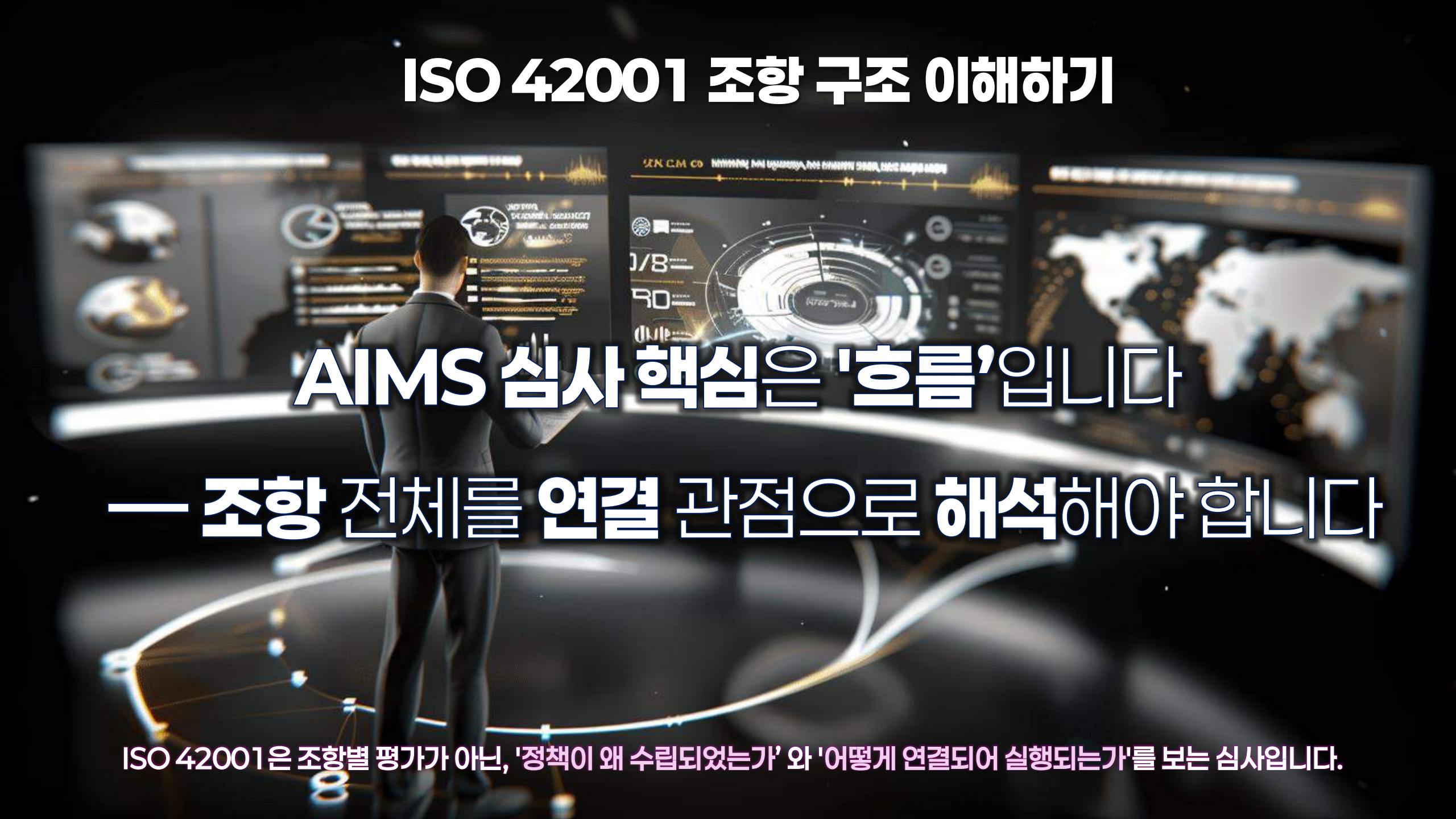
ISO 42001 조항 구조 이해하기



AIMS 심사 핵심은 '흐름'입니다

— 조항 전체를 연결 관점으로 해석해야 합니다

ISO 42001은 조항별 평가가 아닌, '정책이 왜 수립되었는가' 와 '어떻게 연결되어 실행되는가'를 보는 심사입니다.

ISO 42001 조항 구조

기초 조항 (1~3)	실행 흐름 조항 (4~10)
1. 적용 범위 어떤 조직/업무에 적용되는가?	**4. 조직 맥락** 전략은 분석에 근거했는가?
2. 준거 문서 기준 해석의 공식 레퍼런스	**5. 리더십** 정책-자원배분-책임이 연결되는가?
3. 정의 용어 해석의 기준점	**6. 기획** 리스크 기반의 실행 계획 수립 여부
	7. 지원 역량, 커뮤니케이션 등 실행 기반
	8. 운용 리스크 대응과 시스템 운영 절차
	9. 성과 평가 모니터링과 KPI 추적 체계
	10. 개선 결과가 구조 개선으로 이어지는가?

ISO 42001은 '**정책 수립의 근거가 명확해야**' 평가가 가능합니다'

조항 4는 '조직이 왜 이런 시스템을 설계했는가'를 해석하는 시작점이다.

조직의 맥락, 어디서부터 연결되는가?

4 조직

심사원이 던져야 할 핵심 질문들

조항	핵심 질문
4.1 조직 내·외부 **환경 분석**	"외부 변화가 우리의 AI 정책에 영향을 주었는가?"
4.2 이해관계자 **요구사항** 식별	"고객과 규제기관의 요구는 실제 업무에 녹아 있는가?"
4.3 AIMS **적용 범위** 결정	"고위험 AI 시스템의 정의와 적용 범위는 명확한가?"
4.4 운영 **프레임워크** 수립	"각자의 역할과 책임이 실제 운영 속에서 작동하는가?"

문서로는 충분하지 않다.

'왜'를 이해하고 '어떻게' 연결되는지를 물어야 한다

조항 5, 리더십은 오더(order)가 아니라 오너(owner)다

5 리더십

지시가 아닌 책임이 남는 리더십을 ISO는 묻는다.

리더십을 점검하는 두 가지 핵심 질문

조항	핵심 질문
5.1 **최고경영진**의 **리더십**	"**경영진**은 **정책 수립**에 실질적으로 관여했는가?"
5.3 **역할**과 **책임 부여**	"데이터 책임자/AI 감사관 등은 **실무**에서 **작동 중**인가?"

리더십은 선언이 아니라 **구조 설계**다.

조직이 '**누구의 책임인가**'를 명확히 할 때, 시스템은 움직이기 시작한다.

기획은 분석과 실행을 잇는 연결 구조다

심사원이 확인할 기획의 세 가지 실행 포인트

조항	핵심 질문
6.1.2 AI **리스크** 평가	“AI 모델의 편향, 보안 리스크는 사전에 구조화되어 평가되고 있는가?”
6.1.4 **사회적 영향** 평가	“고용, 프라이버시, 차별 이슈 등은 조직의 사전 고려 대상인가?”
6.3 **기획 일관성**	“조직의 AI 정책과 실행 계획이 실제 리스크·영향 분석과 연계돼 있는가?”

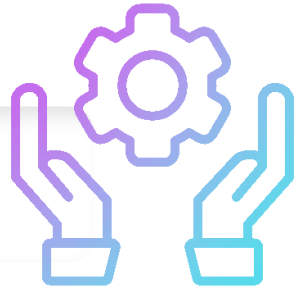
기획은 선언된 목표가 아닌, **연결된 전략**이어야 한다.

조항 7. 자원과 인식, 커뮤니케이션은 전략을 움직이게 하는 실질적 인프라로 작동해야 한다

지원은 보조가 아니라, 작동을 위한 구조다

7 지원

심사원이 확인할 지원의 세 가지 실행 포인트



조항	핵심 질문
7.1 자원 제공	“AI 시스템 운영에 필요한 인력·기술·재정 자원이 실제로 할당되어 있는가?”
7.2 역량과 인식	“AI 윤리, 리스크 대응에 대해 구성원들이 실제로 교육받고 인식하고 있는가?”
7.4 커뮤니케이션	“내부 커뮤니케이션 체계가 AIMS 운영에 맞춰 재설계되어 있는가?”

지원은 ‘도와주는 기능’이 아니라, ‘**돌아가게 만드는 구조**’다.

조항 8. 운영은 매뉴얼이 아니라 반복 가능한 실행 루틴이 작동하는 상태를 의미한다

8 운영

운영은 문서가 아닌, 작동이 지속되는 상태를 말한다.

운영을 점검하는 3가지 실질 기준

조항	핵심 질문
8.1 운영 계획과 통제	“운영 절차가 실제 업무에 따라 반복·통제되고 있는가?”
8.2 운영 실행의 증거	“작동 로그, 이력, 책임자 기록 등 실제 운영 흔적이 있는가?”
8.3 외주/공급망 통제	“위탁된 AI 시스템 운영도 내부 기준과 동일하게 관리되고 있는가?”

운영은 정적 상태가 아니라, **‘지속 가능하게 반복**되는 **역동성’**이다.

평가는 끝이 아니라, 다음을 움직이는 설계 시점이다

심사원이 확인할 평가의 3가지 핵심 포인트

조항	핵심 질문
9.1 모니터링·측정·분석	“운영 결과가 주기적으로 측정되고 분석되고 있는가?”
9.2 내부 심사	“AI 시스템 운영 전반에 대해 독립적 내부 점검이 이루어지는가?”
9.3 경영 검토	“경영진이 실제 데이터를 바탕으로 운영 적합성·성과를 검토하고 있는가?”

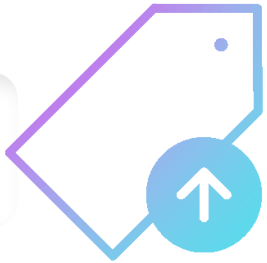
평가는 ‘정리’가 아니라, 다음을 구성하는 구심점이자 **재설계**의 **출발점**이다.

조항 10. 개선은 단순한 수정이 아닌, 반복을 분석해 연결 구조를 재설계하는 과정이다

10 개선

개선은 흐름을 되짚고 구조를 다시 설계하는 연결 기술이다

심사원이 확인할 개선의 3가지 실행 포인트



조항	핵심 질문
10.1 부적합 및 시정조치	“운영 중 발견된 문제에 대해 적절한 원인 분석과 조치가 있었는가?”
10.2 시정조치 프로세스	“반복 방지를 위한 시스템 차원의 개선이 설계되었는가?”
10.3 지속적 개선 노력	“운영 데이터나 심사 결과가 다음 실행에 반영되어 변화로 이어지고 있는가?”

개선은 실수를 드러내고, 연결의 틈을 찾아 **구조를 다시 설계**하는 기술이다.

ISO 42001을 입체로 읽는 5가지 질문 기술

심사원이 되기 위한 5가지 실전 질문력

1 🌐 **조항 간 연결성 추적**

단일 조항이 아닌 **시스템 전체 흐름**을 본다

2 📁 **AIMS 문서 작동성**

단지 '있다'가 아니라 '**돌아간다**'를 증명한다

3 🧠 **ISO 42001 고유항목 숙지**

편향, 설명가능성, 인간 감독 등 특수 요구사항 인식

4 🔍 **내부 감사 설계력**

주기성, 독립성, 반복성 있는 구조인지 확인

5 👔 **경영진 인터뷰 전략**

"정책은 누가, 왜, 무엇을 근거로 만들었나?" 질문

심사원보는 **요건**을 **확인**한다.

심사원은 **흐름**을 **질문**한다.

ISO 42001의 작동 깊이를 꿰뚫는 5가지 보완 질문

심사원이 반드시 던져야 할 질문의 두 번째 레이어

1 시스템 설명 가능성

AI 시스템의 목적과 작동 원리를 조직은 설명할 수 있는가?

2 윤리 원칙의 운영 설계 반영

투명성·책임성·공정성 등 원칙이 구조에 반영되어 있는가?

3 사회적 영향의 실질 반영

고용, 차별, 프라이버시 등 영향 요인이 리스크 분석에 포함됐는가?

4 데이터 거버넌스와 품질 관리

수집, 보안, 출처, 적합성 기준이 마련돼 있는가?

5 정책-실행 간 구조적 연결성

정책, 리스크 분석, 실행이 선형이 아닌 순환 구조로 설계돼 있는가?

질문 하나가 문서를 넘고, 구조 하나를 드러낸다.

핵심 질문은 문서가 아닌 구조를 여는 열쇠다

ISO 42001, 조항이 아니라 작동의 연결을 보는 눈

ISO 42001 심사원 핵심 7조항 요약 카드 (4~10조)

조항	핵심 질문 요지
4 조직	**왜 이 시스템을 만들었는가?** — 설계의 출발점은 '맥락'이다
5 리더십	**누가 책임지는가?** — 리더십은 선언이 아니라 구조다
6 기획	**어떻게 전략은 연결되는가?** — 계획은 문서가 아니라 작동 구조다
7 지원	**무엇이 작동을 가능하게 하는가?** — 자원은 기능이 아닌 인프라다
8 운영	**반복 가능한 실행인가?** — 운영은 문서가 아닌 루틴이다
9 평가	**다음을 위한 점검인가?** — 평가는 구심점을 남기는 기술이다
10 개선	**실수를 다시 설계로 바꾸는가?** — 개선은 구조를 되감는 힘이다

조항은 읽고 넘기는 것이 아니라, **연결**해 **묻는 것**이다.

질문 하나가 작동의 흔적을 드러낸다.

ISO 42001, 질문은 시스템을 작동시키는 리허설이다

놓치기 쉬운 작동 점검 질문 5가지

이 다섯 질문이 작동을 가른다.

연결되지 않으면, 시스템은 움직이지 않는다.

1. AI 시스템은 설명 가능한가?

운영자가 목적·방식·데이터 흐름을 실제로 말할 수 있는가?

2. 윤리 원칙은 정책에 그치지 않는가?

책임·투명성·공정성 등 원칙이 구조에 녹아 있는가?

3. 영향 분석은 실제 기획에 반영됐는가?

사회적 영향(차별, 고용 등)이 전략 수립에 반영됐는가?

4. 데이터 기준은 사전에 정해져 있는가?

출처·적합성·보안 등의 판단 기준이 명확한가?

5. 정책-실행-평가-개선이 연결되어 있는가?

AIMS가 단절 없이 순환 작동하는 구조인가?

작동을 위한 구조는 책임의 연결로부터 시작된다.

ISO 42001은 조항이 아닌 흐름이다

04. 조직: 시스템의 이유를 묻다 (맥락)

05. 리더십: 누가 책임지는가 (구조의 시작점)

06. 기획: 전략이 연결되려면 어떻게 설계해야 하는가

07. 지원: 작동 가능한 인프라 확보

08. 운영: 반복 가능한 실행 루틴

09. 평가: 작동 흔적을 남기는 구조

10. 개선: 구조를 되감고 다시 설계하다

ISO 42001은 조항을 확인하는 기준이 아니라,
조직의 연결된 작동 구조를 해석하는 도구입니다.

AI 전략/기술/윤리 프레임워크, 조직 유형별 적용은 어떻게 달라져야 할까?

조직의 규모와 책임이 전략을 바꾼다

조직

시스템의 목적을 밝히는 **맥락**

리더십

구조의 시작점,

책임의 연결선을 그린다

[조직 유형별 적용 방식 예시]

글로벌 대기업

- 부서 간 책임 충돌 → **AI 윤리 오너십 (owner-ship) 명확화**
- 전략은 복수 부서 협업형, 조정 메커니즘 필요

스타트업 조직

- 민원 발생 후 윤리 반영 시도 → 구조 미비
- 전략은 실행 중심이나, **윤리 검토는 사후적 흐름**

공공 기관

- 시민단체 민원 대응 → **개인정보 보호 우선**
- 구조는 명확하나 유연성 부족 가능성 존재

문서보다 흐름 — 실행의 흔적을 확인하라

AIMS 심사를 위한 핵심 흐름 5단계 점검

AI 전략·기술·윤리 프레임워크는 조직의 책임 구조에 따라 달라져야 한다

조직 역량 따라 달라지는 실행 설계 흐름

目 구조 제안: 수직 흐름형 + 조직 유형별 예시 (스타트업 / 대기업 / 공공)

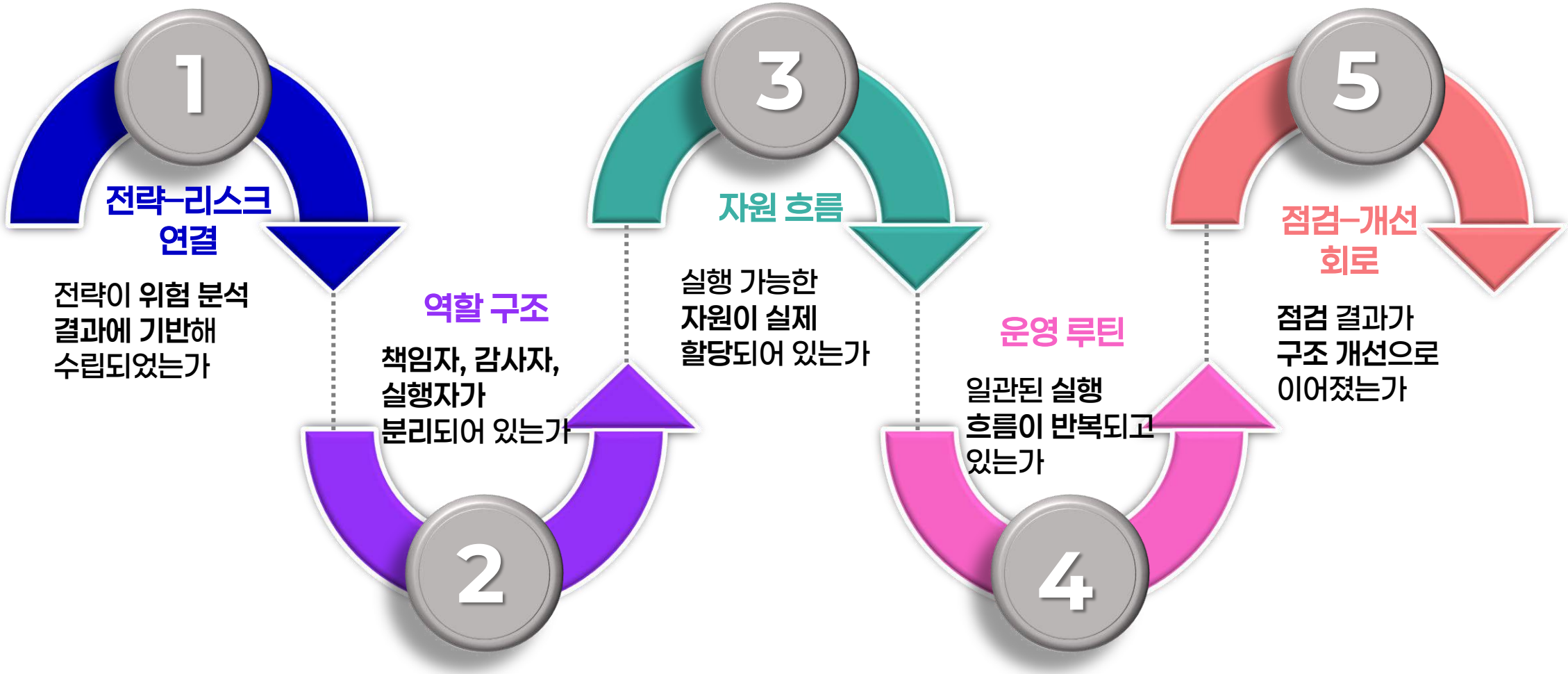
단계	핵심 체크포인트	스타트업 조직	글로벌 대기업	공공 조직
기획	전략-리스크 연결 설계	단기 목표 중심 전략	리스크 기반 정합 구조	사회적 영향 기반 전략 수립
지원	자원·역량 확보 체계	핵심 인력에 집중	다부서 자원 통합 필요	예산 및 교육 제도 중심
운영	반복 가능한 실행 구조	초기 MVP 반복	표준화 프로세스 중시	규제 준수 기반 절차화
평가	작동 점검 및 내부 감사	데이터 수집 미비	정기적 점검 프로세스 있음	독립성 확보 어려움 존재
개선	구조적 보완 및 순환 설계	실행 경험 중심의 개선	포트폴리오 관점 개선 체계	법/정책 연계 중심 개선

ISO 42001은 모든 조직에 동일한 방식으로 적용되지 않는다.

전략은 문서가 아니라 실행 구조에서 증명되어야 한다.

5단계 흐름으로 검증하는 AIMS 작동성 :설계가 아닌 흐름, 연결성과 반복성을 입증하라

ISO 42001, 작동성을 증명하는 흐름 기반 설계



설계는 선언이 아니라 흐름이다.

AIMS는 **흐름의 작동성**으로 평가받는다.

문서는 단서일 뿐, 흐름을 드러내는 질문이 시스템을 움직인다

ISO 42001, 작동성을 파악하는 다섯 개의 핵심 질문

전략-리스크 연결 확인

01

"이 전략은 어떤 리스크 분석에서 출발했습니까?"

"누가, 어떤 기준으로 책임을 나눴습니까?"

02

구조·책임·역할 분리 확인

선언된 자원이 실제 투입됐는가

"이 자원은 실제로 작동 중입니까?"

03

""평가 결과는 구조를 어떻게 바꿨습니까?"

04

루틴화·표준화 여부 점검

"사람이 바뀌어도 운영은 반복 가능합니까?"

점검→개선의 순환성 확인

05

문서 존재 여부보다 흐름 작동 증명이 핵심이다.

AIMS는 흐름의 작동을 문서로 입증해야 한다

질문 영역	작동 입증 수단 예시
🧠 전략–리스크 연결	위험 평가서, 전략 수립 기록
🚧 구조·역할 분리	책임 분장표, 의사결정 체계도
⚙️ 자원 작동 여부	예산 배정표, 시스템 운영 로그
🔁 반복 가능 운영	표준운영절차(SOP), 훈련 기록
🔍 점검 → 개선	내부 감사 보고서, 개선 조치 기록

ISO 42001은 '있다'는 문서를 찾지 않는다.

'흐름이 실제로 작동했는가'를 물으며,

그 **입증**은 문서가 아닌 '**흔적**'과 '**연결성**'으로 판단된다.

작동 흐름을 입증해야 한다 — 문서 존재는 출발점일 뿐

문서는 증거가 아니다

"서류 ≠ 작동"

01 문서만 존재

❌ 형식만 존재

-삭제 정책만 문서화

-절차에 명시만 되어 있음

-교육 계획만 등록됨

■ 흐름 없음,
실행된 흔적 없음

02 일부 흔적

⚠️ 수동적 흐름

- 담당자·시간 명시는 되어 있음
- 일정/계획 일부 로그 존재
- 실행 여부는 불분명

● 흐름이 끊기고,
일부 증적(證跡)만 존재

03 객관적 증거

✅ 작동 확인 가능

- 실제 수행 로그 + 인터뷰 일치
- 담당자가 설명 가능
- 수행 결과 + 피드백 기록 존재

● 흐름과 연결성까지 입증됨

ISO는 '**실행 여부**'를 묻는다.
문서보다 흐름과 피드백이 입증의 기준이다

실행이 작동하게 만드는 연결 설계의 5가지 조건

흔적을 남기려면, 흐름을 설계해야 한다

01

전략은 리스크 분석 기반으로 수립되었는가?

02

책임자·감사자·실행자 역할이 구분되어 있는가?

03

자원이 선언만이 아닌 실제 작동 중인가?

04

실행이 반복 가능한 루틴으로 구성되어 있는가?

05

결과가 구조 개선으로 이어지는 순환이 존재하는가?

흐름이 없으면 흔적도 없다.

연결되지 않은 선언은 '입증'이 아니라 '의심'의 시작이다.

연결되지 않은 조항은 작동하지 않는다

흐름 없는 설계가 만드는 3가지 오류

X

❌ 작동하지 않는 X 구조

① **전략 따로**

→ 리스크 분석과 무관한 선언

② **구조만 있음**

→ 책임이 연결되지 않음 (이름만 있음)

③ **평가만 있음**

→ 개선으로 이어지지 않고, 순환 구조 없음

O

✅ 작동 흐름을 위한 O 구조

① **전략 ↔ 리스크 연계**

→ 위험 분석 기반의 전략 수립

② **구조 ↔ 책임 연동**

→ 명확한 책임 연결과 실행 체계

③ **평가 → 개선 순환**

→ 평가 결과가 구조 개선으로 이어짐

설계는 **연결**되어야 한다.

고립된 조항은 작동하지 않는다.

ISO 42001 핵심 리마인드 – 선언과 흐름의 차이

흐름 기반 구조, 이렇게 기억하자

📊 “선언 기반 vs 흐름 기반”

구분	❌ 선언 기반 구조	✅ 흐름 기반 구조
전략 설계	단편 선언, 리스크와 무관	🔗 **리스크 분석 기반 연결된 전략**
책임 구조	이름만 존재, 실행 연계 없음	👥 **책임자 ↔ 실행자 간 역할 흐름 존재**
개선 구조	평가 후 단절, 순환 없음	🔄 **피드백 → 구조 개선으로 순환**

📌 AIMS는 ‘흔적’과 ‘연결성’으로 움직인다.

📄 문서는 ‘있다’고 말할 뿐,

흐름만이 ‘작동’을 입증한다.

흐름 없는 선언은 증거가 아니다

— 연결된 작동이 기준이다.

ISO 42001 실행 체크리스트 (조항 4~6):실행 흐름을 점검하는 마지막 확인표

조항 번호	조항 요소	세부 조항	세부 조항 요소 (설명)	경영시스템 프로세스	고객관리 프로세스	개발 프로세스	인적자원 프로세스	구매·외주 프로세스	생산 프로세스	품질 프로세스
4	조직의 맥락	4.1	조직 내·외부 환경분석 (기술,규제,시장 등 환경요소 평가)	●	○	●	○	○	○	●
		4.2	이해관계자의 요구사항 식별 (고객·규제기관·직원등 요구 파악)	●	●	○	○	○		●
		4.3	AIMS 적용 범위 결정 (AI시스템 유형·위험도 기반 범위 설정)	●	○	●			●	●
		4.4	운영 프레임워크 수립 (절차·역할 정의등 통합 관리 체계)	●	○	●	●	○	●	●
5	리더십	5.1	최고경영진 책임 강화 (AI 정책 수립, 자원배분, 리더십)	●			●			●
		5.3	역할 · 책임 할당 (데이터 책임자, AI 감사관 등 지정)	●			●			●
6	기획	6.1.2	AI 리스크 평가 방법론 (편향성·보완 등 리스크 평가)	●	●	●			●	●
		6.1.4	사회적 영향 평가 (고용·프라이버시 등 영향 분석)	●	●		●			●

ISO 42001 실행 체크리스트 (조항 7~10)

조항 번호	조항 요소	세부 조항	세부 조항 요소(설명)	경영시스템 프로세스	고객관리 프로세스	개발 프로세스	인적자원 프로세스	구매·외주 프로세스	생산 프로세스	품질 프로세스
7	지원	7.2	역량개발 프로그램 (데이터 과학자등 교육 훈련)			●	●			
		7.4	커뮤니케이션 체계 (고객 내부 소통 구조)	●	●	●	●			
		7.5.3	문서 보관 · 폐기 (감사 추적성, 보관·폐기 절차)	●		●				●
8	운영	8.2	주기적 리스크 재평가 (AI 모델 성능· 편향성 재검증)			●			●	●
		8.4	고위험 시스템 보고 (영향 평가 보고서 제출)	●	●					●
9	성과 평가	9.1	KPI 모니터링 (정확성 · 편향성등 지표 관리)	●	●					●
		9.3.3	검토 결과 문서화 (개선 조치 실행 계획)	●	●					●
10	개선	10.2	시정조치 프로세스 (편향 검출 시 재 훈련등)	●	●					●

“모든 프로세스는 연결된 흐름 안에서 설계되고 평가되어야 한다. 문서의 존재는 시작일 뿐, **흔적과 작동성**이 입증의 기준이다.”

단순 문서 존재보다 '실행된 흔적'을 중심으로 질문하라

흐름 작동의 증거는 무엇인가? — 인터뷰 체크 5문항 핵심 점검표

질문 항목	확인 내용	체크 박스		
		✅	▲	✕
1. 전략 수립은 어디서 출발했는가?	리스크 분석 기반인지 확인			
2. 책임자는 연결되어 있는가?	실행자-감사자-책임자 흐름 확인			
3. 자원은 실제 투입됐는가?	예산·시간·인력 집행 여부 확인			
4. 반복 가능한 실행인가?	일회성 아닌 루틴 구조 여부 확인			
5. 결과는 개선으로 이어졌는가?	피드백 → 구조 수정 흐름 확인			

🧭 **"이 전략은 어떤 리스크 분석에서 출발했는가? "**

→ 선언된 전략이 **실제 어떤 위험 분석 결과에서 출발했는**지 확인해야 합니다.

👫 **"책임자의 역할은 실제로 구분되어 있는가?"**

→ 책임자·감사자·실행자 **각자의 흐름이 실제 존재하는**가를 묻는 것입니다.

🔌 **"선언된 자원이 실제로 작동했는가?"**

→ 서류에 있는 선언이 아니라, **정말 투입되어 작동 중인**지 살펴보아야 합니다.

🔁 **"일회성이 아닌 루틴으로 구성되어 있는가?"**

→ 우연이 아닌, **루틴이 존재하고 있는**가를 확인해야 합니다.

🔄 **"결과는 구조 개선으로 이어졌는가?"**

→ 점검은 끝이 아니라 시작입니다. **순환과 피드백 구조가** 핵심입니다.

문서가 아닌 흐름으로 증명합니다 —AIMS는 흔적과 연결성으로 작동을 증명합니다

흐름 기반 구조, 이렇게 입증합니다

전략 연결 기반 설계

리스크 분석 결과에 기반한
전략 수립
→ 선언이 아닌 분석에서 출발

실행 가능한 흐름 구조

역할·자원·루틴이 연결된 구조
→ 단순 역할 나열 아님, 작동 흐름
존재

점검 → 개선으로 이어지는 순환

점검은 끝이 아니라 구조 개선의 시작
→ 평가 → 수정 → 재작동 순환 구조

ISO 42001, **질문**이 작동을 이끌어내는 가장 실전적인 도구였다.

"**ISO 42001**는 문서를 보는 것이 아니라,
연결된 작동을 묻는 심사다."

"**문서**를 넘기던 손이,
질문을 던지는 시선으로 바뀌었다"

ISO 42001 AIMS 전문가로 성장하고 싶으신가요?

국제AI교육원의 체계적인 AIMS 과정을 통해 그 첫걸음을 시작하세요

[국제AI교육원 AIMS 과정 바로가기

(https://interaiedu.com/product/iso-42001-ai-auditor/)]