을 지지 않는다.