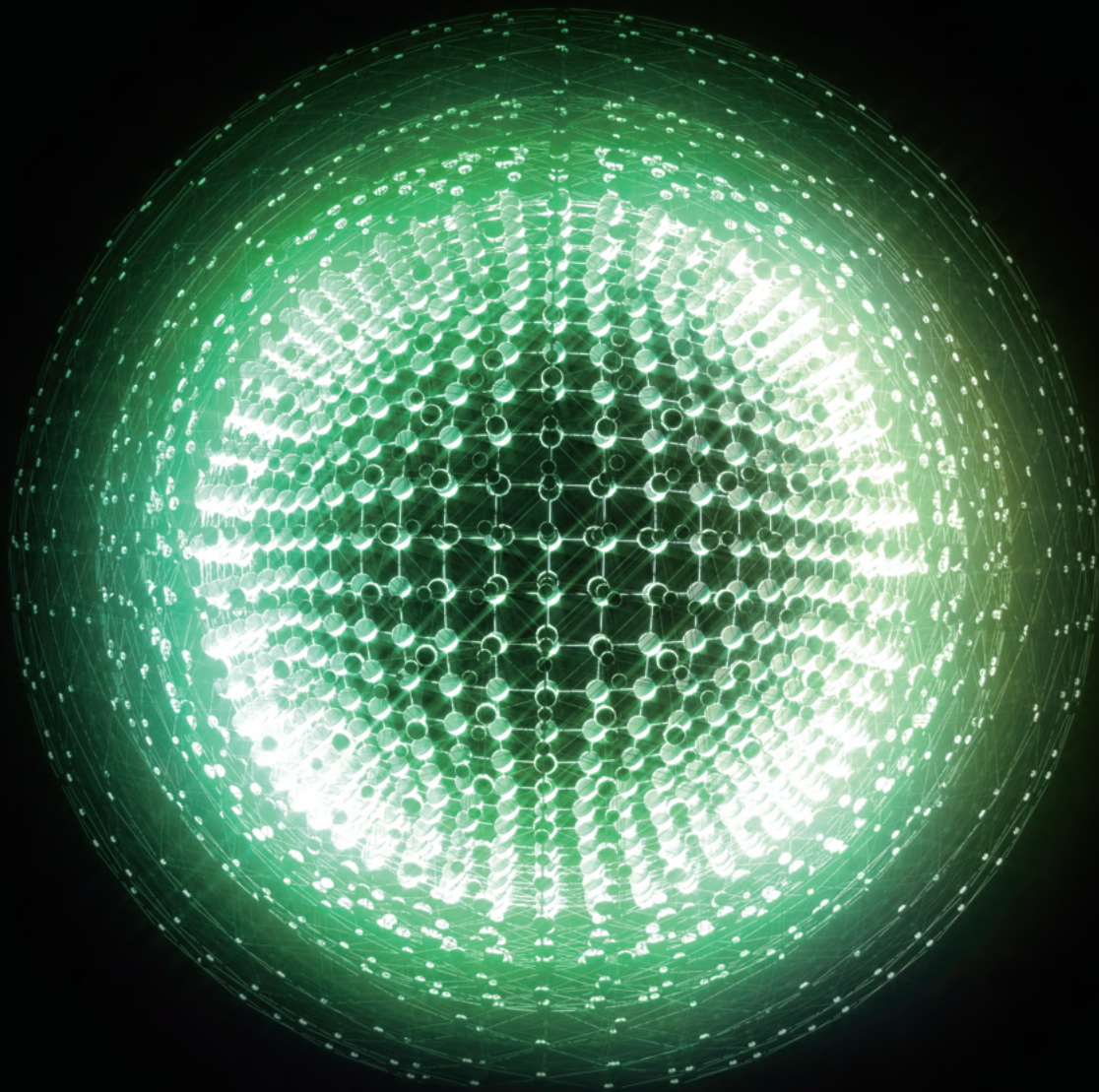


Deloitte.



Virtual CISO 서비스

보안 리더십 공백,
vCISO로 전략수립부터 실행 · 모니터링까지

한국 딜로이트 그룹 | One Cyber & Resilience

Virtual CISO 서비스

보안 리더십 공백,
vCISO로 전략수립부터 실행 · 모니터링까지

목차

급증하는 사이버 위협과 기업의 보안 리더십 공백	3
왜 지금, CISO가 필요한가	4
단일 역할이 아닌 복합 리더십으로서의 CISO	5
vCISO 서비스 활용 시 기대 효과	6
vCISO 도입 효과 - 정량적 비교	7
vCISO 수행 조직 구조	8
딜로이트 vCISO 서비스	9
Why Deloitte? + Contact	11

급증하는 사이버 위협과 기업의 보안 리더십 공백

사이버 위협은 기하급수적으로 증가하고 있으나,
이를 통제할 보안 의사결정은 점점 더 복잡해지고 있습니다



단순한 IT 장애가 아닙니다.
국가 경제 규모에 맞먹는 천문학적 손실이 매년 발생하고 있습니다



왜 지금, CISO가 필요한가

보안 책임은 확대되고 있지만,
이를 전담할 보안 리더십은 여전히 부족합니다

보안 규제 • 컴플라이언스 환경의 구조적 변화



- 인증제도 개선**
- ISMS 인증 기준 강화
 - 정보보호 수준 평가 제도 도입
 - 개인정보 보호 인증 의무화
- 제재 수단 강화**
- 이행강제금* 도입
 - 신고 의무 및 반복적 의무 위반 등에 대한 과징금 증가

보안 책임 주체에 대한 요구 증가



- 기업의
보안 책임 강화**
- 정보보호 전문인력 및 예산확보 의무
 - CISO 지정 기준 상향
 - 기존 임직원 겸직에서 임원급 책임자로 상향
 - CISO 업무 범위 확대
 - 정보보호에 필요한 인력 관리 및 예산 편성
 - 정보보호 현황 및 주요 사항의 이사회 보고
 - 보안 및 정보의 안전한 관리 사항 등을 추가

보안 규제 대응의 실질적 병목은 ‘기술 역량’이 아니라
이를 책임질 CISO 부재입니다

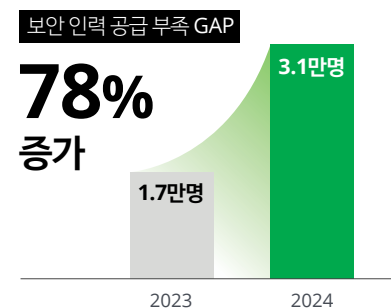
* 시정명령 불이행, 자료제출 불이행 시 이행기간이 지난 이후 부과

CISO 확보의 구조적 • 현실적 한계

보안 리더십은 필수가 되었지만, 모든 기업이 이를 상시 보유하기는 어렵습니다

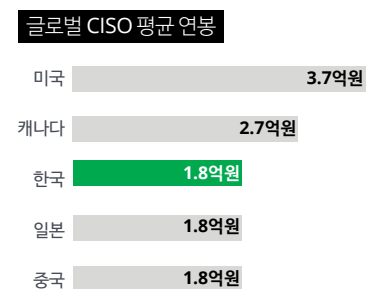
보안 전문 인력 공급 부족 심화

- 국내 보안 인력 수요 대비 공급 약 3.1만명 부족 (전년 대비 78% 증가)
- 적합한 인재 채용 까지 평균 6개월 + α 소요



숙련된 CISO 인력의 높은 채용 • 유지 비용

- 국내 평균 CISO 연봉 1.8억
- 미국 평균 CISO 연봉 3.7억



중소 • 중견기업의 경우, 풀타임 CISO 확보는 구조적 부담

- 2023년 국내 기업 CISO 임명률 평균 18.1%
- 국내 기업 30%, ‘정보보호 투자 우선순위’ 제외

기업 규모별 CISO 임명 여부

규모 (근로자 수)	임명률 (%)	임명하지 않음 (%)
10~49명	18.4	81.6
50~249명	6.4	93.6
250명 이상	70.6	29.4

단일 역할이 아닌 ‘복합 리더십’으로서의 CISO

오늘날 CISO는 보안 책임자가 아니라,
전략·의사결정·위험·기술을 동시에 책임지는 경영 리더십입니다



이 네 가지 역할은 단일 직무가 아니라, **복합 리더십**에 가까운 요구사항입니다
그러나 모든 기업이 이 수준의 보안 리더십을 **상시 보유하기는 쉽지 않습니다**
기업들은 역할은 유지하면서, 확보 방식은 달리 가져가는 접근을 고민하기 시작했습니다

대안으로서 vCISO의 등장

vCISO는 보안 리더십을 ‘채용’이 아닌 ‘활용’의 방식으로 제공하는 서비스입니다

vCISO
Virtual Chief Information Security Officer

What? 외부의 숙련된 보안 리더가 조직의 정보보호 책임자 역할을 서비스 형태로 수행하는 모델

- 상근 임직원이 아닌 외부 보안 리더십
- 시간제 • 계약 기반 또는 프로젝트 단위 활용
- 경영진 수준의 보안 전략 수립 및 의사결정 지원
- ‘Fractional CISO’ 또는 ‘CISO-as-a-Service’

Why? CISO의 역할과 책임은 유지하면서 확보 방식만 현실적으로 전환합니다

보안 리더십
즉시 확보

책임은
명확하게

비용과
유연성의 균형

운영은
효율적으로

vCISO 서비스 활용 시 기대 효과

vCISO는 보안 리더십의 수준은 유지하면서,
비용 속도 전문성 전략 측면에서 실질적인 변화를 만듭니다



비용 효율적인 보안 리더십 확보

필요한 수준의 보안 리더십을 필요한 만큼만 활용

- 상근 CISO 채용 대비 고정 인건비 부담 최소화
- 조직 상황에 맞춘 서비스 범위 조정 가능



폭넓은 전문성과 객관적 시각 제공

개인 역량이 아닌, 조직의 전문성을 활용

- 다양한 산업과 환경에서 축적된 실무 기반 경험
- 내부 관성이나 이해관계에서 벗어난 객관적 진단



유연하고 신속한 보안 역량 강화

보안 공백 없는 대응 체계 확보

- 채용 절차 없이 즉시 투입 가능한 보안 리더십
- 규제·감사·사고 등 상황 변화에 따른 탄력적 대응



전략 중심의 정보보안 거버넌스 체계 수립

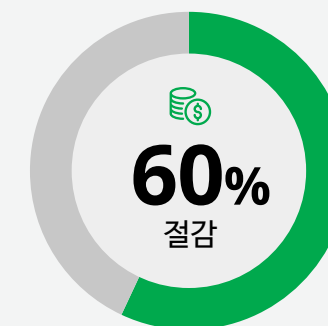
보안을 '운영'이 아닌 '전략'의 영역으로 전환

- 단기 대응이 아닌 중장기 보안 전략·로드맵 수립
- 비즈니스 목표와 연계된 보안 의사결정 체계 정립

vCISO 도입 효과 - 정량적 비교

보안 리더십의 '확보 방식'에 따라
비용·시간·효율은 크게 달라집니다

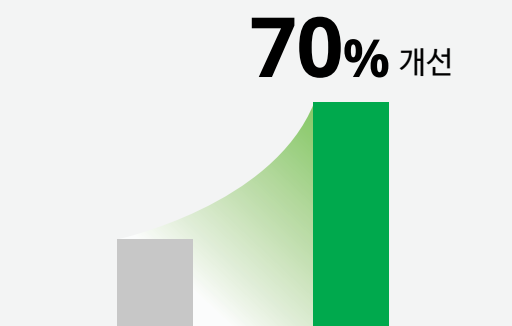
연간 보안 리더십 비용



고정 CISO 채용 시
연 24~35만 달러

vCISO 활용 시
연 10~15만 달러

활용 가능한 보안 전문 영역



고정 CISO 채용 시
1~2개 영역 중심

vCISO 활용 시
3~5개 이상 전문 영역

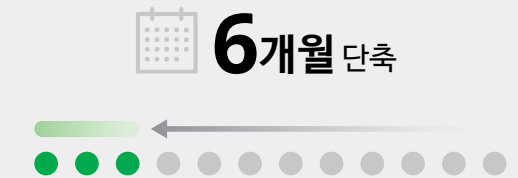
보안 리더십 확보 소요기간



고정 CISO 채용 시
약 3~6개월

vCISO 활용 시
수일~수주 이내

보안 전략·거버넌스 체계 구축 기간



고정 CISO 채용 시
6~12개월 이상

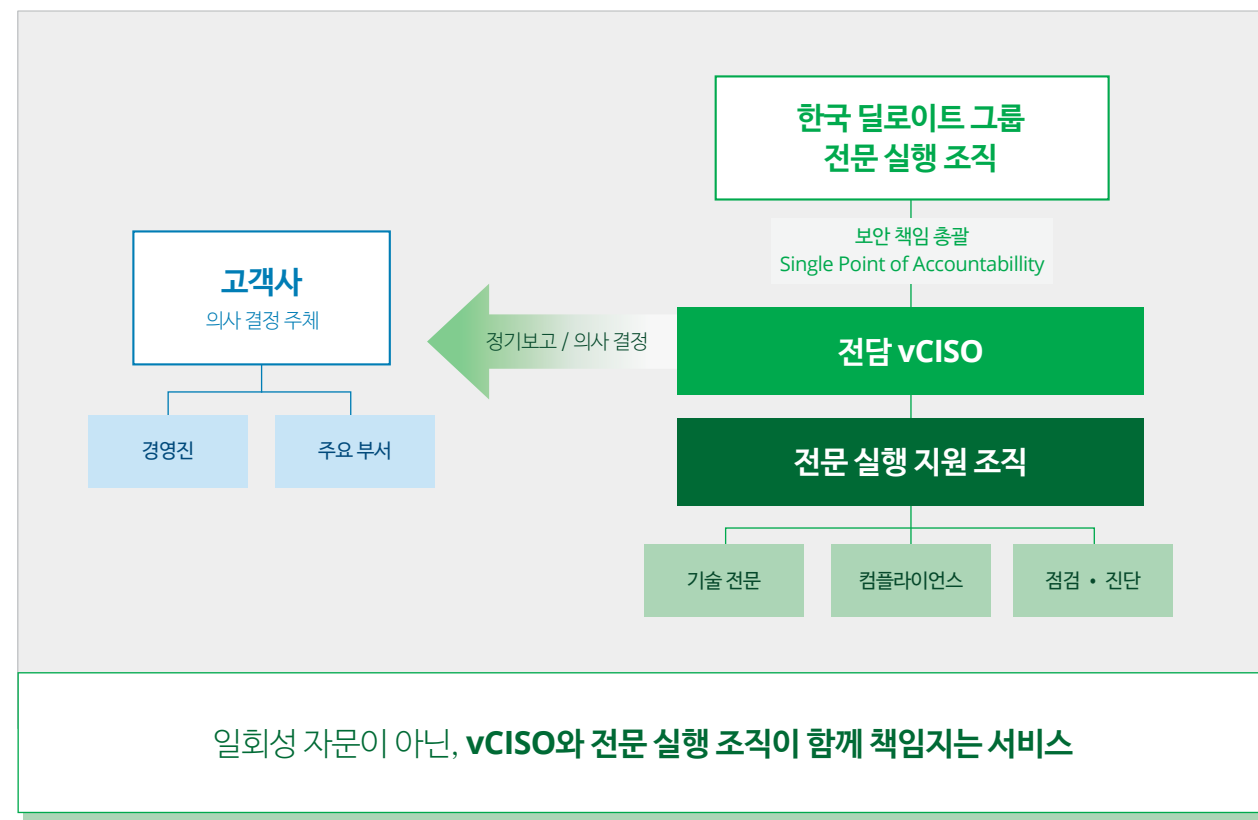
vCISO 활용 시
약 2~3개월 내 초기 체계 구축

vCISO는 보안 리더십의 '수준'은 유지하면서,
비용·시간·운영 효율 측면에서 훨씬 합리적인 선택지입니다

vCISO 수행 조직 구조

단일 책임 체계 하에,
전문 실행 조직이 유기적으로 지원하는 수행 구조

vCISO 조직 구성



조직별 역할 요약

고객사 경영진 Decision Maker 보안 정책 및 주요 의사결정 승인 | vCISO 보고 기반의 전략적 판단

한국 딜로이트 그룹 전문 실행 조직 Single Point of Accountability	전담 vCISO (Service PM)	전사 보안 전략 및 우선순위 결정 보안 거버넌스·이행 현황 총괄 경영진 단일 보고 및 책임 청구
	기술 전문 조직	보안 기술 과제 실행 지원 취약점·위협 대응 및 기술 통제 이행
	컴플라이언스 조직	법·규제·인증 대응 지원 ISMS 및 대외 기관 대응
	점검 · 진단 조직	정기·수시 점검 수행 보안 리스크 및 성숙도 평가

딜로이트 vCISO 서비스

전략 수립부터 실행·모니터링까지,
보안 리더십을 End-to-End로 제공합니다

vCISO 서비스 프레임워크

딜로이트 안진회계법인 보안 관리 Lifecycle

01

전략
Strategy

보안 중장기
전략 · 로드맵 수립

- 현 보안 수준 진단
- 중장기 목표 및 실행 과제 정의

02

거버넌스
Governance

정책 · 조직 ·
의사결정 체계 정립

- 정책·규정 수립 및 정비
- 경영진 보고 및 의사결정 체계 구축

03

운영 · 이행
Operation

보안 과제 실행 및
운영 관리

- 보안 과제 관리(PMO)
- 기술·관리적 통제 이행 지원

04

모니터링 · 개선
Monitoring

지속적 점검 및 개선

- 정기 점검 및 리스크 재평가
- 개선 과제 도출 및 반영

vCISO

Control Hub

보안 관리 Lifecycle 전 단계를 관통하는 통제 및 조정의 중심

실행 영역

Execution Layer

Lifecycle 각 단계에서 필요한 실행이 이루어지는 기능 영역



딜로이트 vCISO 서비스

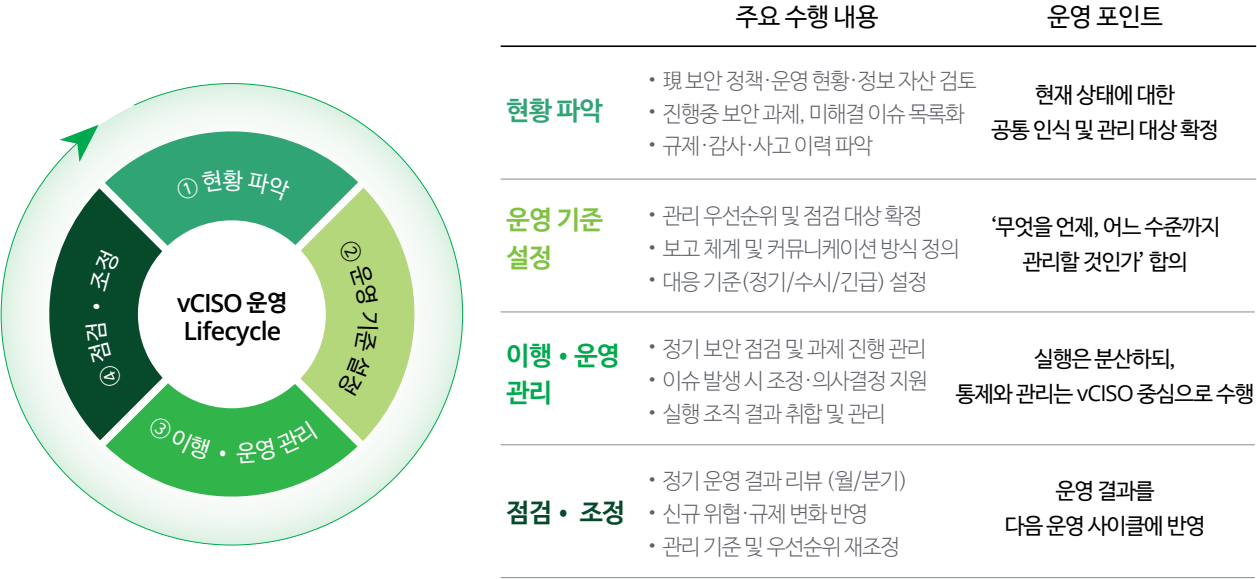
딜로이트 안진회계법인은 vCISO는
보안 관리 전반에 걸쳐 핵심 의사결정과 관리 책임을 포괄합니다

제공 범위

5대 서비스 제공 영역				
				
보안 리더십 및 전략 자문	거버넌스 · 정책 체계 정비	보안 리스크 관리	규제 · 인증 · 대외 대응 지원	침해사고 대응 및 체계 고도화
제공 영역 정의				
조직의 '보안 의사결정 기준'을 제공하는 역할	보안이 일관되게 작동하도록 만드는 관리 기준	모든 리스크가 아닌 중요한 리스크에 집중	규제 대응을 '일회성'이 아닌 '관리 영역'으로 전환	기술 대응이 아닌 '책임 있는 대응'을 보장
세부 제공 범위				
경영진 관점의 보안 의사결정 지원	보안 정책 · 규정 체계 정비	주요 자산 · 위협 · 취약점 식별	ISMS 등 인증 대응 총괄	침해사고 대응 체계 및 절차 수립
보안 투자 우선순위 및 방향성 제시	조직 내 보안 의사결정 구조 설계	리스크 기반 관리 기준 수립 및 우선순위 설정	감독 · 감사 · 대외 기관 대응 지원	사고 발생 시 의사결정 및 대응 방향 총괄

수행 방식

vCISO 통제 하에, 정기 운영·이슈 대응·점검이 반복되는 표준 운영 흐름으로 서비스가 수행됩니다



Why Deloitte?

딜로이트 안진회계법인은 글로벌 경험과 전문성을 바탕으로
귀사의 정보보호 수준을 체계적으로 고도화 합니다

**Global No.1 Cyber Service 전문성**

Security 부분 No.1 전문성 보유
다양한 Global 표준 Framework 활용

**Global 협업 체계 구성**

Deloitte Korea, Vietnam 등
다양한 국가의 전문가와 협업 체계 보유

**전문가 Pool을 상황에 맞게 유동적 활용**

80명 규모의 Compliance, 정책, 모의해킹,
AI, ZTA 등 전문가 보유

**전사적 위험관리 관점의 업무 수행**

정보보호 뿐만 아닌, 전사의 경영목표,
위험관리체계를 고려한 업무 수행
(전사 위험관리 전문가 활용)

**사고 대응 경험을 통한 Know-How 제공**

사고대응, 피해 최소화 경험 다수 보유 (소송, 증거 확보 대응 등)
기밀, 기술 정보 관리 강화를 통한 추가 수익 기반 조성

Contact	백철호 Lead Partner One Cyber & Resilience 02-6676-2250 cbaek@deloitte.com	서영수 Partner One Cyber & Resilience 02-6676-1929 youngseo@deloitte.com	이창성 Partner One Cyber & Resilience 02-6099-4888 changsulee@deloitte.com
---------	---	---	---



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and the unrelated entities, are legally separate and independent entities.