

국제SI교육원

무료 샘플 · 발췌 · 재구성본

ISO/IEC 27001·27701 교육 교재 미리보기

정보보안 · 개인정보보호

외주 업무 한 건을 따라가며,
기준과 증거를 연결해 판단합니다



외주 지시·재위탁·작업본 사례 한 편
공개 사례 · 가상 심사 · 작성 연습 · 해설

24쪽 무료 PDF
2026년 10월 · 국제SI교육원

이 샘플에 들어 있는 것

한 사례를 끝까지 판단해 봅니다

정보보안과 개인정보보호의 질문을 구분하고, 같은 업무 기록으로 연결하는
미니교재입니다.

부분	학습 내용	쪽
읽기	자료의 성격과 두 표준의 확인 관점	3~4
공개 사례	AdvanceTrack의 외주 정보보호 설명과 확인 한계	5~6
가상 심사	온유 자막제작사 D의 기준·증거·질문·작성	7~13
해설·응용	추가 증거, 발견사항 보고서, 조건 변경, 후속 조치	14~18
직접 작성	보고서·후속 확인·우리 조직 적용 양식	19~21
마무리	학습 정리·출처·이용 안내	22~24

기존 교재를 발췌·재구성했습니다

원본 v0.1 정리본의 공개 R04(185~190쪽)와 가상 A04(200~206쪽)를
발췌해 증거·해설·작성란을 보완했습니다.

읽는 방법과 판단 범위

공개 사실과 가상 판단을 나눠 읽습니다

무료 샘플도 실제로 공부할 수 있도록, 자료의 성격과 판단 가능한 범위를 먼저 밝힙니다.

5~6쪽 · 공개 자료

회사가 공개한 설명을 요약했습니다. 실제 계약, 운영 기록과 인증서 원본을 모두 검증한 자료가 아니며 해당 기업의 부적합을 평가하지 않습니다.

7~21쪽 · 별도의 가상 조직

온유 자막제작사 D, 고객 C, 기준 OUT-07·K-7, 증거·대화·판정 분기는 교육용 설정입니다. 공개 기업의 사건이나 심사 결과를 재현하지 않습니다.

제시한 기준과 확인한 표본 안에서 판단

이 연습은 내부 절차·계약의 충족 여부를 판단합니다. ISO 표준별 부적합으로 연결하려면 적용 판본·요구사항·범위와 증거를 별도로 대조해야 합니다.

정본·법규·계약 검토를 대신하는 자료가 아닙니다. 인증 결과나 법 위반, 중·경 등급을 이 샘플만으로 확정하지 않습니다.

두 표준을 연결하는 방법

같은 작업본에서 서로 다른 질문을 합니다

ISO/IEC 27001:2022와 ISO/IEC 27701:2025를 구분해 살펴봅니다.

관점	이 사례의 질문	대조할 증거
정보보안 27001	누가 어떤 경로로 접근하고, 종료 후 저장·권한을 어떻게 관리하나요?	권한 승인, 전달 로그, 저장 위치, 삭제·접근 제한 결과
개인정보보호 27701	누구의 지시로 무엇을 처리하며, 외부 검수자 변경과 종료 처리는 어떻게 승인하나요?	처리 지시, 역할·계약, 재위탁 승인, 보유 예외·종료 확인
통합 확인	동일 프로젝트의 대상·담당자·시점이 서로 일치하나요?	지시 → 제공 → 작업 → 종료 기록을 같은 건으로 연결

기준은 구분하고 증거는 연결합니다

권한 승인만으로 개인정보의 모든 사용을 허용한 것으로 보지 않습니다. 하나의 기록이 두 관점에 관련되어도 판단 이유는 각각 설명합니다.

공개 사례 / AdvanceTrack

외주 업체의 공개 설명은 확인의 출발점입니다

회계 아웃소싱 기업 E-Accounting Solutions Limited(상호 AdvanceTrack)의 공식 공개 자료를 읽습니다.

공식 보안 FAQ의 설명

회사 FAQ는 직원 교육, 업무에 따른 접근 제한, 물리적 보안과 연례 심사를 설명합니다. 경영진에게도 모든 정보에 접근이 허용되는 것은 아니라고 밝힙니다.

공식 전환 사례의 설명

2023년 공개한 전환 사례는 ISO/IEC 27001:2022 전환을 소개합니다. 공개 발표를 확인한 것이며, 실제 심사보고서나 고객별 운영 기록을 검증한 것은 아닙니다.

교육에서 이어갈 질문

“접근을 제한한다”는 설명을 맡긴 업무 한 건의 승인 대상, 현재 권한, 작업 기록과 종료 처리로 확인할 수 있을까요?

공개 설명에서 확인 질문을 도출하는 교육용 해석입니다. 이어지는 가상 조직 D의 미이행을 AdvanceTrack에 적용하지 않습니다.

인증 판본과 처리 역할을 업무 범위에 맞춰 읽습니다

회사 웹사이트의 표기와 인증서 원본 확인은 구분합니다.

항목	확인한 내용	아직 확인하지 않은 것
인증 표기	공식 개인정보 안내는 27001:2022·27701:2025 인증 보유를 명시합니다.	인증서 원본의 상세 범위·사업장·유효기간
안내 대상	방문자·문의자·지원자 등이 대상입니다. 계약 고객·포털 이용자는 별도 안내로 구분합니다.	회계 외주 고객별 계약과 실제 처리 역할
운영 설명	보안 FAQ의 교육·접근 제한 등 회사 설명을 확인했습니다.	개별 고객 업무의 실행 기록과 종료 처리

컨트롤러라는 표기를 모든 업무에 복사하지 않습니다

웹사이트 안내의 역할과 외주 계약의 역할은 다를 수 있습니다. 실제 업무의 목적·수단
결정과 계약·지시·운영을 함께 확인합니다.

가상 심사 / 온유 자막제작사 D

납품 승인을 받으면 작업본 처리도 끝났을까요?

고객 C가 제공한 임직원 인터뷰 영상 6편의 자막 제작을 맡았습니다. 이름과 음성이 포함되어 있습니다.

심사를 시작하는 장면

프로젝트 납품은 9월 1일 승인됐습니다. 9월 10일 외부 검수자의 임시 저장 목록에 작업본 파일명이 보입니다. 담당자는 “납품 승인을 받았으니 끝났다”고 설명합니다.

이 연습에서 정한 업무 관계

고객 C가 자막 제작 목적과 지시를 정하고 D가 이를 수행합니다. 이 처리 활동의 C는 컨트롤러, D는 프로세서로 설정했습니다. D 자체 인사 처리는 별도 활동입니다.

아직 결론을 내릴 수 없습니다

파일명이 보인다고 실제 내용 잔존을 확정하지 않습니다. 검수자의 소속·승인 관계, 실제 파일 상태와 보유 예외를 먼저 확인해야 합니다.

날짜·조직·역할은 가상 설정입니다. 납품 승인일과 개인정보 처리의 종료 조건을 별도로 확인합니다.

가상 심사 / 기준 OUT-07 · K-7

이 연습의 기준을 먼저 읽습니다

실제 ISO 의무 문구를 옮긴 것이 아닌 가상 조직의 내부 절차·계약 조건입니다.

기준	이 연습에서 요구하는 내용
OUT-07 제공 대상·범위	승인된 검수자에게 자막 검수에 필요한 자료만 제공한다.
계약 K-7 처리 지시	지시된 자막 제작·검수 범위로 처리한다. 홍보 재사용은 지시되지 않았다.
계약 K-7 재위탁 변경	재위탁 대상 변경은 고객의 사전 승인을 받는다. 계정명이 다르다는 사실만으로 변경을 확정하지 않는다.
계약 K-7 작업본 종료	프로젝트 종료 후 7일 안에 작업본을 삭제하고 확인한다. 이 연습은 9월 1일을 종료일, 9월 8일을 기한으로 정한다.
보유 예외 연습 보완 조건	보유 예외가 있으면 대상·근거·기간·승인·접근 제한을 확인한다. 예외 설명만으로 전체 사본 보유를 인정하지 않는다.

원본 A04의 OUT-07·K-7에 처리 범위·기한 계산·예외 확인을 명시했습니다. 7일은 이 가상 계약의 조건이며 모든 조직의 보편적 삭제 기한이 아닙니다.

처음 제시된 증거 / E1~E3

지시·승인 목록·전달 로그를 같은 프로젝트로 묶습니다

원본 A04의 R1~R2를 독학용 E번호로 나누었습니다. 지금은 추가 자료를 확인하기 전입니다.

E1 · 작업 지시서

프로젝트 P-09: 인터뷰 6편의 자막 제작·검수. 이름과 음성이 포함됩니다. 홍보용 재사용은 지시에 없습니다.

E2 · 승인된 검수자 목록

승인 목록에는 V1이 기재돼 있습니다. V2가 같은 업체의 승인 범위에 속하는지, 별도 검수자인지는 아직 확인하지 않았습니다.

E3 · 실제 전달 로그

P-09의 자료 전달 로그에 V1과 V2 계정이 보입니다. V2의 소속은 기재돼 있지 않습니다. 계정명만으로 신원·역할·승인 여부를 확정할 수 없습니다.

확인 사실: V2 계정으로 전달한 로그가 있습니다. 미확인: V2의 소속·역할과 승인 관계. 이 둘을 한 문장에 섞지 않습니다.

처음 제시된 증거 / E4~E6

종료일과 저장 상태는 별도 증거로 확인합니다

원본 A04의 R3~R4를 E번호로 나누었습니다. 목록과 실제 내용, 설명과 실행을 구분합니다.

E4 · 납품 승인 기록

9월 1일 고객이 P-O9의 자막 납품을 승인했습니다. 이 기록은 납품 승인 사실이며 모든 외부 작업본의 삭제 완료를 입증하지는 않습니다.

E5 · 임시 저장 폴더 목록

9월 10일 외부 검수자의 임시 작업 폴더 목록에 관련 파일명이 남아 있습니다. 실제 내용 잔존, 접근 가능 여부와 보유 예외는 미확인입니다.

E6 · 담당자의 최초 설명

“접근이 막혔을 수 있습니다. 검수자 변경 승인과 삭제 확인은 찾아보겠습니다.” 아직 자료를 찾지 못한 상태이며 미실시가 확인된 것은 아닙니다.

최초 자료만으로 미승인 재위탁·삭제 미이행·개인정보 유출을 단정하지 않습니다. 확인 범위를 넓힐 다음 질문을 정합니다.

먼저 작성하기 / 해설은 14쪽부터

판단 전에 모르는 정보를 적습니다

8쪽 기준과 9~10쪽 증거만 사용합니다. 세 선택은 충족·미충족·추가 확인입니다.

확인 항목	잠정 판단·증거 번호	남은 질문
제공 대상·필요 자료 범위		
처리 지시·재사용 범위		
검수자 역할·재위탁 승인		
종료일·실제 작업본 상태		
보유 예외·삭제 결과 확인		

판단 보류도 이유를 씁니다. “자료 없음” 대신 누가 어떤 자료를 아직 제시하지 않았는지 기록합니다.

인터뷰 설계 / 누구에게 무엇을 묻나

답변을 듣고 기록 한 것을 함께 봅니다

인터뷰·문서·실행 기록을 대조합니다. 아래 질문은 최초 자료의 모르는 정보를 확인하기 위한 예시입니다.

대상·질문 의도	사실 확인 질문
작업 책임자 지시와 사용 범위	① 고객 지시를 검수자에게 어떻게 전달했나요? ② 실제 제공한 자료 범위를 보여 주세요. ③ 재사용 요청이 있었다면 승인 기록은 무엇인가요?
외주 관리자 역할과 승인 관계	① V2는 어느 업체의 어떤 담당자인가요? ② 승인 목록과 V2의 관계를 확인할 기록은요? ③ 별도 재위탁이면 고객 사전 승인은 어디 있나요?
저장 관리자 기한과 실제 상태	① 9월 10일 목록은 내용이 남은 파일인가요? ② 삭제·접근 제한 결과는 어떻게 확인하나요? ③ 보유 예외의 대상·기한·승인 기록이 있나요?

실제 개인정보를 임의로 열거나 복원하지 않습니다. 권한을 갖춘 담당자의 승인된 확인 방식과 필요한 최소 증거를 사용합니다.

증거 설계 / 무엇을 대조하나

자료를 세 묶음으로 연결해 확인합니다

서식 수를 늘리는 것이 목적은 아닙니다. 같은 프로젝트의 대상·시점·승인·실행 결과를 맞춥니다.

증거 묶음	함께 볼 자료	대조할 내용
지시·역할·승인	계약 K-7, 작업 지시, 업체·담당자 목록, 고객 승인	지시된 목적과 V2의 역할·승인 범위
전달·접근·작업	제공 항목, 전달 로그, 권한 목록, 검수 기록	승인 범위와 실제 자료 제공·접근·사용
종료·삭제·예외	종료일, 저장 위치, 삭제 결과, 예외 승인	기한 내 처리와 실제 파일 상태·잔여 작업

증거가 서로 다르면 추가 질문을 남깁니다

“삭제했다”는 설명과 보존 목록·실제 상태를 비교합니다.
차이가 있으면 각 기록의 뜻부터 확인합니다.
기록 한 개로 전체 처리 경로를 보증하지 않습니다.

해설 / 원본 A04의 분기 B를 이어서

추가 증거가 들어오면 판단을 바꿉니다

이 페이지부터는 최초 자료에 이어 추가 확인한 가상 증거입니다. 17쪽의 다른 분기와 섞지 않습니다.

추가 확인 ① · V2의 승인 관계

V2는 승인된 검수자로 확인됐습니다. 따라서 최초 로그만으로 미승인 재위탁이라고 판단한 결론은 수정해야 합니다. 재사용의 실제 실행 여부는 이 자료로 확정하지 않습니다.

추가 확인 ② · 실제 작업본과 기한

종료 표본 12건 중 P-09의 실제 다운로드본 1건이 9월 10일에도 남아 있음을 승인된 방식으로 확인했습니다. 해당 건의 보유 예외 승인은 없습니다. 다른 11건은 삭제 확인 기록이 있습니다.

확인 범위 안의 결론

K-7이 정한 9월 8일 기한을 넘긴 실제 작업본이 확인됐습니다. P-09의 삭제 의무 미충족을 기록할 수 있습니다. 실제 유출이나 조직 전체의 미작동은 이 증거만으로 단정하지 않습니다.

해설 / 두 표준의 판단을 구분

같은 사실을 사용해도 판단 이유는 따로 씁니다

내부 계약의 미충족을 확인한 뒤, 적용 표준의 요구사항과 연결할 근거를 각각 검토합니다.

관점	분기 B에서 설명할 내용
정보보안 27001	외부 작업본의 저장 위치와 종료 후 삭제가 계약 기준으로 관리됐는지 봅니다. 접근 차단이 확인되어도 K-7의 삭제 조건 충족을 자동 입증하지 않습니다.
개인정보보호 27701	처리 지시·승인 관계·보유 예외와 종료 의무를 봅니다. V2의 승인은 확인됐지만 P-09의 계약상 삭제 조건은 충족되지 않았습니니다.
통합 보고	K-7의 삭제 미충족 사실을 분명히 적습니니다. 같은 사실을 두 표준의 부적합으로 기계적으로 중복 등록하지 않고, 적용 기준·심사 방식에 맞춰 연결습니니다.

등급보다 기준과 증거를 먼저 적습니니다

등급은 영향·반복·체계의 작동과 인증기관 기준을 추가 확인해 정습니니다. 이 샘플은 중·경 등급을 확정하지 않습니다.

해설 / 발견사항 보고서 예시

기준·객관적 증거·미충족을 세 부분으로 썩니다

14쪽 분기 B의 가상 확인 사실에 근거한 예시입니다. 원본 A04의 판단을 독학용 보고서로 구체화했습니다.

보고서 항목	작성 예시
요구사항·기준	계약 K-7은 종료 후 7일 안에 작업본 삭제·확인을 요구한다. P-09 종료일은 9월 1일, 기한은 9월 8일이다.
객관적 증거	9월 10일 종료 표본 12건을 확인했다. P-09의 외부 검수자 저장 공간에 실제 다운로드본이 남아 있음을 승인된 방식으로 확인했으며 해당 건의 보유 예외 승인은 없었다.
충족되지 않은 내용	P-09의 외부 검수 작업본이 계약상 기한 후에도 남아 있어, K-7에 따른 작업본 삭제 의무가 충족되지 않았다.

현장 보고서에는 실제 문서 판본·식별 정보·확인 방식·대상 범위를 더합니다. 가상 인원·건수·날짜를 실제 증거처럼
재사용하지 않습니다.

조건 변경 연습 / 독립적인 대안

추가 증거가 달라지면 결론도 달라집니다

A·B·C·D는 독립된 대안 상황입니다.

B의 실제 잔존 사실에 A의 삭제 완료 여부를 더하지 않습니다.

분기	추가로 확인한 상황	판단 방향
A	V2 승인과 기한 내 내용 삭제가 확인됨. 파일명만 남는 보존 목록.	삭제 미이행으로 쓰지 않음. 설명 보완 필요 여부 검토
B	승인된 V2. 표본 12건 중 1건의 실제 작업본이 기한 후 잔존, 예외 없음.	해당 건의 K-7 미충족. 범위·등급은 추가 평가
C	고객 3곳의 12건 모두 외부 검수자·저장 위치 목록과 종료 확인 없음. 미승인 업체 전달도 확인됨.	OUT-07·K-7의 관리 결함 범위를 확대 확인
D	승인·최소 제공·종료일·삭제·고객 확인이 연결되고 보유 예외는 승인·격리됨.	확인한 표본에서 충족. 표본 밖으로 확대하지 않음

직접 연습: A에서는 16쪽 보고서의 어떤 증거·결론을 지워야 하나요? C에서는 추가로 누구와 어떤 기록을 확인해야 하나요?

후속 조치 / 분기 B에 적용

삭제 한 건의 처리와 재발 방지를 구분합니다

아래는 교육용 대응 제안입니다. 원인을 먼저 조사하고 실제 완료·효과를 따로 확인합니다.

구분	예시와 확인할 증거
시정 현재 미충족 처리	P-09의 보유 근거·범위를 확인하고 필요한 접근 통제와 작업본 처리를 수행한다. 승인된 확인 방식으로 처리 결과를 남긴다.
원인 조사 아직 가설	납품 승인으로 종료 체크가 끝났는지, 외부 저장 위치가 누락됐는지 조사한다. 절차·배정·알림·담당자 설명을 대조한다.
시정조치 원인에 맞춰 변경	확인한 원인에 맞게 외부 저장 위치·책임자·기한·결과 확인을 종료 절차에 반영한다. 체크리스트 추가만으로 완료를 선언하지 않는다.
효과 확인 이후 실행 검증	변경 후 종료한 프로젝트에서 기한 내 작업본 처리와 예외 관리를 추적한다. 시점·표본·성공 기준을 정하고 재발 여부를 확인한다.

시정 ≠ 시정조치 ≠ 효과 확인. 삭제 결과 한 건만으로 반복 방지 체계의 효과까지 입증하지 않습니다.

작성 양식 ① / 발견사항 보고서

추정 없이 보고서를 다시 씁니다

B를 선택하거나 17쪽의 다른 분기를 하나 선택하세요. 확인하지 못한 정보는 빈칸을 채우는 사실로 쓰지 않습니다.

항목	작성란
선택 분기·확인 범위	
요구사항·기준 문서·판본·요구 내용	
객관적 증거 대상·시점·자료·확인 방식	
충족되지 않은 내용 또는 충족 근거	
아직 모르는 정보 추가 확인 대상	

작성 후 점검: 담당자를 찾았나요? “못 찾음”을 “미 실시”로 바꾸지 않았나요? 표본 밖의 사실을 덧붙이지 않았나요?

작성 양식 ② / 후속 확인 계획

종결에 필요한 결과와 효과를 정합니다

조치 계획, 실제 실행과 이후 효과를 서로 다른 항목으로 적습니다.

항목	작성란
현재 미충족의 시정	
원인 가설·조사 자료	
확인된 원인	
원인에 맞춘 시정조치	
책임자·일정·확인 방식	
효과 확인 시점·표본 성공 기준·증거	

실습 기록에 실제 고객 영상·개인정보를 복사하지 않습니다. 프로젝트 식별번호와 필요한 최소한의 확인 결과를 사용합니다.

작성 양식 ③ / 우리 조직에 적용

외부에 맡긴 업무 한 건을 따라가 봅니다

영상·상담·급여·디자인·클라우드 등 개인정보가 포함된 외부 처리 업무 한 건을 고릅니다.

항목	작성란
업무·맡긴 자료·처리 목적	
우리 조직과 상대의 역할 지시·변경 승인 책임	
27001 질문·증거 전달·접근·저장·종료	
27701 질문·증거 목적·재위탁·보유·삭제	
실제 종료 조건·예외 결과 확인 담당자	
남은 질문·다음 표본	

우리 조직에는 가상 K-7의 7일을 그대로 적용하지 않습니다. 실제 법규·계약·보유 기준과 업무의 처리 역할을 확인합니다.

학습 정리

납품·권한·개인정보 처리는 각자의 완료 조건이 있습니다

같은 프로젝트로 연결하되, 한 단계의 승인으로 다른 단계의 완료를 대신하지 않습니다.

스스로 설명할 수 있나요?

- ① 파일명이 남은 목록과 실제 작업본 잔존은 어떻게 구분하나요?
- ② V2 계정명만으로 미승인 재위탁을 단정할 수 없는 이유는요?
- ③ 접근 차단과 계약상 삭제 의무는 어떤 증거로 나누어 보나요?

보고서에서 무엇을 남기나요?

기준의 요구 내용, 실제 확인한 대상·시점·증거, 그 사이의 미충족 또는 충족 근거를 남깁니다. 미확인 정보와 판단의 한계도 함께 적습니다.

다음 업무에서 한 가지를 바꾼다면

외부 저장 위치까지 포함한 종료 조건을 담당자와 함께 확인해 보세요.
실제 기록 한 건으로 지시·승인·실행·결과를 설명할 수 있는지 살펴봅니다.

출처와 표준 확인

원자료와 판본을 직접 확인합니다

확인일: 2026년 10월 1일. 공개 소개와 실제 인증서·계약·운영의 검증 수준을 구분했습니다.

공개 사례 원자료

[AdvanceTrack 공식 보안 FAQ · 직원 교육·접근 제한](#)

[AdvanceTrack 공식 27001:2022 전환 사례 · 2023년 발표](#)

[AdvanceTrack 개인정보 안내 · 적용 대상·인증 판본 표기](#)

ISO 공식 표준 안내

[ISO/IEC 27001:2022 · 정보보안 경영시스템](#)

[ISO/IEC 27701:2025 · 개인정보보호 경영시스템](#)

기존 인증이 자동으로 새 판본 인증이 되는 것은 아닙니다. 실제 심사에서는 대상의 적용 판본·범위·전환 상태를 확인합니다. 이 샘플의 보고서는 가상 조직 기준을 사용하며 ISO 조항별 대조 완료본으로 제시하지 않습니다.

이용 안내와 다음 학습

증거를 따라 우리 업무를 설명해 보세요

무료 샘플의 질문·판단·작성 흐름을 실제 업무에 맞춰 활용하세요.

발체와 재구성 범위

원본 v0.1 정리본의 R04·A04를 중심으로 구성했습니다. 공개 사실과 가상 심사를 구분하고, 증거·기한·보고서·후속 확인·작성란을 보완했습니다.

공유와 재사용

이 무료 PDF는 원본 그대로 공유할 수 있습니다. 공개 자료의 권리는 각 원출처에 있습니다. 수정·발체본은 원자료와 수정 범위, 가상 사례임을 표시해 주세요.

ISO/IEC 27001·27701 심사원 자격 확대 과정

과정의 교육 내용과 참여 요건을 확인하세요.

27001·27701 공개 실제 사례 모음 보기

© 2026 국제시교육원 · 무료 교재 미리보기 v1.1

표지: AI 생성 교육용 개념 장면 · 실제 심사 현장 사진이 아닙니다.