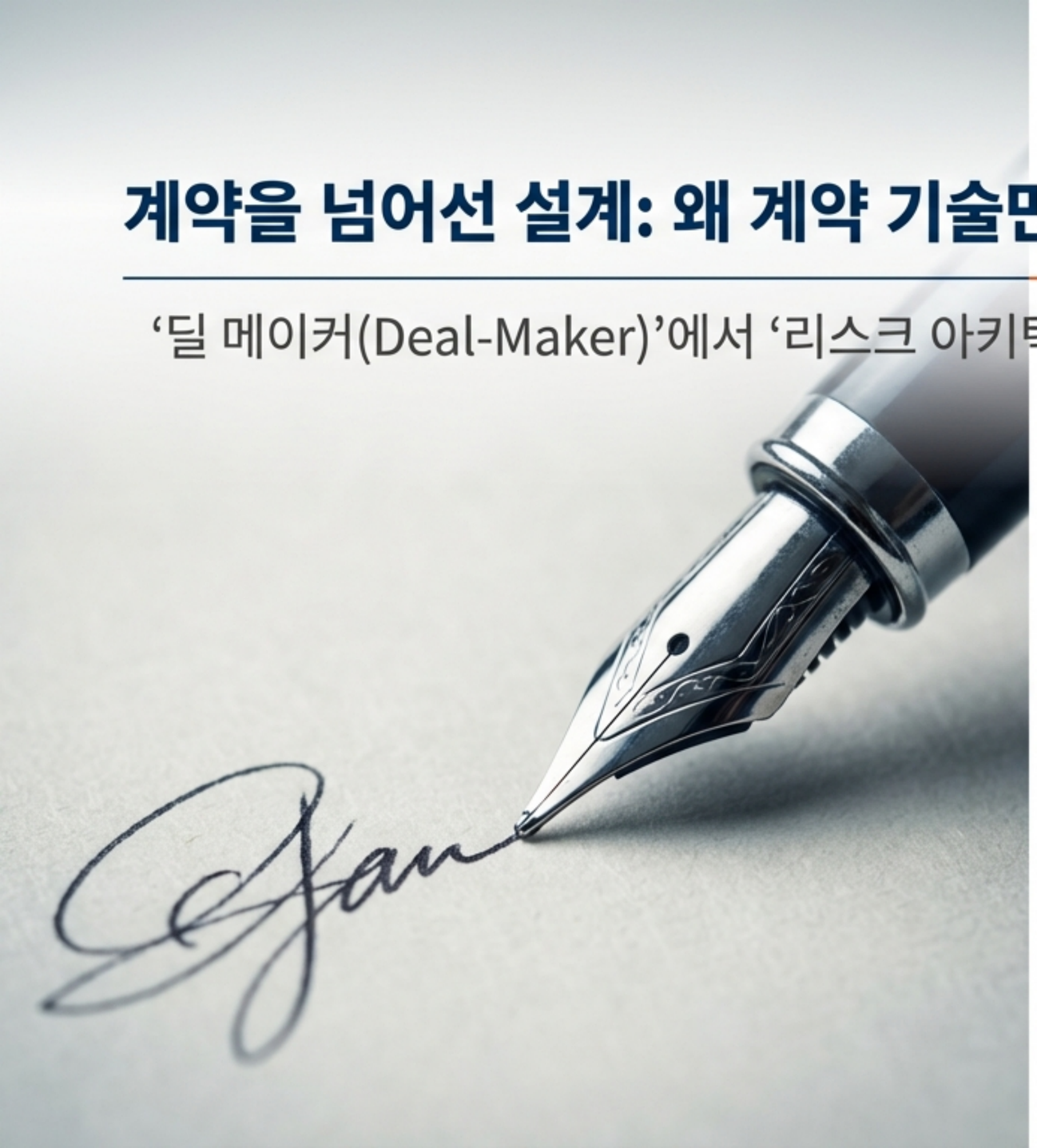
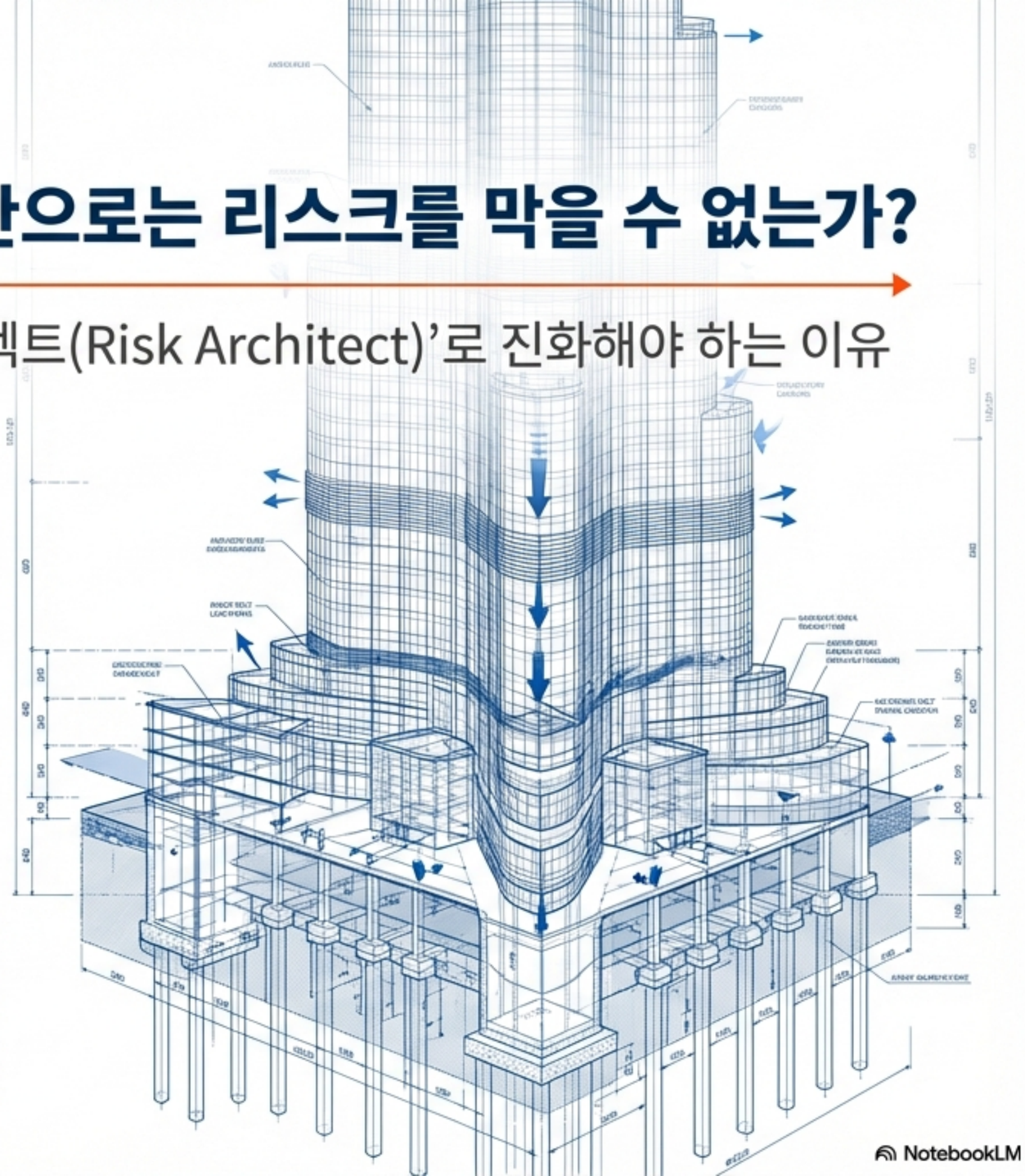
계약을 넘어선 설계: 왜 계약 기술만으로는 리스크를 막을 수 없는가?

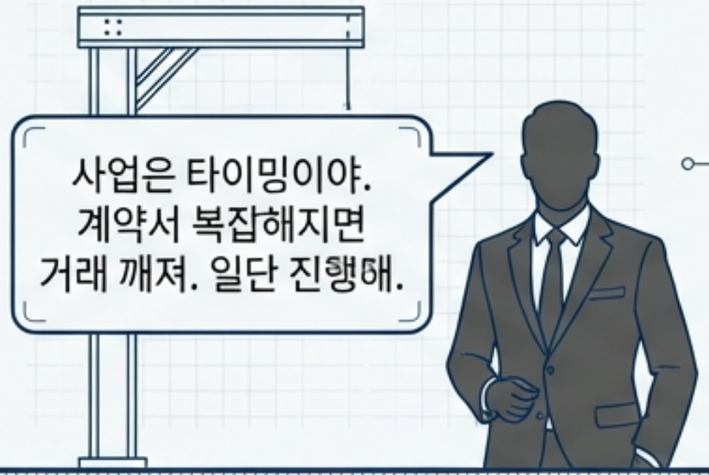
‘딜 메이커(Deal-Maker)’에서 ‘리스크 아키텍트(Risk Architect)’로 진화해야 하는 이유





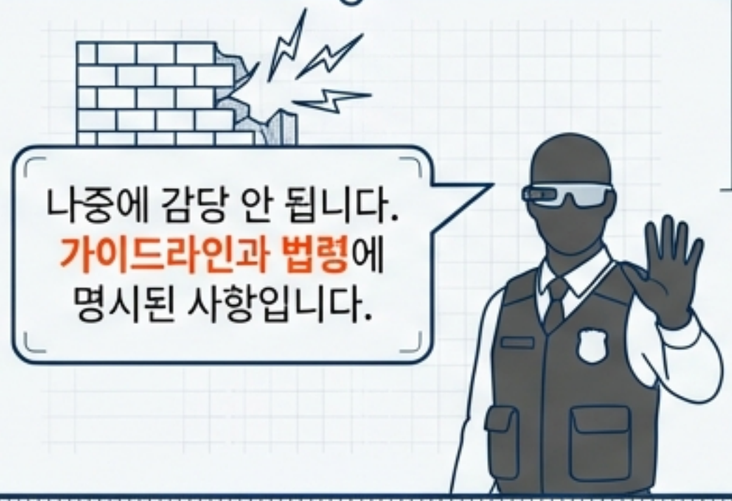
ARCHITECTURAL AUTHORITY: THE RISK BOOMERANG

계약 시점 (The Deal)



속도 중심의 결정
(Speed-Driven Decision)

경고 (The Warning)



보안 및 컴플라이언스 우려
(Security & Compliance Concerns)

1년 후 (The Boomerang)

강제적인 정책 시행
(Mandatory Policy Implementation)

속도를 위해 뺀 조항이 1년 뒤 지주사의 '지시'로 돌아온다면, 그동안 방치된 리스크는 누구의 책임이었을까요?

착각의 근원: 법적 도구(Tool) vs. 경영 시스템(System)

계약 (Contract)

- 거래 성사
- 법적 도구
- 단기적 (Transaction)
- 조건 합의

정보보호 거버넌스 (Governance)

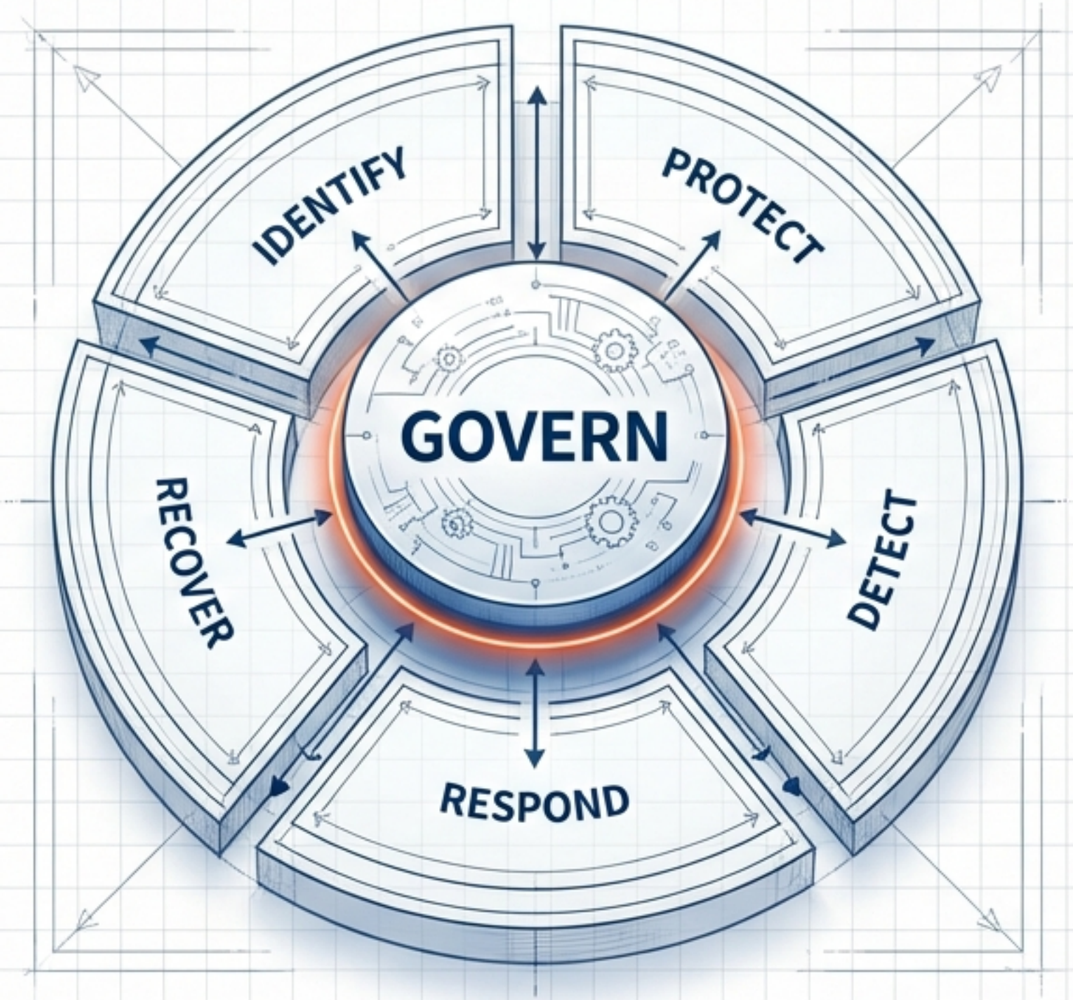
- 리스크 아키텍처
- 정책 (Standard)
- 책임 배치 (RACI)
- 지속적 경영 시스템

계약은 거버넌스의 '하위 구현물'일 뿐입니다.
거버넌스가 없으면 계약은 딜을 위한
타협으로 흔들립니다.

핵심 속성 비교: 딜(Deal)과 아키텍처(Architecture)의 차이

구분	계약 (Contract)	거버넌스 (Governance)
1차 목적	딜 성사, 분쟁 예방	리스크 허용치 및 통제의 지속 운영
시간축	체결~종료 (프로젝트 단위)	상시 (조직 단위, 계약보다 오래 지속)
결정의 기준	협상력, 시장 관행	법·규제, 상위 표준, 리스크 선호(Risk Appetite)
'실패'의 형태	미체결, 마진 악화	사고 은폐, 규제 위반, 구조적 반복 사고
핵심 질문	이 조항을 상대가 받을까?	이 요구가 우리 리스크 전략과 일치하나? 예외면 누가 책임지나?

글로벌 표준의 시각: NIST CSF 2.0과 'GOVERN'의 위상



NIST CSF 2.0 정의

GOVERN 기능은 사이버 리스크 관리 전략, 정책, 모니터링을 정의하며 이를 전사적 위험관리(ERM)와 연결함.

계약의 위치

계약은 독립된 행위가 아니라, 거버넌스가 정한 표준을 집행하는 수단(Implementation Tool).

GV.OC (Organizational Context)

법·규제·계약상 요구사항을 통합 관리하는 것이 거버넌스의 핵심 역할.

"거버넌스가 표준을 정하고, 계약은 그 표준을 집행합니다."

압력의 실체: 계약으로 피할 수 없는 법적 의무

법령 의무
(Domestic Law)

정보통신망법 제47조의4

소프트웨어사업자의 취약점 보완 프로그램 제작 시 KISA 통지 및 사용자 통지 의무.

SLA나 면책 조항으로 계약을 잘 썼더라도, 법적 통지 의무는 사라지지 않습니다.

공급망 가이드라인
(Supply Chain Guidelines)

SW 공급망 보안 가이드라인 (2024.05)

C-SCRM을 전사 위험관리(ERM)에 통합.

레벨(Level) 구조: 레벨-1(전사 정책) → 레벨-2(프로세스) → 레벨-3(운영).

계약만 있고 거버넌스가 없을 때 발생하는 일 (Case Studies)

SolarWinds (SEC 제소)

- Situation: CISO가 리스크 및 통제 미흡 공시 문제로 제소됨.
- Failure: 계약 문구가 아니라 '내부 통제와 공시의 불일치'가 문제.

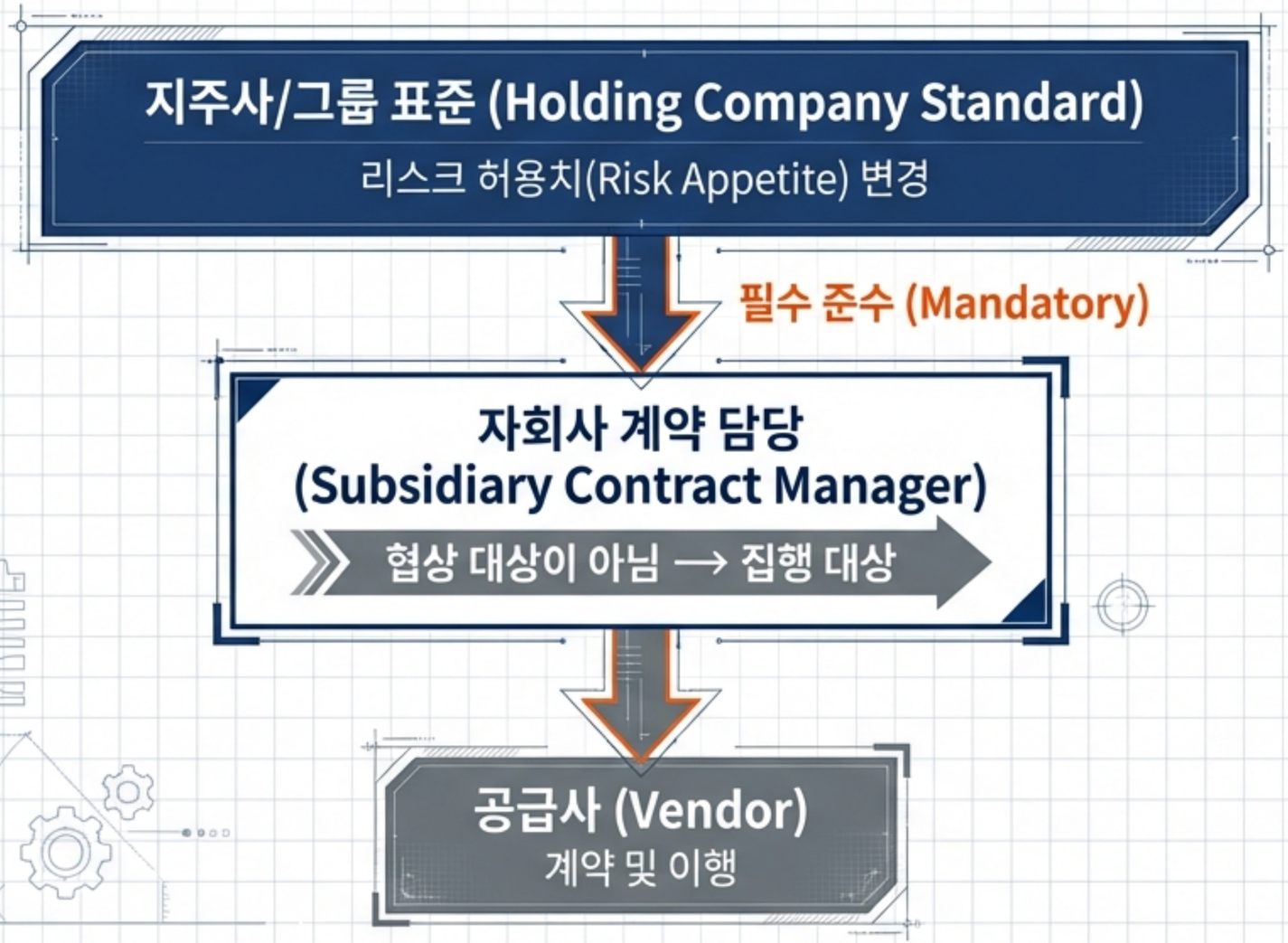
Log4j (10년의 부채)

- Situation: 취약점 제거에 10년이 소요될 것으로 예상 (CSRB 보고서).
- Failure: 자산 가시성(SBOM) 부재로 인해 어디를 고쳐야 할지 모름. 패치 조항만으로는 해결 불가.

Uber (은폐와 유죄)

- Situation: CSO가 침해사고를 은폐하려다 유죄 판결(집행유예).
- Failure: 계약(합의/NDA)으로 사고를 덮으려 했으나, 거버넌스(윤리/보고) 위반으로 개인 형사 책임 발생.

지주사의 개입은 '리스크 신호'다



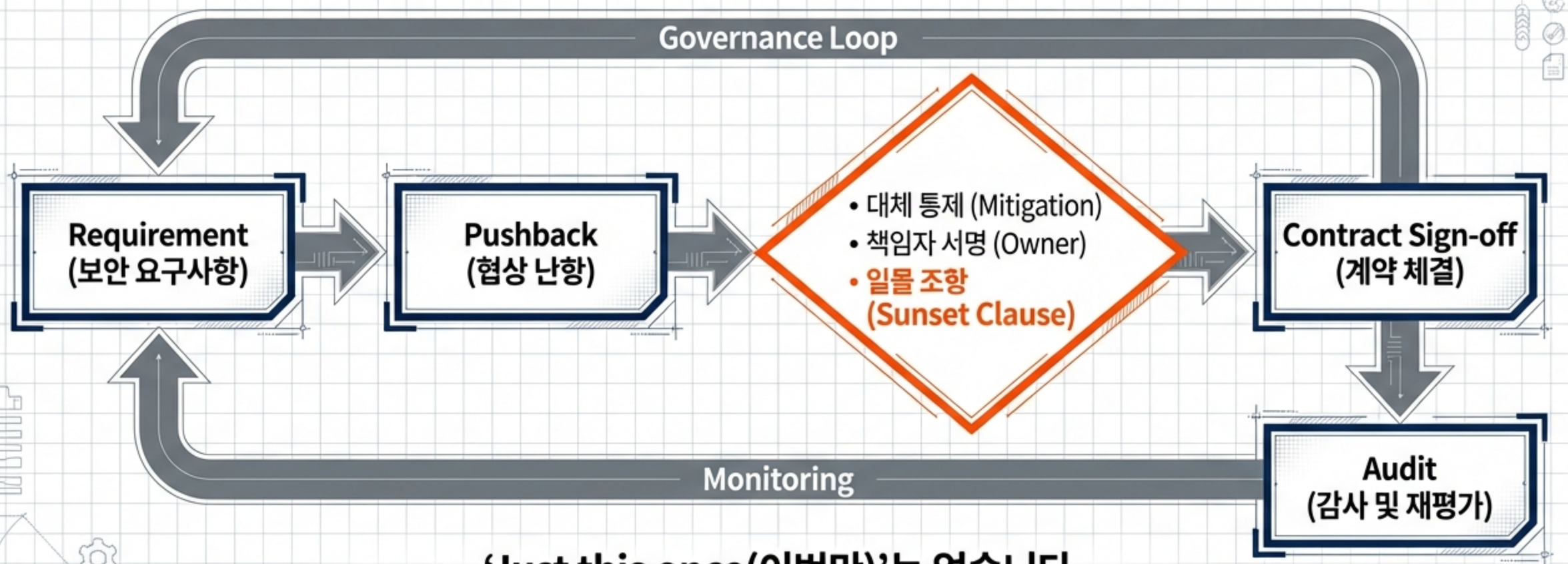
해석 (Interpretation)

- 상황: 보안 담당자가 협상 과정에서 제외했던 조항이, 지주사 감사나 표준 강화 지시로 다시 내려오는 경우.
- 의미: 이는 개인의 협상 역량 부족이 아니라, 조직의 리스크 허용치가 낮아졌다는 신호.
- Action: '협상으로 빼보자'가 아니라 '상위 표준 변경에 따라 필수 적용'으로 대응 논리를 전환.

질문의 전환: 딜(Deal) 관점에서 거버넌스(Governance) 관점으로

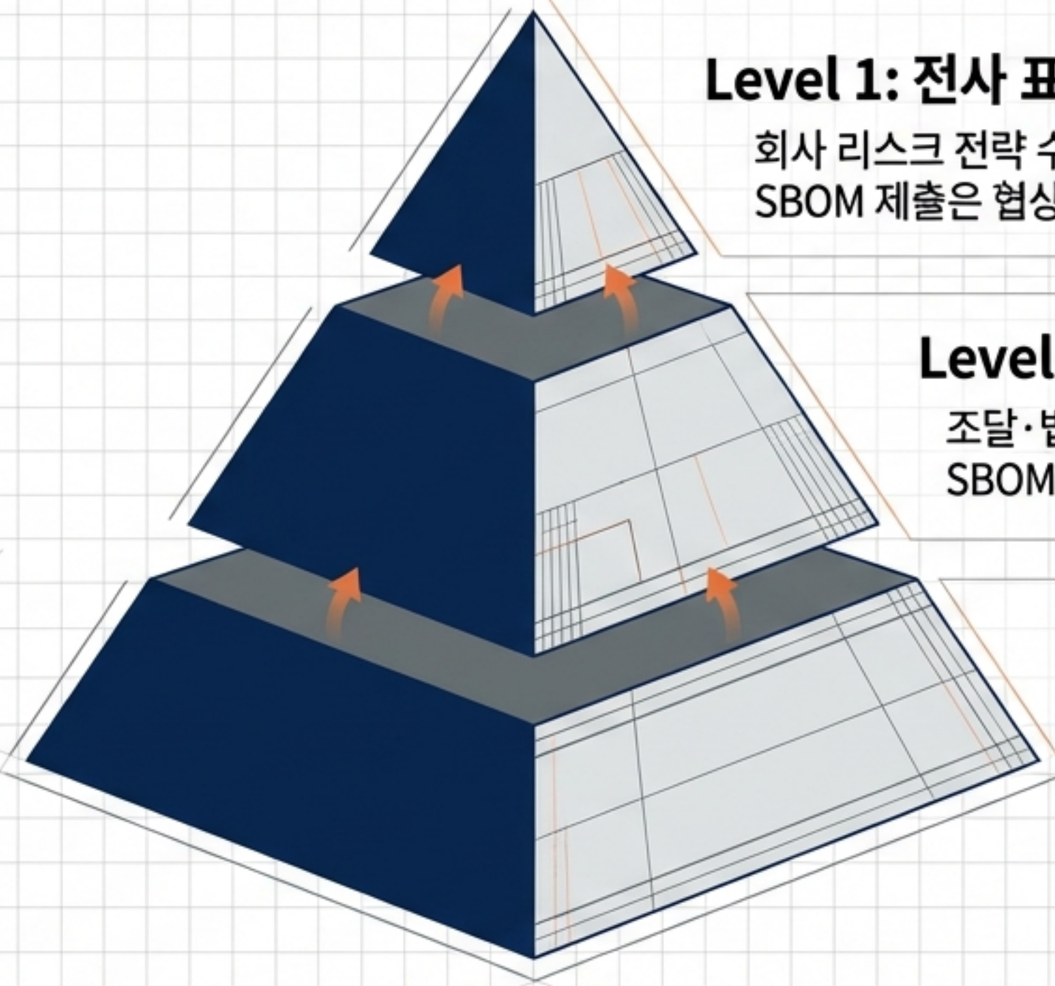
	~~이 조항을 상대방이 받아들일까?~~	이 요구는 상위 표준(지주사/법규)의 필수 조항인가? 협상 대상이 아니라 예외 프로세스 대상인가?
	~~요구를 완화해주면 사업이 좋아하겠지?~~	요구를 완화하면 그 리스크는 누가 책임지는가? (RACI, 경영진 승인)
	~~이번 한 번만 예외로 하자.~~	예외의 유효기간(Sunset Clause)은 언제인가? 재평가는 언제 하는가?

무단 삭제 대신 '공식적 예외(Exception)'를 설계하라



'Just this once(이번만)'는 없습니다.
모든 예외에는 '만료일'과 '책임자'가 명시되어야 합니다.

실행 가이드: SW 공급망 보안의 3단계 적용 (C-SCRM)



Level 1: 전사 표준/거버넌스

회사 리스크 전략 수립.
SBOM 제출은 협상 대상이 아닌 필수 표준임을 명시. (지주사 표준 등)

Level 2: 프로세스/통합

조달·법무·HR 등 이해관계자 참여.
SBOM 표준 포맷(SPDX, CycloneDX) 및 제출 시점 정의.

Level 3: 운영/모니터링

계약 후 실제 이행 점검.
패치 미이행 시 제재, 취약점 모니터링.

리더십 모델: 계약 관리자에서 거버넌스 리더로의 성장

계약 역량 (Contract Skills)

- 가격/납기 최적화
- 법무/구매팀과의 협상
- 일회성 계약 체결 집중

거버넌스 역량 (Governance Skills)

- 리스크 허용치(Appetite) 설정 및 정책 수립
- 이사회/경영진 대상 리스크 커뮤니케이션
- 계약 이후의 집행(증적, 점검) 및 예외 승인 루프 설계

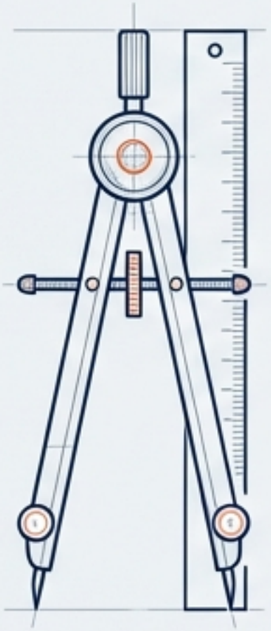
계약을 잘 아는 것은 거버넌스의 '집행 기능' 하나를 마스터한 것에 불과합니다.
진짜 리더는 판(System)을 설계합니다.

Action Plan: 즉시 실행해야 할 3가지 변화

01

Define (정의하라)

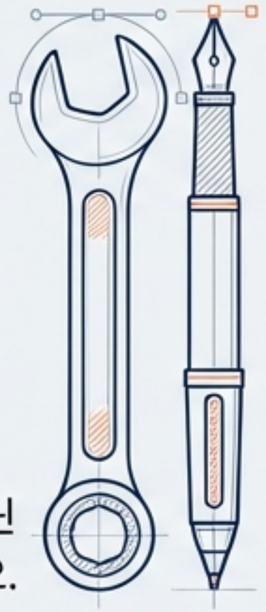
딜이 시작되기 전에 '리스크 허용치'와 '필수 표준(지주사 포함)'을 먼저 확립하십시오.



02

Execute (도구로 써라)

계약을 전략이 아닌 '통제 집행 도구'로 사용하십시오. 필수 조항은 협상이 아닌 예외 절차로 다루십시오.



03

Monitor (감시하라)

계약 서명은 끝이 아닙니다. 예외 사항의 만료일을 추적하고, 공급사의 이행 여부를 주기적으로 감사하십시오.

좋은 계약은 돈을 아끼지만, 좋은 거버넌스는 회사를 지킵니다.

지금 당장의 '속도'를 위해 뺀 조항은 미래의 '부채'가 됩니다.
여러분의 역할은 딜을 성사시키는 것에서 멈추지 않습니다.
리스크를 정의하고, 승인하고, 책임지는 '거버넌스 아키텍트'가 되십시오.

Call to Action: 지금 바로 여러분 조직의 '예외 승인 프로세스'를 점검해 보십시오.