

GAON PRACTICE EDITION

GAON

ISO/IEC 42001 AIMS

Statement of Applicability & Internal Audit Checklist Practice

적용성 보고서(SoA)에서 내부심사 체크리스트까지, GAON 과 함께 실무로 연결하는 실습 프롬프트

Evidence Before Conclusion

국제 AI 교육원

Version 1.0

Version Information

본 자료의 관련 요구사항 표기는 ISO/IEC 42001:2023 을 기준으로 합니다.

표준 개정판이 공식 발행되면 해당 반영에 맞춘 개정본으로 업데이트됩니다.



CONTENTS

목차

How to Use This Kit --- 3

What is GAON?--- 4

실습 01 — ISO/IEC 42001 적용성 보고서(SoA) 작성--- 6

실습 02 — ISO/IEC 42001 내부심사 체크리스트 생성--- 8

마무리 노트 --- 14

HOW TO NAVIGATE

실습 01과 실습 02는 이어지는 흐름입니다.

실습 01에서는 적용성 보고서(SoA)에서 확정한 '적용' 통제를

실습 02의 내부심사 체크리스트가 그대로 이어받습니다.

순서대로 진행하는 것을 권장합니다.

GUIDE

How to Use This Kit

이 키트는 우리 조직의 실제 정보를 GAON에게 입력하고, 단계별 질문에 답하며 ISO/IEC 42001 적용성 보고서와 내부심사 체크리스트 초안을 함께 완성해가는 실습용 자료입니다.

각 실습은 다음 네 단계로 진행합니다.

STEP 01 실습 선택

적용성 보고서(SoA) 작성을 먼저 진행한 뒤, 그 결과를 이어받아 내부심사 체크리스트를 생성하는 순서를 권장합니다.

STEP 02 프롬프트 복사

COPY & USE PROMPT 박스의 내용을 그대로 복사해 GAON에 입력합니다. 문구를 임의로 줄이거나 순서를 바꾸지 않습니다.

STEP 03 단계별 질문에 답변

GAON이 순서대로 묻는 질문에 우리 조직의 실제 정보로 답변합니다. 확인되지 않은 내용은 추정하지 말고 '확인 필요'로 남겨둡니다.

STEP 04 결과 검토 및 확정

GAON이 정리한 초안을 그대로 사용하지 않고, 실제 현장 Evidence와 대조하여 담당자·심사원이 최종 검토·확정합니다.

GAON이 생성하는 질문과 초안은 실제 심사 준비를 위한 실습 자료입니다. 적용성 판단과 최종 내부심사 판단은 현장에서 확보한 객관적 Evidence를 바탕으로 담당자와 심사원이 직접 수행해야 합니다.

PRINCIPLE

What is GAON?

GAON은 통제가 존재하는지 묻지 않습니다.

GAON은 그 통제가 책임·권한·Evidence로 실제 연결되어 작동하는지를 묻습니다.

GAON Practice Flow

위험·요구사항

AI 위험, 영향, 이해관계자, 법적·규제적 요구사항을 확인한다



SoA 적용성 판단

Annex A 통제의 적용 여부와 그 근거를 하나씩 검토한다



적용 통제 → 내부심사 질문

적용된 통제가 실제로 어떻게 운영되는지 인터뷰 질문으로 설계한다



Operational Evidence

책임자, 권한, 로그, 기록 등 객관적 운영 증거를 확인한다



통제 효과성

통제가 실패했거나 예외가 발생했을 때도 작동하는지 확인한다



심사원 판단 → 개선

최종 판단은 심사원이 직접 수행하고, 결과는 개선으로 연결한다

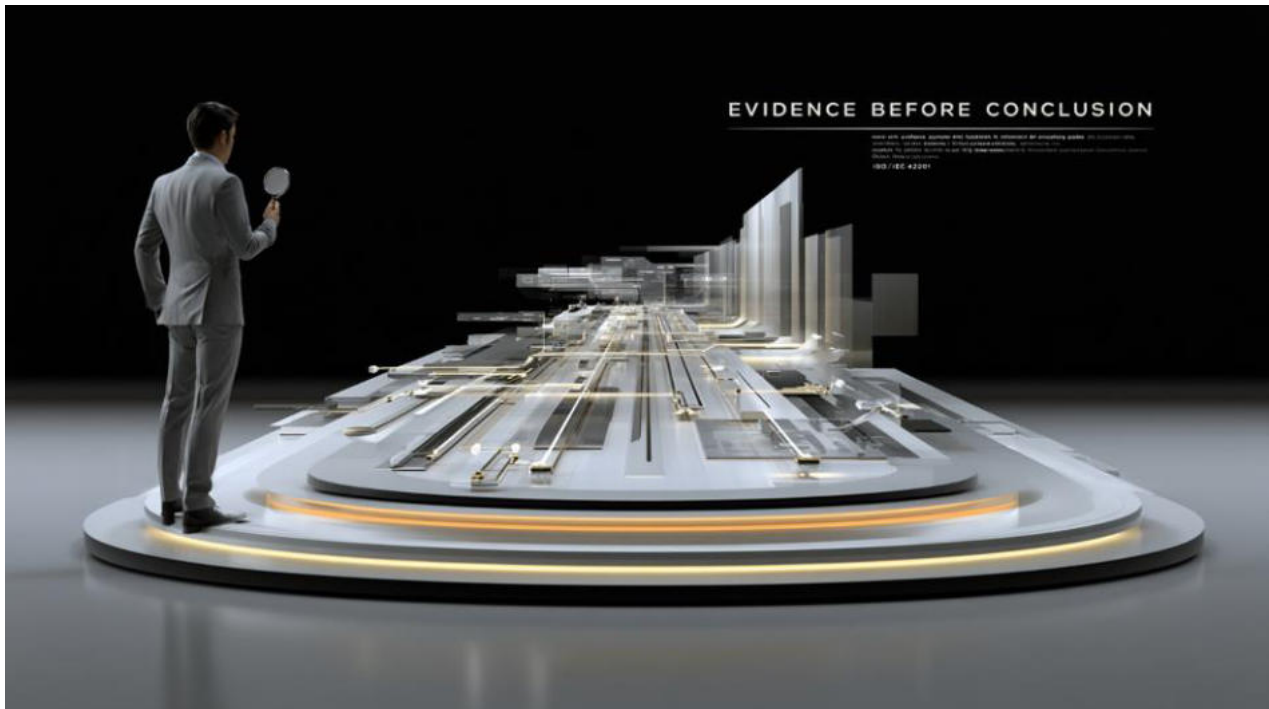
Evidence Before Conclusion

확인되지 않은 정보는 사실로 만들지 않습니다.

Evidence 가 부족하면 판단을 멈춥니다.

요구사항과 통제 목록은 질문의 출발점이지, 결론이 아닙니다.

최종 판단은 심사원과 담당자가 직접 수행합니다.



PRACTICE · 01

실습 01 — ISO/IEC 42001 적용성 보고서(SoA) 작성

적용성 보고서(Statement of Applicability, SoA)는 ISO/IEC 42001 AIMS에서 Annex A 통제의 적용 여부와 그 근거를 정리한 핵심 문서입니다. GAON은 통제를 일괄 적용하지 않고, 우리 조직의 실제 상황을 단계별로 질문하며 SoA 작성을 돕습니다.

STEP 01 역할 확인

GAON은 SoA 작성을 함께 진행하는 조력자 역할을 수행합니다. 임의로 완성하지 않고, 단계별로 질문하도록 안내되어 있습니다.

STEP 02 조직 정보 준비

AIMS 적용범위, 관련 AI 시스템, 역할과 책임, 위험·영향평가 결과, 법적·규제적 요구사항을 미리 정리해두면 진행이 빨라집니다.

STEP 03 프롬프트 복사 후 진행

아래 COPY & USE PROMPT를 그대로 복사해 GAON에 입력하고, 1번부터 순서대로 질문에 답변합니다.

COPY & USE PROMPT · 실습 01

아래 프롬프트를 그대로 복사하여 GAON에 입력하십시오. 임의로 순서를 바꾸거나 항목을 생략하지 마십시오.

우리 조직의 ISO/IEC 42001 적용성 보고서(SoA) 작성을 준비하고 있습니다.

SoA를 임의로 완성하거나 Annex A 통제를 일괄적으로 적용하지 말고,
제가 우리 조직의 실제 상황을 바탕으로 적용 여부를 판단할 수 있도록
단계별로 질문하며 작성 과정을 가이드해 주세요.

다음 순서로 진행해 주세요.

1. 우리 조직의 주요 업무와 AIMS 적용범위를 확인해 주세요.
2. 적용범위에 포함되는 AI 시스템과 AI 활용 목적을 확인해 주세요.
3. 우리 조직이 AI 시스템과 관련하여 수행하는 역할과 책임을 확인해 주세요.
4. 주요 AI 위험, 영향 및 이해관계자를 확인해 주세요.

5. AI 위험평가, AI 영향평가 및 위험처리 결과가 있다면 확인해 주세요.
6. 관련 법적·규제적·계약적 요구사항을 확인해 주세요.
7. 위 정보를 바탕으로 ISO/IEC 42001 Annex A 통제의 적용 필요성을 하나씩 검토해 주세요.
8. 각 통제의 적용 또는 미적용 판단에 필요한 근거를 질문해 주세요.
9. 적용되는 통제는 실제 구현 상태, 책임자, 관련 문서 및 운영 증거를 확인해 주세요.
10. 근거가 부족하거나 확인되지 않은 항목은 임의로 작성하지 말고
'추가 확인 필요'로 표시해 주세요.

특히 정책이나 절차가 존재한다는 이유만으로 통제가 효과적으로 구현되었다고 판단하지 말고,
실제 책임, 실행, 모니터링 및 운영 증거까지 확인해 주세요.

필요한 경우 AI 오류, 환각, 개인정보 문제, 편향, Human Oversight 또는 AI 사고 상황을 가정하여
탐지 → 개입 → 에스컬레이션 → 책임 → 증거 → 개선
과정이 실제로 작동할 수 있는지도 질문해 주세요.

최종 SoA 초안에는 최소한 다음 항목을 포함해 주세요.

- 통제 번호
- 통제명
- 적용 여부
- 적용 또는 미적용 사유
- 관련 AI 위험·영향·요구사항
- 구현 현황
- 책임자
- 관련 문서
- 객관적 운영 증거
- 추가 확인 또는 개선 필요사항

SoA 내용 검토가 완료되면,

Excel에서 활용할 수 있도록 CSV 형식으로 변환할 것인지 저에게 물어봐 주세요.

지금부터 SoA 를 작성하지 말고,

먼저 우리 조직의 AIMS 적용범위를 확인하기 위한 첫 번째 질문부터 하나씩 시작해 주세요.

PRACTICE · 02

실습 02 — ISO/IEC 42001 내부심사 체크리스트 생성

실습 01에서 확정한 SoA의 '적용' 통제 목록을 이어받아, 그 통제가 실제 운영에서도 작동하는지 검증하는 내부심사 체크리스트를 만듭니다. 통제의 존재가 아니라 책임·권한·실행·Evidence의 연결을 확인하는 질문으로 설계합니다.

STEP 01 실습 01 결과 준비

SoA에서 '적용'으로 판단된 Annex A 통제 목록을 손 닿는 곳에 준비해 두면 3번 질문에 바로 답할 수 있습니다.

STEP 02 심사 목적·범위 정하기

정기 내부심사인지, 인증심사 준비인지, 특정 프로세스 추적인지 먼저 정합니다.

STEP 03 프롬프트 복사 후 진행

아래 COPY & USE PROMPT를 그대로 복사해 GAON에 입력하고, 1번부터 순서대로 질문에 답변합니다.

COPY & USE PROMPT · 실습 02

아래 프롬프트를 그대로 복사하여 GAON에 입력하십시오. 임의로 순서를 바꾸거나 항목을 생략하지 마십시오.

우리 조직의 ISO/IEC 42001 내부심사 체크리스트 작성을 준비하고 있습니다.

체크리스트를 임의로 완성하거나 통제의 존재 여부만 확인하는 질문을 생성하지 말고,
제가 우리 조직의 실제 운영 상황을 바탕으로 심사 질문과 확인 범위를 결정할 수 있도록
단계별로 질문하며 작성 과정을 가이드해 주세요.

내부심사의 목적은 문서의 존재를 확인하는 것이 아니라,
책임구조(Accountability), Human Oversight, 운영 통제 및 Operational Evidence가
실제 업무에서 연결되어 작동하는지를 확인하는 것입니다.

다음 순서로 진행해 주세요.

1. 이번 내부심사의 목적과 범위를 확인해 주세요.

예: 정기 내부심사 / 인증심사 준비 / 특정 프로세스 추적 / 이전 부적합 후속 확인

2. 심사 대상 프로세스와 부서, 역할 및 AIMS 적용범위에 포함되는 관련 AI 시스템을 확인해 주세요.

3. 우리 조직의 SoA(적용성 보고서)에서 '적용'으로 판단된 Annex A 통제 목록과 해당 통제가 적용된 이유를 확인해 주세요.

4. 각 통제와 관련하여 다음 사항을 확인해 주세요.

- 통제의 목적
- 관련 AI 위험·영향 또는 요구사항
- 통제 책임자
- 의사결정 또는 승인 권한
- 실제 운영 절차
- 관련 문서
- 최근 운영 Evidence

5. 최근 AI 관련 사건, 이슈, 부적합, 시정조치 또는 변경사항이 있다면 확인해 주세요.

예: AI 오류, 환각, 편향, 개인정보 문제, 성능 문제, Human Oversight 공백, 승인 실패, 모니터링 이상, 외부 AI 서비스 변경 등

6. 확인이 필요한 통제별로 실제 심사 인터뷰에서 사용할 질문을 설계해 주세요.

단순히

'정책이 있습니까?'

'절차가 있습니까?'

라고 묻는 질문보다,

'이 통제가 실제로 어떻게 운영되고 있습니까?'

'누가 이 판단을 수행하고 어떤 권한을 가지고 있습니까?'

'최근 실제 운영 사례를 보여줄 수 있습니까?'

'통제가 작동했다는 것을 어떤 Evidence로 확인할 수 있습니까?'

와 같이 실제 작동 여부를 검증할 수 있는 질문을 우선해 주세요.

7. 각 최초 질문에 대해 예상되는 답변에 따라 이어질 후속(꼬리) 질문을 설계해 주세요.

특히 다음 연결이 끊어지는 지점을 확인할 수 있도록 질문해 주세요.

책임 → 권한 → 실행 → Evidence → 검토 → 개선

8. Accountability, Human Oversight, 사고 대응, 모니터링 또는 통제 효과성과 관련된 항목은 필요한 경우 실제 사건 또는 가상 운영 상황을 이용해 검증 질문을 만들어 주세요.

예:

AI 오류 또는 사고 발생

- 누가 탐지하는가?
- 누가 개입할 권한이 있는가?
- 누가 중단 또는 수정 여부를 판단하는가?
- 어디로 에스컬레이션되는가?
- 누가 최종 책임을 지는가?
- 어떤 Evidence가 남는가?
- 이후 어떻게 개선되는가?

실제 사건이 없었다는 사실만으로 통제가 효과적이라고 판단하지 마세요.

9. 각 질문에 대해 확인해야 할 객관적 Evidence와 적절한 샘플링 대상을 제안해 주세요.

Evidence는 가능한 경우 다음과 같이 구분해 주세요.

- Level A: 로그, 승인 기록, 모니터링 기록, 사고 기록,
Human Oversight 활동 기록 등 직접적인 운영 Evidence
- Level B: 정책, 절차, 역할 정의, 교육자료 등 지원 Evidence
- Level C: 인터뷰 또는 문서화되지 않은 설명

문서가 존재한다는 사실만으로 통제 효과성이 입증되었다고 판단하지 마세요.

10. 생성된 질문을 다시 검토하여 다음을 확인해 주세요.

- 통제의 존재가 아니라 실제 작동 여부를 확인하는가?
- 책임과 권한을 추적할 수 있는가?
- Human Oversight의 실제 개입 가능성을 확인하는가?
- Operational Evidence를 확인할 수 있는가?
- 통제 실패 또는 예외 상황을 추적할 수 있는가?
- 결과가 검토와 개선으로 이어지는지 확인할 수 있는가?

11. 근거가 부족하거나 현재 정보만으로 질문 범위를 확정할 수 없는 항목은

임의로 가정하지 말고 '현장 확인 필요'로 표시해 주세요.

12. 최종 체크리스트는 실제 심사 인터뷰 흐름에 맞게 정렬해 주세요.

운영 상황 확인 → 역할과 책임 확인 → 관련 위험·영향 확인 → 통제 실행 확인
→ Evidence 확인 → 예외·실패 상황 확인 → 검토 및 개선 확인

최종 체크리스트에는 최소한 다음 항목을 포함해 주세요.

- 통제 번호 / 통제명
- 관련 프로세스
- 관련 위험·영향 또는 요구사항
- 통제 책임자
- 심사 질문
- 후속(꼬리) 질문
- 확인할 객관적 Evidence
- Evidence Level
- 샘플링 대상
- 현장 확인 결과

- 심사원 판단
- 비교 / 추가 확인사항

'현장 확인 결과'와 '심사원 판단'은 GAON 이 미리 결정하지 마세요.

GAON 은 질문 설계, Evidence 확인 및 판단에 필요한 정보를 지원하지만,
적합·부적합 등의 최종 내부심사 판단은 실제 현장에서 Evidence 를 확인한
심사원이 수행하도록 해 주세요.

체크리스트 검토가 완료되면,
Excel에서 활용할 수 있도록 CSV 형식으로 변환할 것인지 저에게 물어봐 주세요.

지금부터 체크리스트를 작성하지 말고,
먼저 이번 내부심사의 목적과 범위를 확인하기 위한 첫 번째 질문부터 하나씩 시작해 주세요.

FINAL NOTE

마무리 노트

이 키트는 GAON 과 함께 ISO/IEC 42001 적용성 보고서와 내부심사 체크리스트를 실무 수준으로 연습하며, AI Governance 심사 사고(Audit Thinking)의 흐름을 몸에 익히는 데 목적이 있습니다.

GAON 의 답변과 초안은 실무 준비를 위한 연습 자료일 뿐, 실제 조직의 최종 판단을 대신하지 않습니다.

실제 심사에서는 GAON 의 초안이 아니라, 현장에서 직접 확보한 객관적 Evidence 를 바탕으로 담당자와 심사원이 최종 판단을 수행해야 합니다.

실습 01 과 02 는 한 번으로 끝내지 말고, 조직의 상황이 바뀔 때마다(신규 AI 시스템 도입, 조직 개편, 사고 발생 등) 반복해 갱신하는 것을 권장합니다.

질문이 막혔을 때는 GAON Practice Flow 를 다시 펼쳐보십시오.

GAON Practice Flow

