
심사원 사고 알고리즘

심사원이 판정 흐름 4- Step

- 판단은 느낌이 아니라 절차다

판정은 증거 + 리스크 + 요구사항의 교차점이다

판정은 “느낌”이 아니다

Risk-based thinking (RBT)

- 판정은 감정이 아니라 **요구사항 + 증거 + 리스크**의 결과
- “잘했다 / 못했다” ❌
- “충족 여부 + 시스템 영향” ⭕

- 우리는 **사실(Fact)**만 본다
- 그 사실이 **리스크**를 만들면 **평가**한다
- 그리고 표준이 허용하는지로 **판정**한다

Audit judgment is based on Risk-based Thinking

관찰사항(Observation)이란, 요구사항은 '존재'하지만 그 효과성과 일관성이 아직 '검증되지 않은 상태'이다.

관찰사항(Observation)의 정체

관찰사항이란?

- 요구사항은 **일부 충족**
- 운영 흔적과 증거는 **존재**
- 그러나 **효과성·일관성·지속성**에 리스크 존재

관찰사항 키워드

- 일부 확인됨
- 일관성 부족
- 개선 여지

"아직 망가진 건 아니지만,
이대로 두면 망가질 수 있는 상태"

부적합의 본질: '실행 실패'가 아니라 '시스템 실패'다

부적합(NC)의 정체

부적합이란?

- 요구사항은 명확히 존재
- 이행 증거가 **없거나 중단됨**
- 시스템 목적 달성에 **직접적 리스크 발생**

부적합의 본질

- 부적합은 단순한 실수나 누락이 아니다
- 요구사항을 지속적으로 충족하지 못하는 구조적 결함이다
- 즉, 사람의 문제가 아니라 시스템의 고장이다

"이미 시스템이 역할을 못 하고 있는 상태"

"관찰사항은 경고가 아니라 '조기 진단'이다"

관찰사항(Observation)의 본질

🔭✓ 요구사항은 '형식적으로' 충족

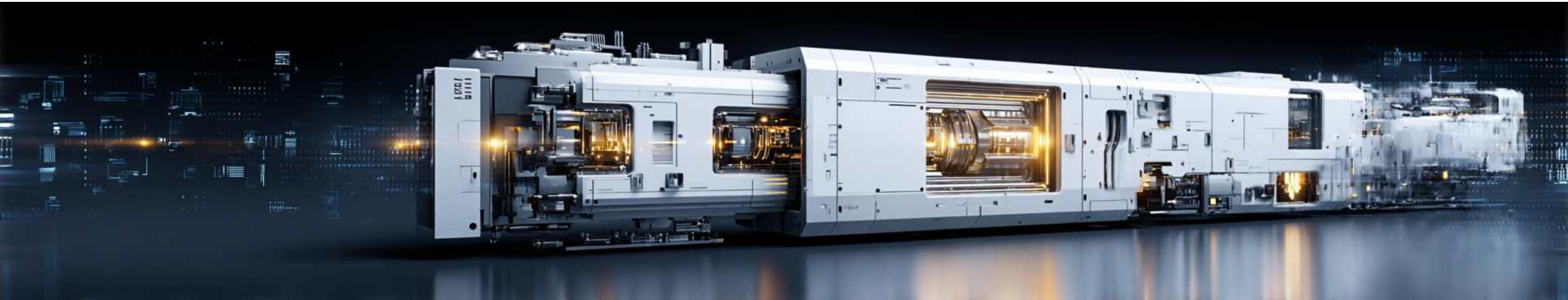
🔭✓ 실행 흔적은 존재

🔭❗ 리스크가 누적·확대될 가능성 확인

🔭❗ 방치 시 부적합(NC)으로 전환 가능

👉 즉, 관찰사항은 '결과'가 아니라 '추세(Trend)'에 대한 판정이다

💭 "관찰사항은 지금 틀렸다는 선언이 아니라,
지금 고치지 않으면 틀리게 될 것이라는 전문가의 경고다."



관찰사항과 부적합의 경계는 '존재 여부'가 아니라 '작동 여부'다

관찰 vs 부적합 경계선

심사원의 사고

- 문서가 있다 ≠ 시스템이 있다
- 활동이 있다 ≠ 관리가 된다
- 결과가 반복되면 '개선 실패' → 부적합

심사원 판단 공식

- 흔적은 있다 → Observation
- 작동하지 않는다 → Nonconformity
- 반복·방치되고 있다 → Nonconformity

관찰사항은 유예, 부적합은 판정

판정은 '느낌'이 아니라, 항상 같은 사고 흐름을 거친 결과다.

심사원의 판정 기준 요약

① 사실 확인

→ 실제로 무엇이 발생했는가? (증거 있음/없음)

② 리스크 존재 여부 판단

→ AI의 신뢰성·책임성·안전성에 영향을 주는가?

③ ISO/IEC 42001 요구사항 연결

→ 해당 리스크를 관리하라고 요구한 조항이 있는가?

④ Observation / NC 결정

→ 관리 흔적 有 → Observation

관리 체계 無 / 반복 / 구조 붕괴 → Nonconformity

부적합은 공격이 아니라, 시스템을 살리는 처방이다

심사원의 언어가 결과를 만든다

❌ “이건 안 돼요 / 틀렸습니다”

⭕ “이 리스크를 관리하는 체계가 확인되지 않습니다”

❌ “규정 위반입니다”

⭕ “ISO/IEC 42001 ○○ 요구사항에 대한 이행 증거가 부족합니다”