Deloitte.

퍼블릭 클라우드 DNA의 보안 내재화 전략

2023년 10월
Deloitte Insights

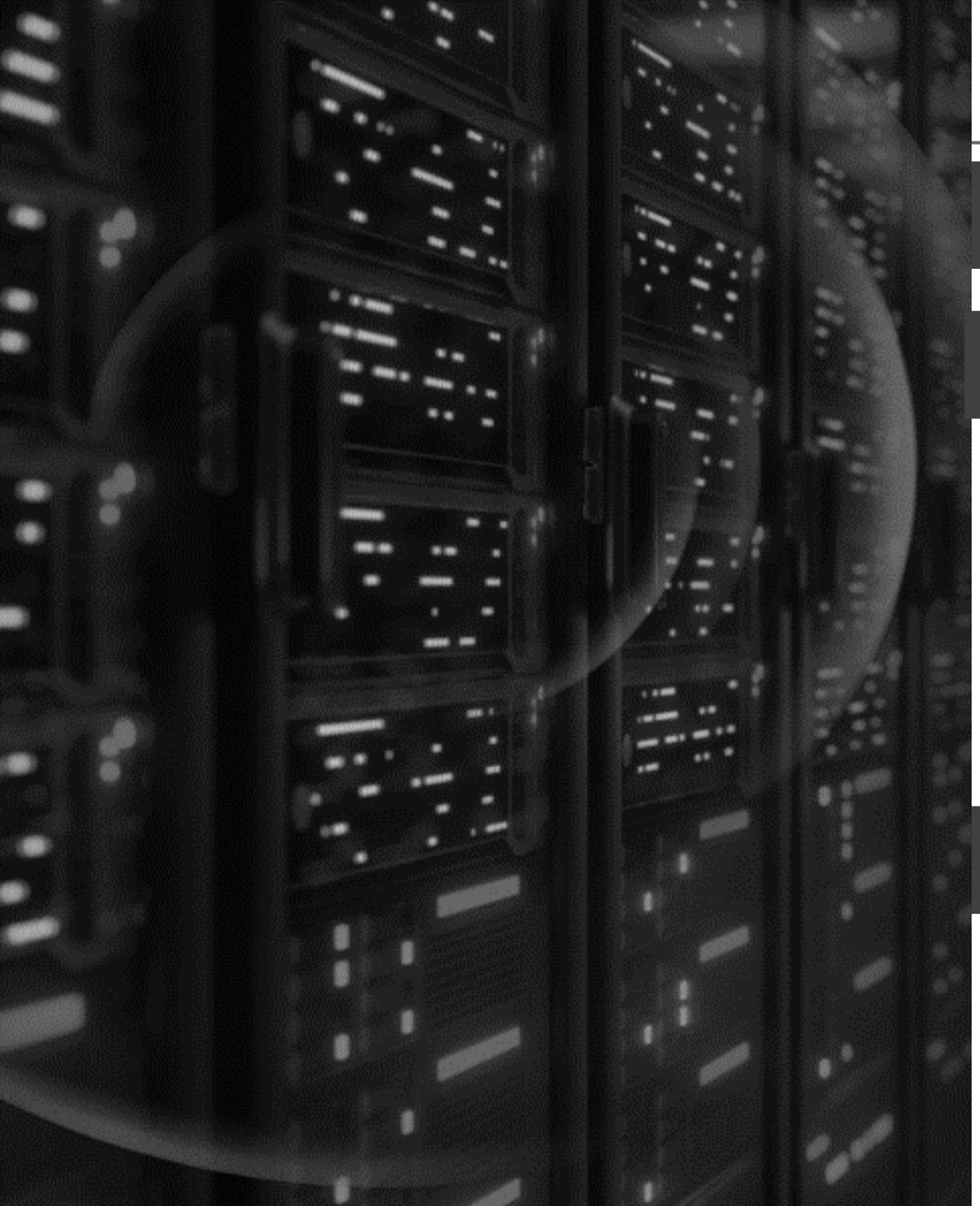


Table Of Contents

퍼블릭 클라우드 전환 시 주요 쟁점

퍼블릭 클라우드 전환 시 기업은 새로운 애플리케이션을 신속하게 도입하고 배치하여 업무 자동화를 가속화할 수 있지만,
기존 보안 시스템과의 호환성 문제와 효율성 저하 가능성을 사전에 파악하고 이를 해결하기 위한 리스크 관리 방안이 필요

업무 자동화 VS. 보안강화

퍼블릭 클라우드 전환 → 리스크 관리 방안 수립 필요

새로운 애플리케이션의 신속한 도입과 배치 실현

보안 문제는 후 순위

- API 활용해 업무 어플리케이션 설치 시간 단축
- 배포 파이프 라인 구축으로 추가 사양 설치 용이
- 비용과 성능 최적화 실현

기존 시스템과 호환성 문제와 효율성 저하 리스크 최소화

충분한 보안검증 필요

- 사전에 보안 요건 검토 후 보안 검증 과정을 E2E 프로세스에 통합
- 보안 솔루션과 클라우드 벤더 간 협의로 DevSecOps 도입 및 관리
- 보안 프로세스 전문인력 배치

퍼블릭 클라우드 전환의 주요 리스크와 관리 방안

	퍼블릭 클라우드 리스크	리스크 대응법
1	기존 비즈니스 정책과 IT 프로세스 고수	**퍼블릭 클라우드 리스크 관리 전략 수립**
2	애플리케이션 배포/적용 시 보안 위험 증가	클라우드 네이티브 서비스 활용하여 **클라우드 통제 환경 구축 및 실행**
3	보안사고 위험 누락 및 과소 평가 가능성	On-Promise프로세스와 클라우드 보안 통합으로 **사이버 보안 운영 범위 확대**
4	보안팀 한계를 넘는 애플리케이션 도입 범위와 속도 증가	**클라우드 보안 관리 자동화**
5	보안 관리 실무 인력의 부재 (외주화 지양)	비즈니스 프로세스와 기술 역량을 동시에 갖춘 **맞춤형 보안 전문 인력 양성**

리스크 대응안 – 1 퍼블릭 클라우드 리스크 관리 전략 수립

책임공유모델 기반으로 리스크 책임 범위 설정 및 운영/배포 관리

퍼블릭 클라우드 전환 시, 기업은 클라우드 서비스 공급자(CSP)와 리스크 책임 범위를 설정하고, 조직에 맞는 리스크 프레임워크를 활용한 평가 수행 및 리스크 관리 전략을 수립을 통해 애플리케이션 배포 시 서비스 유형별 인터페이스 상의 보안위험 관리 필요

1단계 CSP-사용자간 리스크 책임 범위 설정

CSP와 책임공유모델 (SRM) 구축

- NIST[1], CSA[2] 프레임워크 활용해 리스크 책임 범위 설정 및 표준화
  - 자사 배포 모델과 서비스 유형 고려
  - 자사 보안, 프로세스 등 인프라 성숙도 관련 벤치마크 실행

리스크 모델링

- 보안에 중점을 둔 발생 가능한 리스크 사례 식별 및 교육
- 사례를 참조한 보안 아키텍쳐, 전략 로드맵 및 실행 안 정립

보안 솔루션 도출

- 보안 규제와 클라우드 실행방식에 부합하는 보안 솔루션 도출/선정

2단계 조직 맞춤형 리스크 관리 전략 수립

리스크 관리 세부 영역 설정

- 사람, 프로세스, 기술 관점으로 클라우드 리스크 요소 파악
  - NIST 리스크 프레임워크 비교 및 참조
  - 사이버 리스크 영역별 리스크 요소 식별

리스크 평가 기준 마련

- NIST, CSA, 딜로이트 사이버 전략 프레임 워크 활용 (세부 지표 원문 참조)

평가 및 리스크 관리 전략 수립

- 업계 실행 방식과 비교 및 개선
- 조직 세부적 요소(핵심기술,사이버, 운영)의 리스크/성숙도 평가
- 클라우드 배포/적용의 맞춤형 아키텍쳐 설계 및 리스크 전략 수립

3단계 애플리케이션 배포 시 리스크 관리

평가 기준선 설정

- 업계 선도 앱 기준으로 평가
  - 클라우드/컨테이너 보안
  - 계정관리, 역할 책임
  - 정책/규제 준수 사항
- 리스크 결과 보고서 생성 (보안 취약점 확인 및 솔루션 선정)

애플리케이션 보안 평가 자동화

- CSPM[3], CWPP[4] 활용하여 배포 유형별 (IaaS, PaaS) 평가 자동화
- 서비스형 소프트웨어(SaaS)는 최종단계에 사용자 인수테스트(UAT) 실행

인터페이스 보안 위험 평가

- 전환 클라우드와 애플리케이션의 메타계층간 취약점 점검/평가
- 클라우드와 자체 솔루션, 워크로드, 관리포털 간 인터페이스 보안 점검

1) 미국표준기술연구소(National Institute of Standards and Technology)
2) 미국 클라우드 보안협회(Cloud Security Alliance)
3) 클라우드 보안 형상 관리(cloud security posture management)
4) 클라우드 워크로드 보호 플랫폼(cloud workload protection platform

리스크 대응안 – 2 클라우드 통제 환경 구축 및 실행

클라우드 환경의 보안 영역 식별 및 통제

애플리케이션 배포시 보안 취약성 해소를 위한 사용자 식별/접근관리 시스템과 DevSecOps를 구축하고, 제로트러스트 원칙하에 보안상 취약점 분석으로 애플리케이션 실행 전략 수립 및 클라우드 네이티브 서비스를 활용하여 데이터 보호 시스템 설계 및 운영

1단계 식별/승인 시스템 설계

클라우드 네이티브 서비스 활용

- 계정 접근 권한 관리 및 다중 단계 계정 인증 (MFA) 기능 제공
- 계정 손상, 악의적 공격, 컨피그 오류 등의 파괴적 이벤트의 '폭발 반경' (blast radius) 제한

On-Promise 프로세스와 통합

- 사용자·역할·권한, 인증/승인 등 세부 요건 정의 및 설계
- PIM[1]/PAM[2] 프로세스 구축
- 다중 단계 계정 로그인 과정 (MFA) 적용
- 식별/접근 권한 등 사용자 관리 프로세스 구축 및 실행

2단계 DevSecOps 구축 및 활용

자사 클라우드 성숙도 평가 분석

- 업계 표준과 클라우드 선도사를 기준으로 성숙도와 격차 분석
  - 보안 역량 평가
  - 클라우드 환경 통제 기능 분석

DevSecOps 설계, 실행, 운영 및 모니터링

- 클라우드 애플리케이션 보안 강화 실현
  - (핵심요소) 거버넌스, 사람, 프로세스, 기술
  - (구축 단계) 설계, 기획 개발, 구축, 테스트, 운영 및 모니터링

3단계 제로트러스트 원칙 도입

제로트러스트 범위 결정

- 사용자, 워크로드, 데이터, 네트워크 및 기기 등에 대한 보안 취약 요소 분석
- 원격측정/애널리틱스/자동화 및 오케스트레이션 구조 정립

제로트러스트 원칙 이행

- 제로 트러스트 환경 구축
  - 기기 보안 서비스 실행
  - 네트워크 보안/접근 제한
- 애플리케이션 실행 전략 수립
  - 가상화, 보안아키텍쳐 수립
  - 네트워크 보안 전략 수립

4단계 데이터 보호 시스템 설계

클라우드 네이티브 기능 활용

- 데이터 암호화/토큰화
- 전송 계층 보안 강화
- 클라우드 호스트 키 관리

데이터 보호 시스템 설계

- 매니지드 서비스 설계, 실행 및 배치
- 데이터 암호화, 전송, 저장 과정상의 보안 강화

1) PAM (Privileged Access Management)
2) PIM (Privileged Identity Management)

리스크 대응안 – 3 사이버 보안 운영범위 확대

On-Promise와 클라우드 서비스 통합

클라우드 서비스와 On-Promise상에서 운영 처리되는 모든 정보자산을 통합적으로 모니터링하고, 사용자 등의 보안 위반 사항을 실시간으로 대응할 수 있는 중앙집중화 된 프로세스와 솔루션 확보

1단계 사이버 공간내 정보 자산의 통합적 모니터링

정보자산 모니터링 역량 확보

- CSP의 로깅 및 모니터링 솔루션을 On-Promise와 연결/통합
- 보안 정보 및 이벤트 관리(SIEM) 솔루션 확보
- 단일 창 아키텍처 점검
- 데이터 보안 조치는 별도 수행

모니터링 활동의 중앙 집중화

- CSP가 제공하는 정보자산 모니터링 솔루션 및 관리방안 활용
  - 사용자 On-Promise 규제와 요구사항을 반영한 로그 스토리지 구축
  - 로그 엑스포트 구축
  - 민감 데이터 필터링 규정 정립
- 민감데이터 접근 사용자들의 로그 모니터링

2단계 보안 준수 사항 실시간 대응 처리 프로세스/솔루션 확보

IT 서비스 관리(ITSM) 시스템 구축

- 클라우드 보안 통제 프레임워크 (준수규정/기준/지표 포함) 수립
- CSPM과 CWPP를 사용자 On-Promise ITSM시스템에 통합
- 지속적인 지표/규정 업데이트
- 클라우드 네이티브 솔루션(CNAPP) 활용 안 검토

보안 리스크 실시간 모니터링

- 보안 위반/잠재위험 사항 실시간 식별
- DevSecOps 운영 수준을 목표 로 보안 이벤트 대응/처리 프로세스 정립

리스크 대응안 – 4 클라우드 보안 자동화

솔루션 기반 클라우드 자동화 실현

보안기준을 설정하여 어플리케이션을 클라우드 환경으로 이전 시 보안점검을 수행하고, 보안관리 자동화 솔루션의 전략적인 선택과 조직 SIEM 솔루션과의 연계 및 IaC내 보안 관리 패턴을 내재화 해 보안관리 활동을 상시 모니터링

1단계 보안 통제기준 설정 및 적용

보안 관리 대상 및 기준 설정
- 애플리케이션 보안 관련 기술 요소
- 제공되는 클라우드 서비스
- 보안 기준/정책/표준 설정

→ **보안 라이브러리 개발 지속 업데이트**
- 보안 패턴을 반영하여 라이브러리 개발
- 라이브러리 지속 업데이트

2단계 애플리케이션 탑재 시 보안 점검

보안 상태 점검
- 체크리스트 기반 점검
- 일회성 특정 시점(Time)과 특정 지점(Point) 보안 취약 요소 식별

→ **보안 강화 (Hardening)**
- 보안 취약점 파악 및 보완(이슈 해결)
- 보안 자동화 실행

3단계 보안 관리 자동화 실현

CSPM
- 인프라의 보안 위험을 자동식별

CWPP
- On-Promise 워크로드에 보안위험 자동식별

CIEM
- 클라우드내 원칙에근거한 신원및접근권한관리

CNAPP
- 클라우드 환경 모니터링 및 보안위험 탐지/보고

IaC
- 적정 인프라 설정/배치 및 DevSecOps로 오류 제거

→ **전략적 선택** → **보안 솔루션 구성**

4단계 보안관리 활동 상시 모니터링

조직내 SIEM 솔루션 활용
- 보안 자동 관리 솔루션을 자사의 이벤트 관리 (SIEM)솔루션에 내재화
- 보안 이벤트 발생시 보안팀/담당자 상시 알람

IaC 형 자체 보안 관리
- 인프라구축 시간단축
- 자동화에 따른 효율성 개선으로 중대한 보안 문제 수반 가능성

IaC구현 및 보안사고위험 방지

코드형 정책 (policy as code)
- 보안관리패턴을 코드형인프라(IaC)에 내재화
- 개발자 인프라 규모 산정 시 자동으로 취약사항 식별

1) 코드형 인프라(IaC, Infrastructure-as-Code) :퍼블릭 클라우드 및 프라이빗 데이터센터 등의 프로비저닝을 자동화 솔루션

리스크 대응안 – 5 맞춤형 보안 전문 인력 확보

맞춤형 교육과정 설계 및 경험 주도 학습 추진

조직의 실제 클라우드 보안 환경에 대한 교육 커리큘럼을 설계하고 경험 주도형 교육 실행으로 자사 맞춤형 보안 전문 인력 양성

1단계 맞춤형 교육 커리큘럼 설계

자사 보안 환경을 재현한 교육 과정 개발

- 클라우드 및 기술 관련 실무 인력 대상
- 조직 인프라 보호를 위한 보안 감각 학습 내용 포함
- 보안팀과 유관 부서의 커뮤니케이션 방안
- 사이버 공격 및 대응 방안

클라우드 보안 집중 과정 설계

- 지속적 컴플라이언스 및 보안 모니터링
- 보안 구성/ 성숙도 플래닝 (로드맵, SAST/DAST 등)
- DevSecOps 주제(설계, 도입, 운영 등)
- 제로 트러스트 성숙도
- 제로 트러스트 참조 아키텍처 설계

2단계 조직의 목표와 교육 커리큘럼 통합

보안 관리 특수상황 설정

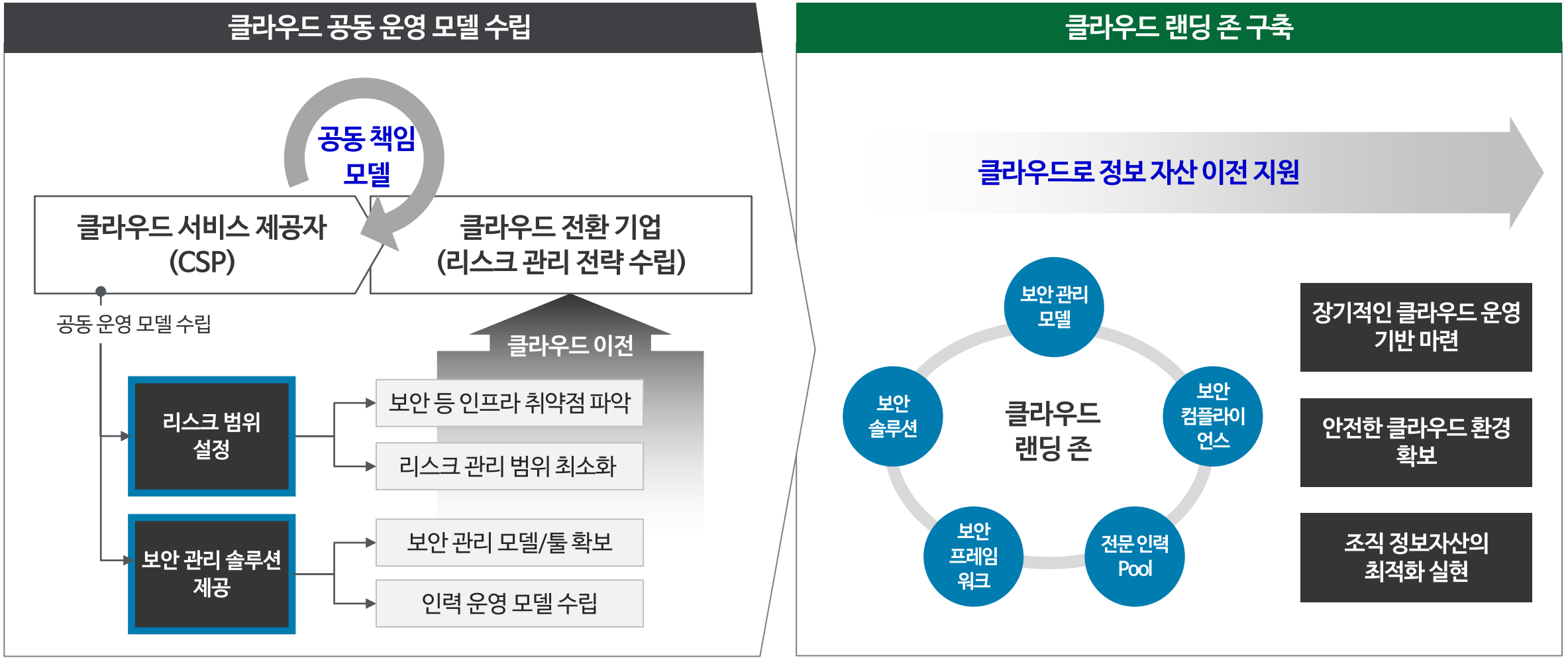
- 새로운 플랫폼 적응 등 조직 내 특수한 상황 설정(랩) 및 교육

경험 기반 교육 실행

- 실행 가능한 보안 솔루션 또는 프로토타입 개발
- 프로토타입 솔루션 실행으로 보안 대응 상황 경험

퍼블릭 클라우드 사이버 보안 위험 관리 방안

퍼블릭 클라우드사와 공동 운영 모델을 적용하여 리스크 관리 전략의 수립하고 랜딩존 구축함으로써 장기적이고 안전한 클라우드 운영 기반 마련 및 정보자산의 최적화 실현



Deloitte.
Insights

딜로이트 안진회계법인·딜로이트 컨설팅
성장전략 본부

손재호 Partner
고객산업본부 본부장
jaehoson@deloitte.com

정동섭 Partner
딜로이트 인사이트 리더
dongjeong@deloitte.com

김사헌 Director
딜로이트 인사이트 편집장
sahekim@deloitte.com

HOT LINE
02) 6099-4651