무료 백서

ISO 27001 취득 백서

누구나 이해할 수 있는 정보보안경영시스템 국제 인증 가이드

Based on ISO/IEC 27001:2022

취득 절차 · 비용 · Annex A 93 개 통제 · ISMS-P 비교

백 지 석

2026

머리말 — 이 백서를 시작하며

'우리 회사도 ISO 27001 을 받아야 하나요?' — 보안 컨설팅 자리에서 가장 자주 듣는 질문입니다. 글로벌 시장에 진출하려는 SaaS 스타트업, 외국계 대기업과 거래를 시작한 IT 회사, 클라우드 기반 서비스를 운영하는 모든 조직이 한 번쯤 고민하는 인증입니다.

그런데 막상 알아보면 ISO 27001 은 만만치 않습니다. 본문 조항 7 개와 Annex A 93 개 통제, 적용성 명세서(SoA), 위험평가, Stage 1·2 심사 같은 낯선 용어가 한꺼번에 쏟아집니다. 게다가 2022 년 10 월에 표준이 개정되면서(114 개 → 93 개 통제), 인터넷에 떠도는 자료들이 오래된 정보와 새 정보가 뒤섞여 있어 더 혼란스럽습니다.

이 백서는 'ISO 27001 을 처음 검토하는 담당자'가 의사결정에 필요한 정보를 한 권으로 얻을 수 있도록 정리했습니다. ISO 27001:2022 최신판을 기준으로, 인증의 의미부터 통제항목, 비용, 절차, 그리고 ISMS-P 와의 관계까지 '쉬운 한국어'로 풀어 썼습니다. 정보보안 비전공자도 끝까지 읽을 수 있도록 용어를 친절하게 풀고, 표와 체크리스트를 충분히 넣었습니다.

이 백서는 무료입니다. 부담 없이 읽고, 경영진 보고와 전사 공유에 활용해 주세요. 내용 중 보완할 점이 있다면 알려 주시면 다음 판에 반영하겠습니다.

저자 백지석

목 차

01. ISO 27001, 무엇을 인증하는가

한 문장 정의

ISO 27001(정확한 명칭 ISO/IEC 27001)은 '정보보안경영시스템(ISMS, Information Security Management System)'의 국제 표준입니다. 회사가 정보의 '기밀성·무결성·가용성(CIA)'을 지키기 위해 체계적인 관리 시스템을 갖추고 있다는 사실을 국제적으로 공인된 인증기관이 검증해 주는 제도라고 이해하면 됩니다.

여기서 핵심은 '체계(System)'입니다. 방화벽 한 대, 백신 프로그램 한 종을 도입했다고 정보보안이 되는 것이 아니라, 정책을 만들고 운영하고 점검하고 개선하는 '경영' 관점의 사이클이 회사에 자리잡고 있어야 한다는 뜻입니다. 즉 ISO 27001 은 IT 부서가 아니라 '회사'가 받는 인증입니다.

정보보안 3 대 요소(CIA)

요소	의 미	예 시
기밀성 (Confidentiality)	허가된 사람만 정보에 접근	암호화, 접근통제, 권한 분리
무결성 (Integrity)	정보가 위·변조 없이 정확하게 유지	전자서명, 해시, 변경관리
가용성 (Availability)	필요할 때 정보를 사용할 수 있음	백업, 이중화, 재해복구

ISO 27001 의 모든 통제항목은 이 세 가지 가치 중 하나 이상을 지키기 위해 설계되어 있습니다. '이 통제는 무엇을 위해 존재하는가?' 라고 물었을 때, 답이 항상 C·I·A 중 하나로 귀결되어야 합니다.

ISO 27001 을 받는 세 가지 이유

1. 글로벌 비즈니스 진입권 — 외국계 대기업·정부 조달·해외 파트너십에서 ISO 27001 은 사실상 '기본 자격'입니다. 인증서 한 장이 RFP 통과의 전제 조건이 되는 경우가 많습니다.

2. 보안 사고 시 면책의 근거 — '적정 수준의 보안 조치'를 입증하는 가장 강력한 증거입니다. 사고 후 손해배상 소송이나 규제기관 조사에서 인증서가 회사에 유리한 정황으로 작용합니다.

3. 조직 보안 수준의 종합 점검 — 93 개 통제를 점검하는 과정에서 그동안 보이지 않던 빈틈이 드러나고, 보안 책임 분담과 절차가 명확해집니다.

ISO 27001 과 '27000 시리즈'

ISO 27001 은 '인증 가능한 표준'이지만, 같은 패밀리에는 27002(통제 가이드), 27017(클라우드), 27018(개인정보), 27701(개인정보 관리체계) 등 30 개가 넘는 보조 표준이 있습니다. 이들은 인증 표준이 아니라 '구현 가이드라인'으로, 27001 을 준비할 때 함께 참고하면 좋습니다.

02. ISO 27001:2022 개정판 — 무엇이 달라졌나

ISO 27001 은 2022 년 10 월에 9 년 만에 개정되었습니다. 본문 조항(4~10 조)에는 큰 변화가 없었지만 Annex A 통제항목이 대폭 손질되었습니다. 인증을 처음 받는 회사는 자동으로 2022 년판으로 받게 되며, 2013 년판으로 인증을 보유한 회사는 '전환심사(Transition Audit)'를 통해 2022 년판으로 이행해야 했습니다(전환 마감 2025 년 10 월 31 일).

Annex A 통제항목 변화

구 분	ISO 27001:2013	ISO 27001:2022
통제 수	114 개	93 개
테마 수	14 개	4 개
테마 구성	정책, 조직, 인사, 자산, 접근통제 등 14 개	조직 / 사람 / 물리적 / 기술적 4 개
속성 분류	없음	5 개 속성 (사이버보안 개념·운영 능력 등)
신규 통제	—	11 개 추가

11 개 신규 통제 — 외워둘 가치가 있는 항목들

2022 년판에서 새로 도입된 11 개 통제는 최근 10 년간의 보안 트렌드를 그대로 반영합니다. 클라우드, 위협 인텔리전스, 데이터 유출 방지, 보안 코딩 등 '예전엔 부속품, 이제는 필수품'이 된 영역들이 표준에 정식 편입되었습니다.

조항	통제명	주 요 내 용
A.5.7	위협 인텔리전스	외부 위협 정보를 수집·분석·공유하는 체계
A.5.23	클라우드 서비스 보안	클라우드 서비스 도입·이용·종료 전 단계 보안 관리
A.5.30	ICT 비즈니스 연속성	재해 시 ICT 서비스의 중단 없는 운영
A.7.4	물리적 보안 모니터링	보호구역의 모니터링·이상 행위 감지
A.8.9	구성 관리(Configuration)	시스템·네트워크 구성정보의 표준화 및 관리

A.8.10	정보 삭제	보유 만료 시 안전한 삭제·파기
A.8.11	데이터 마스킹	민감 데이터의 가명화·익명화·은닉
A.8.12	데이터 유출 방지(DLP)	비인가된 정보 외부 유출 차단
A.8.16	모니터링 활동	이상행위·이상 트래픽의 지속적 감시
A.8.23	웹 필터링	악성·부적절 웹사이트 차단
A.8.28	보안 코딩	시큐어 코딩 가이드 적용 및 점검

이미 ISMS-P 를 운영 중이라면

신규 11 개 통제 대부분은 ISMS-P 통제항목과 매핑되는 내용입니다. 즉 국내에서 ISMS-P 를 운영 중인 회사라면 11 개 신규 통제 대응에 큰 부담이 없습니다. 반대로 ISO 27001:2013 으로만 운영하던 회사는 DLP·웹 필터링·구성 관리 영역에서 새 문서와 도구가 필요할 수 있습니다.

03. ISO 27001 vs ISMS-P — 무엇을 받아야 하나

'ISO 27001 과 ISMS-P 둘 다 받아야 하나요?' — 결론부터 말하면 '영업 무대가 어디인가'에 따라 달라집니다. 두 인증의 성격을 표 한 장으로 정리합니다.

항 목	ISO 27001	ISMS-P
인증 성격	국제 표준 인증	국내 법정 인증
발행 주체	ISO/IEC (국제표준화기구)	KISA (한국인터넷진흥원)
인증 의무	자발적 취득	법적 의무 (정보통신망법 제 47 조)
통제 수	Annex A 93 개	ISMS 80 개 / ISMS-P 102 개
개인정보 영역	27018·27701 별도 표준	ISMS-P 에 통합 (22 개 통제)
인증서 인지도	글로벌 (전 세계 통용)	국내 중심 (한국 시장)
심사 수수료	약 1,000~2,000 만 원/년	ISMS-P 1,000~1,800 만 원 (3 년)
유효기간	3 년 (매년 사후, 3 년 갱신)	3 년 (매년 사후, 3 년 갱신)

'둘 다 받는' 회사가 늘어나는 이유

두 인증은 통제 수준에서 약 70~80% 정도 겹칩니다. 그래서 '이미 ISMS-P 를 운영 중이라면 ISO 27001 추가 부담이 크지 않다'는 점을 활용해 동시에 받는 회사가 늘고 있습니다. 동시에 받으면 다음과 같은 이점이 있습니다.

- 국내 매출(공공·금융·B2B) + 해외 매출(SaaS·외국계) 양쪽에 대응
- 위험평가, 정책 문서, 위원회 등 공통 기반을 한 번에 운영
- 심사 일정을 묶어 동일 시기 진행 시 사내 부담 분산
- 글로벌 클라우드 진출 시 27017·27018 을 함께 추가하기 쉬움

어느 것부터 받아야 하나

원칙은 단순합니다.

- 주 매출이 국내인 회사 → ISMS-P 우선, ISO 27001 은 해외 거래가 본격화될 때

- 주 매출이 해외(SaaS·B2B 글로벌)인 회사 → ISO 27001 우선
- 두 시장 모두 진출 중인 회사 → ISMS-P 먼저, 6~12 개월 후 ISO 27001 동시 운영
- 정보통신망법상 의무대상 → ISMS-P 무조건 우선 (안 받으면 과태료 3,000 만 원)

'인증서 한 장' 차이가 만드는 영업 결과

글로벌 SaaS 영업에서 ISO 27001 은 협상 테이블에 앉기 위한 '티켓'입니다. 인증이 없으면 RFP 검토조차 받지 못하는 경우가 많습니다. 반대로 한국 공공·금융 입찰에서는 ISMS-P 가 그 '티켓' 역할을 합니다. 시장이 다르면 인증도 달라야 합니다.

04. 본문 조항 4~10 — ISMS 의 뼈대

ISO 27001 은 '본문 조항(4~10)'과 '부속서 A(Annex A)'로 구성됩니다. 본문 조항은 'ISMS 를 어떻게 운영해야 하는가'를 정의하며, 한 항목이라도 빠짐없이 충족해야 인증을 받을 수 있습니다. 반면 Annex A 는 '선택'과 '배제'가 가능합니다. 그래서 본문 조항 7 개를 먼저 이해하는 것이 ISO 27001 공부의 시작입니다.

본문 조항은 PDCA(Plan-Do-Check-Act) 사이클에 정확히 매핑됩니다. 4·5·6·7 조가 Plan(계획), 8 조가 Do(실행), 9 조가 Check(점검), 10 조가 Act(개선)에 해당합니다.

조항	제목	PDCA	핵심 요구사항
4	조직상황	Plan	조직의 내·외부 이슈 식별, 이해관계자·법적 요구사항 파악, ISMS 범위 결정
5	리더십	Plan	최고경영자의 의지 표명, 정보보안 정책 수립, 역할·권한·책임 명확화
6	계획	Plan	위험·기회 식별, 위험평가·위험처리, 정보보안 목표 설정
7	지원	Plan	자원·역량·인식·소통·문서화된 정보 관리
8	운용	Do	운영 계획·통제, 위험평가·위험처리 실행
9	성과평가	Check	모니터링·측정·분석·평가, 내부심사, 경영검토
10	개선	Act	부적합·시정조치, 지속적 개선

꼭 외워둬야 할 다섯 가지 의무 활동

본문 조항이 요구하는 활동 중 심사에서 가장 자주 점검되는 다섯 가지를 정리했습니다. 이 다섯 가지가 '안 굴러가는' 회사는 인증을 받기 어렵습니다.

1. 위험평가(Risk Assessment) — 자산·위협·취약점·영향도를 분석해 위험 등급을 산정 (조항 6.1.2)
2. 위험처리계획(Risk Treatment Plan) — 식별된 위험에 대한 처리 방법(수용/감소/회피/전가) 결정 (6.1.3)

3. 적용성 명세서(SoA) — Annex A 93 개 통제 각각에 대해 적용/배제 여부와 사유 명시 (6.1.3 d)

4. 내부심사(Internal Audit) — 매년 1 회 이상 자체 심사 (조항 9.2)

5. 경영검토(Management Review) — 최고경영자 주재로 ISMS 성과 검토 (조항 9.3)

'서류상 운영'과 '실제 운영'의 차이

위 다섯 활동은 모두 '기록(Documented Information)'이 남아야 합니다. 위험평가 보고서, 내부심사 체크리스트, 경영검토 회의록 — 모두 심사관이 확인합니다. 정책서만 두툼하고 실제 회의록·기록이 없으면 부적합 사유가 됩니다.

05. Annex A 93 개 통제항목 — 4 개 테마 완전 정리

ISO 27001:2022 Annex A 는 93 개의 통제를 4 개 테마로 분류합니다. 모든 통제를 회사가 다 적용해야 하는 것은 아닙니다. 위험평가 결과에 따라 '적용/배제'를 결정하고, 그 사유를 적용성 명세서(SoA)에 기록하면 됩니다.

테마	분 야	통제 수
A.5	조직 (Organizational Controls)	37 개
A.6	사람 (People Controls)	8 개
A.7	물리적 (Physical Controls)	14 개
A.8	기술적 (Technological Controls)	34 개
	합 계	93 개

A.5 조직 통제 (37 개) — 정책과 거버넌스의 출발점

가장 양이 많고 중요한 영역입니다. 정책·역할·자산·공급자·사고대응 등 '회사 전체의 정보보안 체계'를 다룹니다. 이 영역이 부실하면 다른 통제가 아무리 좋아도 ISMS 가 작동하지 않습니다.

- 정보보안 정책, 정보보안 역할·책임, 직무 분리, 경영진 책임
- 당국·이해관계자 연락, 위협 인텔리전스(신규), 자산 분류·라벨링
- 정보 분류·취급·전송, 접근통제 정책, 신원·접근권한 관리
- 공급자(외주) 관계 보안 — 계약·평가·모니터링
- 클라우드 서비스 보안(신규), 정보보안 사고 관리
- 법적·계약·규제 요구사항 식별, 지적재산권 보호
- 비즈니스 연속성·ICT 연속성(신규), 경영진 검토·내부심사

A.6 사람 통제 (8 개) — 가장 약한 고리는 사람

통제 수는 가장 적지만 결함 빈도가 매우 높습니다. 보안사고의 80% 이상이 '사람'에서 시작된다는 통계가 있을 정도로 핵심적인 영역입니다.

- 채용 전 신원 확인 — 학력·경력 검증, 비밀유지서약
- 고용 약관(Employment Terms) — 보안 책임을 계약서에 명시
- 보안 인식·교육·훈련 — 정기 교육, 피싱 모의훈련
- 징계 절차 — 보안 위반 시 처리 절차 문서화
- 퇴직·직무변경 — 권한 회수, 자산 반납, 비밀유지 의무 지속
- 기밀유지 합의(NDA) — 외주·파트너 포함
- 원격근무(Remote Working) — 재택·외부 작업 보안
- 정보보안 사건 보고 — 직원이 사고를 즉시 보고할 수 있는 체계

A.7 물리적 통제 (14 개) — 보이는 것을 지킨다

사무실·서버실·자료실 같은 물리적 공간과 그 안의 자산을 보호하는 통제입니다. 클라우드 시대에 '우리 서버 없는데?' 라고 생각할 수 있지만, 사무실 자체와 노트북·외장디스크·종이 문서 모두 이 영역의 대상입니다.

- 물리적 보호구역 설정·경계, 출입통제, 사무실/시설 보안
- 물리적 보안 모니터링(신규) — CCTV·이상행위 감지
- 외부·환경 위협 보호 — 화재·수해·정전
- 보호구역 작업, 무인 사용자 장비, 클리어 데스크·클리어 스크린
- 장비 배치·보호, 자산 반·출입 통제, 저장매체·매체 폐기
- 지원 유틸리티(전원·공조), 케이블 보안, 장비 유지보수

A.8 기술적 통제 (34 개) — 시스템·네트워크의 핵심

정보보안 담당자에게 가장 익숙한 영역입니다. 접근통제·암호화·로그·취약점 관리·보안 개발 등 기술적 보호대책 전반을 다룹니다.

- 사용자 단말 보안, 특수 권한·접근권한 관리, 정보 접근 제한
- 소스코드 접근통제, 보안 인증, 용량 관리
- 악성코드 방지, 기술적 취약점 관리, 구성 관리(신규)
- 정보 삭제(신규), 데이터 마스킹(신규), 데이터 유출 방지(신규)
- 백업, 시스템 이중화, 로깅·모니터링(신규), 시각 동기화
- 권한 있는 유틸리티 사용, 운영시스템 소프트웨어 설치
- 네트워크 보안·서비스 분리, 웹 필터링(신규), 암호화
- 보안 개발 라이프사이클(SDL), 시스템 변경관리, 시험 환경 분리
- 외주 개발 보안, 보안 코딩(신규), 시험 데이터 보호
- 운영 시스템 사용 감사

통제 수를 보고 미리 겁먹지 마세요

93 개라고 해도 실제로 회사가 '구현해야 하는' 통제는 위험평가 결과에 따라 60~80 개 수준으로 좁혀집니다. 클라우드 전용 회사라면 물리 보안 14 개 중 절반 이상이 '적용 안 함(Not Applicable)'으로 SoA 에 기록될 수 있습니다. 핵심은 '적용 여부'가 아니라 '배제 사유의 합리성'입니다.

06. 적용성 명세서(SoA) — 가장 중요한 문서

ISO 27001 인증 준비에서 가장 신경 써야 할 문서를 한 가지만 꼽으라면 '적용성 명세서(Statement of Applicability, SoA)'입니다. 본문 조항 6.1.3 에 따라 의무적으로 작성해야 하며, 심사관이 가장 먼저 확인하는 문서이기도 합니다.

SoA 가 무엇인가

SoA 는 Annex A 93 개 통제 각각에 대해 '우리 회사가 이 통제를 적용하는가, 적용하지 않는가, 그 이유는 무엇인가'를 표 형태로 기록한 문서입니다. 다음 4 가지가 반드시 포함되어야 합니다.

1. 적용/배제 여부 — 93 개 항목 모두에 'O / X' 표기
2. 적용 사유 — 어떤 위험 때문에 이 통제를 선택했는가
3. 배제 사유 — 왜 이 통제는 우리 회사에 해당하지 않는가
4. 구현 상태 — 현재 어느 정도 운영되고 있는가 (예: 운영 중, 부분 운영, 계획 중)

SoA 작성 예시

통제	적용	사유 / 구현 상태
A.5.1 정보보안 정책	O	정보보안 정책서 v2.1, 위원회 승인(2026-03-10), 전사 공유 완료
A.7.4 물리적 보안 모니터링	O	본사 서버실 CCTV 24/7 운영, 출입 로그 1 년 보관
A.7.13 장비 유지보수	X	클라우드 전용 운영, 자체 보유 장비 없음(공급자 책임으로 위탁 — A.5.19 적용)
A.8.11 데이터 마스킹	O	운영 DB 의 개인정보 6 개 컬럼에 마스킹 적용, 개발/시험 환경은 가명화 데이터만 사용
A.8.23 웹 필터링	O	전사 EDR 의 URL 필터링 모듈로 운영, 카테고리 차단 정책 분기별 검토

SoA 작성 시 자주 하는 실수

- '배제' 사유를 '해당 없음' 한 줄로 끝낸다 — 심사관이 가장 싫어하는 표현입니다. 왜 해당 없는지 구체적으로 설명해야 합니다.
- 위험평가 결과와 SoA 가 따로 논다 — 두 문서는 한 묶음입니다. 위험평가에서 도출된 위험이 SoA 에 반영되어야 합니다.
- '운영 중' 표시만 하고 증적이 없다 — 운영 중이라고 적은 통제는 모두 증적(Evidence)이 필요합니다.
- 통제 버전 관리 누락 — 2022 년판 통제 번호로 작성해야 하는데 2013 년 번호가 그대로 남아 있는 경우

SoA 는 '살아있는 문서'

SoA 는 한 번 작성하고 끝나는 문서가 아닙니다. 회사 사업·시스템·위험이 바뀌면 SoA 도 같이 바뀌어야 합니다. 표준은 '최소 연 1 회 또는 중대한 변경 시 갱신'을 요구합니다. 매년 SoA 를 검토·서명하는 절차를 사내에 정착시키세요.

07. 취득 절차 — Stage 1 과 Stage 2

ISO 27001 인증 심사는 'Stage 1'과 'Stage 2'로 명확히 분리됩니다. 두 단계를 모두 통과해야 인증서를 받을 수 있으며, 일반적으로 Stage 1 종료 후 4~6 주 뒤에 Stage 2 를 받습니다.

Stage 1 — 문서 심사 (Documentation Review)

보통 1~2 일간 진행되며, ISMS 문서가 표준 요구사항을 충족하는지를 점검합니다. 회사가 '인증을 받을 준비가 되었는가'를 확인하는 '레디니스 체크' 단계입니다.

■ 심사관이 확인하는 핵심 문서

- 정보보안 정책서·하위 지침서
- ISMS 범위 명세서(Scope Statement)
- 위험평가 방법론·위험평가 보고서·위험처리 계획
- 적용성 명세서(SoA)
- 내부심사 계획·결과
- 경영검토 회의록
- 정보보안 목표·KPI·측정 결과

Stage 1 에서 심각한 결함이 발견되면 Stage 2 일정이 연기되거나 중단될 수 있습니다. 즉 Stage 1 은 '일종의 사전 진단'이며, 여기서 도출된 지적사항을 4~6 주 동안 보완한 뒤 Stage 2 를 받는 것이 안전합니다.

Stage 2 — 현장 심사 (Main Audit)

보통 2~5 일간 진행되며, 회사가 ISMS 를 '실제로' 운영하고 있는지를 검증합니다. 심사관이 사무실을 방문해 인터뷰·관찰·증적 확인을 병행합니다.

■ Stage 2 에서 일어나는 일

- 직원 인터뷰 — 보안 정책을 알고 있는가, 실제로 따르고 있는가
- 시스템 관찰 — 접근통제·로그·백업이 작동하는지 직접 확인
- 증적 샘플링 — 수십 건의 운영 기록 중 무작위로 샘플 추출 검증
- 물리적 환경 점검 — 서버실·사무실·자료실 출입통제와 환경
- 사고 대응 시나리오 질의 — '만약 ~한 사고가 나면 어떻게 대응하는가'

심사 후 — 부적합 보완과 인증서 발급

Stage 2 종료 시점에 심사관이 '부적합(NCR)'을 정리해 통보합니다. 'Major(중대)'가 있으면 즉시 보완하고 재확인 후 인증, 'Minor(경미)'만 있으면 시정조치 계획서 제출 후 인증이 가능합니다. 최종 인증서는 인증기관 심의위원회 의결을 거쳐 발급되며, 통상 Stage 2 종료 후 3~6 주 안에 전달됩니다.

단계	활동	기간	산출물
① 컨설팅·구축	범위 결정·정책 수립·위험평가·통제 구현	3~5 개월	정책서, 위험평가, SoA
② 운영 누적	최소 2~3 개월 운영 증적 누적	2~3 개월	운영 기록·교육 기록
③ 내부심사	자체 심사 후 부적합 시정	2~4 주	내부심사 보고서
④ 경영검토	경영진 주재 ISMS 검토	1~2 주	경영검토 회의록
⑤ Stage 1	인증기관 문서 심사	1~2 일	Stage 1 보고서
⑥ 보완	Stage 1 지적 보완	4~6 주	보완 증적
⑦ Stage 2	인증기관 현장 심사	2~5 일	Stage 2 보고서·NCR
⑧ 시정조치	NCR 시정·재확인	2~6 주	시정조치 보고서
⑨ 인증의결	인증기관 심의위원회	2~4 주	인증서 발급 ✦

08. 비용은 얼마나 드는가

ISO 27001 비용은 회사 규모와 인증 범위에 따라 천차만별이지만, 한국 시장에서 통용되는 '평균치'는 비교적 명확하게 잡혀 있습니다. 의사결정 단계에서 참고할 수 있는 4 개 카테고리로 정리합니다.

비용 항목	범위	전형적 금액
① 심사 수수료(최초)	Stage 1 + Stage 2 인증기관 심사비	약 800~1,500 만 원
② 사후심사 수수료	1~2 년차 매년 (반일~2 일 심사)	약 500~800 만 원/년
③ 갱신심사 수수료	3 년차 (Stage 2 와 유사 강도)	약 800~1,200 만 원
④ 컨설팅 비용	위험평가·문서화·예비점검·교육 지원	약 3,000~8,000 만 원
⑤ 시스템 구축 비용	DLP·웹 필터링·로그관리 등 신규 도입	약 1,000 만 원~수억 원
⑥ 내부 인건비·교육비	담당자 투입, 교육비, 부대비용	프로젝트당 1,500 만 원 이상

심사 수수료 산정 — 직원 수가 기준

ISO 27001 심사 수수료는 '인증 범위 내 직원 수'를 기준으로 산정합니다.

한국인정지원센터(KAB)가 표준 인증스킴 요구사항에서 직원 수 구간별 최소 심사일수를 정의하고 있고, 인증기관은 이 일수에 심사관 일당을 곱해 수수료를 책정합니다.

인증 범위 직원 수	Stage 1 + Stage 2 (최소 일수)	사후심사 (최소 일수)
10 명 이하	약 3 일	약 1 일
11~25 명	약 4 일	약 1.5 일
26~45 명	약 5 일	약 1.5 일
46~125 명	약 6.5 일	약 2 일
126~425 명	약 8.5 일	약 3 일
426~1,175 명	약 11 일	약 4 일

심사관 일당은 인증기관·심사관 등급에 따라 80~150 만 원 수준입니다. '직원 50 명 회사가 KQA 에서 최초 인증을 받는다'고 가정하면 약 6.5 일 × 100 만 원 = 650 만 원 + 부대비용으로 800 만 원 안팎이 됩니다.

'BSI 에서 받으면 더 비싸지 않나요'

흔한 질문입니다. 일반적으로 외국계 인증기관(BSI·DNV·TUV 등)이 국내 인증기관(KQA 등)보다 20~50% 정도 수수료가 비쌉니다. 그러나 다음과 같은 '무형의 가치' 때문에 외국계를 선호하는 회사가 있습니다.

- 글로벌 고객사가 인증기관 이름을 보고 신뢰도를 판단하는 경우 (특히 영미권)
- 외국 본사·외국계 투자자에게 보고할 때의 인지도
- 다국어 인증서 발급 (영문본 즉시 제공)

다만 '인증의 효력' 자체는 KAB 또는 IAF MLA(국제 상호인정) 인정 인증기관이라면 모두 동일합니다. 국내 영업이 주력이면 KQA, 글로벌 영업이 주력이면 BSI/DNV/TUV/Bureau Veritas 등을 검토하는 것이 합리적입니다.

컨설팅 비용을 줄이는 방법

ISO 27001 컨설팅 비용은 '투입 인원 × 기간 × 등급'으로 결정됩니다. 회사 내부에 정보보안 인력이 있다면 '문서 작성을 회사가, 검토·자문을 컨설팅사가' 분담하는 '부분 컨설팅' 모델로 50~70%까지 비용을 절감할 수 있습니다. 또한 ISMS-P 를 이미 운영 중이라면 컨설팅 범위가 '27001 차이 부분'으로 좁혀져 비용이 크게 줄어듭니다.

09. 기간은 얼마나 걸리는가 — 6 개월 로드맵

'준비 시작'부터 '인증서 수령'까지 평균 6~9 개월이 걸립니다. 단, '최소 2~3 개월의 운영 증적'이 필수이므로, 정책 문서를 만든 직후 곧바로 심사를 받을 수는 없습니다. 일정에 맞춰 다음 9 단계 로드맵을 권장합니다.

월차	주요 활동	마일스톤
M1	킥오프, 인증범위 확정, 컨설팅사 선정, 갭 분석	범위 명세서·갭 분석 보고서
M2	위험평가 방법론·자산 식별·위협 분석	자산 목록·위협 매트릭스
M3	위험평가 실시·위험처리 계획·SoA v0.1	위험평가 보고서·SoA 초안
M4	정책·지침 수립, 통제 구현, 직원 교육	정책서 v1.0·교육 이수
M5	운영 증적 누적, 모니터링·KPI 측정	운영 기록·KPI 대시보드
M6	내부심사 실시, 부적합 시정, 경영검토	내부심사 보고서
M7	Stage 1 심사, 보완 4~6 주	Stage 1 보고서
M8	Stage 2 심사, NCR 시정조치	Stage 2 보고서
M9	인증위원회 의결, 인증서 수령	인증서 ✦

단축할 수 있는 구간과 단축이 위험한 구간

단축이 가능한 구간:

- M1 갭 분석 — 이미 ISMS-P 를 운영 중이라면 1 주 내 종료
- M4 통제 구현 — 클라우드 보안 서비스 활용 시 도입 기간 단축
- M9 인증서 발급 — 인증기관 의결 일정에 따라 빠르면 2 주

단축하면 위험한 구간:

- M5 운영 증적 누적 — 최소 2 개월, 권장 3 개월. 이 기간을 줄이면 부적합이 폭증

- M6 내부심사 — 형식적으로 진행하면 Stage 1·2 에서 같은 결함이 그대로 도출
- M7 Stage 1 보완 — 4~6 주의 '리허설 보완'이 합격률을 결정

10. 사후관리 — 매년 사후심사, 3 년 갱신

ISO 27001 인증서의 유효기간은 발급일로부터 3 년입니다. 그러나 '3 년 동안 자유'가 아니라, 매년 사후심사(Surveillance Audit)를 받아야 인증이 유지됩니다.

연차	심사 종류	기 간	강 도
1 년차	최초심사 (Stage 1+2)	3~7 일 (회사 규모별)	전 통제 점검
2 년차	사후심사 1 차	1~3 일	샘플 점검 + 변경사항
3 년차	사후심사 2 차	1~3 일	샘플 점검 + 변경사항
4 년차	갱신심사 (Recertification)	2~5 일	전 통제 재심사

사후심사에서 자주 점검되는 것

사후심사는 'ISMS 가 변함없이 잘 운영되고 있는가'와 '지난 1 년 동안 발생한 변화가 ISMS 에 반영되었는가'를 봅니다. 따라서 다음 항목이 우선 점검됩니다.

- 지난 심사의 부적합(NCR) 시정 결과
- 조직·시스템·서비스의 중대한 변경사항이 ISMS 에 반영되었는가
- 위험평가·SoA 가 최신 상태인가
- 내부심사·경영검토가 정기적으로 실시되었는가
- 보안 사고·보안 사건 처리 기록

갱신심사를 놓치면

유효기간 만료 전에 갱신심사를 완료하지 못하면 '인증 효력 상실' 상태가 됩니다. 일정 기간(보통 6 개월) 내에 신속 갱신이 가능한 경우도 있지만, 그 기간을 넘기면 '처음부터 다시' Stage 1·2 심사를 받아야 합니다. 만료 6 개월 전부터 일정을 챙기세요.

'인증서 효력'은 인증기관 홈페이지에서 검증 가능

주요 인증기관은 자사 웹사이트에 인증서 검증 페이지를 운영합니다. 거래처가 인증서 진위를 확인할 수 있고, 만료·취소된 인증서를 도용하면 즉시 적발됩니다. 인증서 PDF 만 보고 신뢰하지 말고, 반드시 인증기관 사이트에서 검증해야 합니다.

11. 부적합(NCR) — Major vs Minor

Stage 2 와 사후심사에서 가장 부담스러운 단어가 '부적합(Nonconformity, NCR)'입니다. 표준 요구사항을 충족하지 못한 사항을 의미하며, 심각도에 따라 'Major'와 'Minor'로 구분됩니다.

구분	정의	인증 영향	시정 기한
Major	표준 요구사항을 '완전히 미이행'하거나 시스템적 결함	최초: Stage 2 통과 불가 / 사후: 인증 효력 위협	통상 30~90 일 내 시정 + 재심사
Minor	단발성·국지적 결함, 시스템 자체에는 문제 없음	인증 진행 가능 (시정조치 계획만 제출)	통상 90 일 내 시정 증빙 제출

Major 부적합 사례

- 위험평가를 한 번도 실시하지 않았거나, 위험평가 보고서가 존재하지 않는 경우
- 내부심사가 1 년 이상 미실시
- 방화벽 정책이 잘못 설정되어 외부에서 내부 시스템에 무단 접근 가능
- 백업 정책은 '일 1 회'이지만 실제로는 한 달에 두세 번만 실행
- 다수의 Minor 부적합이 동일 영역에서 반복 → 시스템적 결함으로 격상

Minor 부적합 사례

- 퇴사자의 1 개 시스템 계정이 회수되지 않음 (다른 시스템은 모두 정상 회수)
- 정보보안 정책서의 검토 일자가 1 년을 초과함
- 특정 부서의 보안교육 이수율이 95%로 100% 미달
- SoA 에 '배제 사유'가 'N/A' 한 단어로만 기재됨

부적합 대응의 정석

부적합은 단순히 '발견된 한 건을 고치는 것'으로 끝나면 안 됩니다. 표준은 '근본원인 분석(Root Cause Analysis)'과 '유사 결함 재발 방지 조치'를 요구합니다.

1. 발견 사항 정리 — 무엇이, 어디서, 언제 발견되었는가
2. 근본원인 분석 — 왜 발생했는가 (5 Why)
3. 수정조치 — 발견된 문제 자체를 즉시 해결
4. 예방조치 — 같은 원인의 다른 사례가 없는지 점검 및 처리
5. 효과성 검증 — 일정 기간 후 재발 여부 확인
6. 기록·보고 — 시정조치 기록을 인증기관에 제출

12. 인증기관 선택 — 국내 KQA 부터 BSI·DNV 까지

ISO 27001 인증은 '인정기구(AB) → 인증기관(CB) → 신청자'의 구조로 운영됩니다. 신청자는 인증기관을 선택해 심사를 받게 되는데, 이때 인증기관이 '공신력 있는 인정기구'의 인정을 받았는지 반드시 확인해야 합니다.

인정기구(AB) 이해

인정기구	지역	특 징
KAB (한국인정지원센터)	한국	한국 정부가 지정한 공식 인정기구
UKAS	영국	전 세계에서 가장 신뢰도 높은 인정기구
ANAB	미국	북미 시장 진출 시 우대
JAS-ANZ	호주·뉴질랜드	오세아니아 지역
JIPDEC	일본	일본 시장

이 인정기구들은 'IAF MLA(국제 상호인정 협정)'에 가입되어 있어, 어느 한 인정기구의 인정을 받은 인증기관이 발급한 인증서는 전 세계에서 동일하게 인정됩니다. 즉 KAB 인정 KQA 의 인증서와 UKAS 인정 BSI 의 인증서는 '공식적으로' 동등한 효력을 갖습니다.

한국에서 자주 보이는 인증기관

인증기관	본 사	특 징
KQA (한국품질보증원)	한국	KAB 인정 국내 제 1 호 ISO 27001 인증기관
KSA (한국표준협회)	한국	ISO 9001 등 다양한 표준 통합 심사 강점
KFQ (한국품질재단)	한국	다양한 ISO 표준 인증 가능
BSI (영국표준협회)	영국	ISO 표준의 '본가', 글로벌 인지도 1 위
DNV	노르웨이	에너지·해운·금융 분야 강세
TUV Rheinland / TUV SUD /	독일	제조·자동차 산업 강점, 기술 평판 우수

TUV Nord		
Bureau Veritas	프랑스	글로벌 네트워크 광범위
SGS	스위스	검사·시험 분야 세계 최대
LRQA / Intertek	영국·미국	다국적 기업 다수 채택

인증기관 선택 시 체크리스트

- KAB 또는 IAF MLA 인정기구의 'ISO 27001 분야' 인정을 받았는가
- 우리 회사 업종에 대한 심사 경험이 있는가
- 한국어 심사관·한국어 보고서가 가능한가 (해외 인증기관 선택 시)
- 심사 일정이 우리 회사 일정과 맞는가
- 사후심사·갱신심사 비용까지 포함한 3 년 토탈 견적은 어떤가
- 인증서를 영문·국문 모두 발급해 주는가

주의 — '비공식' 인증기관에 속지 마세요

한국에서 'ISO 27001 인증' 검색 광고를 보면 인정기구 인정 없이 자체 발급하는 '짝퉁 인증'이 섞여 있습니다. 이런 인증서는 거래처가 검증하면 즉시 가짜로 드러납니다. 반드시 KAB 또는 IAF MLA 회원 인정기구 홈페이지에서 인증기관 명단을 확인하세요.

13. ISMS-P 와 동시 취득 전략

한국에서 정보보안 인증을 검토하는 회사라면 십중팔구 'ISMS-P 와 ISO 27001 둘 다 받아야 하나'를 고민합니다. 결론은 '대부분의 경우 둘 다 받는 것이 효율적'이며, 다만 '순서'와 '일정'이 중요합니다.

두 인증의 통제 매핑

ISMS-P 102 개 통제 중 약 70~80 개는 ISO 27001 Annex A 93 개와 직접 매핑됩니다. 즉 한쪽 인증을 운영 중이면 다른 쪽 인증의 약 70~80%가 이미 준비되어 있다는 뜻입니다. 다만 다음 영역은 '추가 작업'이 필요합니다.

방향	추가로 필요한 작업
ISMS-P → ISO 27001 추가	본문 조항 4·6·9 의 '리스크 기반 사고' 강화, SoA 작성, 내부심사·경영검토 형식 정비
ISO 27001 → ISMS-P 추가	개인정보 처리단계별 22 개 통제 (수집·이용·제공·파기·정보주체 권리), 법령 매핑(개인정보보호법·정보통신망법) 강화

권장 순서 — 시장에 따라 다르다

[A] 국내 매출 비중이 높은 회사 (B2B SaaS·이커머스·핀테크)

- 1 단계: ISMS-P 우선 (정보통신망법 의무대상이면 무조건 우선)
- 2 단계: 6~12 개월 후 ISO 27001 추가 (글로벌 영업 본격화 시점에 맞춰)
- 장점: 법적 리스크 우선 해소, 컨설팅 부담 분산

[B] 글로벌 매출 비중이 높은 회사 (해외 SaaS·외국계)

- 1 단계: ISO 27001 우선
- 2 단계: 국내 의무대상이 되는 시점에 ISMS-P 추가

- 장점: 글로벌 영업 즉시 가능, ISO 27017·27018 추가 확장 용이

[C] 두 시장 모두 진출 중인 대기업·중견기업

- 1 단계: ISMS-P 먼저 (3~6 개월 전 시작)
- 2 단계: ISMS-P 인증 후 즉시 ISO 27001 통합 운영 (별도 인증)
- 3 단계: 사후심사 일정을 동일 분기로 묶어 운영

'통합 운영 매뉴얼'이 핵심

두 인증을 받는다고 정책서를 두 벌 만들 필요는 없습니다. 단일 정보보안 정책서·지침서를 두고, '이 항목은 ISMS-P A.B.C 와 ISO 27001 A.X.Y 에 동시 매핑됨' 형태로 통제 매트릭스만 별도 관리하는 '통합 운영 매뉴얼' 방식이 가장 효율적입니다.

14. 인증 준비 체크리스트

Stage 2 심사 전 반드시 확인해야 할 항목을 영역별로 정리했습니다. 각 항목 옆에 ☑ 표시를 하며 점검해 보세요.

[리더십과 거버넌스 (조항 5)]

- ☐ 최고경영자가 정보보안 정책을 서명·승인했는가
- ☐ 정보보안 책임자(CISO 등)와 그 권한이 문서화되어 있는가
- ☐ 정보보안 위원회/협의체가 정기 개최되고 회의록이 보관되는가
- ☐ 정보보안 목표가 SMART(구체·측정·달성·관련·기한)하게 정의되어 있는가

[조직상황과 범위 (조항 4)]

- ☐ ISMS 적용 범위(서비스·조직·시스템·물리적 위치)가 명확히 정의되어 있는가
- ☐ 내·외부 이슈와 이해관계자 요구사항이 식별·문서화되어 있는가
- ☐ 범위에서 제외된 부분과 그 사유가 명시되어 있는가

[위험평가와 SoA (조항 6)]

- ☐ 위험평가 방법론이 문서화되어 있는가 (자산 가치·위협·취약점·영향도 산정)
- ☐ 위험평가 보고서가 1 년 이내에 갱신되어 있는가
- ☐ 위험처리 계획이 작성되어 있고 이행 진척이 추적되는가
- ☐ SoA 에 93 개 통제 모두에 대해 적용/배제 사유가 기재되어 있는가
- ☐ SoA 가 최고경영자의 승인을 받았는가

[지원 (조항 7)]

- ☐ 정보보안 인력의 자격·역량 요구사항이 정의되어 있는가
- ☐ 전 직원의 보안 인식 교육이 정기적으로 시행되고 이수율이 기록되는가

- ☐ 외주 인력에 대한 비밀유지서약(NDA)이 체결되어 있는가
- ☐ 문서·기록의 작성·승인·배포·폐기 절차가 운영되는가

[운용과 통제 (조항 8 + Annex A)]

- ☐ 관리자 계정에 다중 인증(MFA)이 적용되어 있는가
- ☐ 퇴직·직무변경 시 권한 회수 절차가 즉시 작동하는가
- ☐ 정보 분류 체계가 정의되고 라벨링·취급 절차가 운영되는가
- ☐ 백업이 정책대로 실행되고 복구 시험이 정기적으로 수행되는가
- ☐ 보안 사고 대응 절차와 비상연락망이 최신 상태인가
- ☐ 공급자(외주·클라우드) 보안 평가 기록이 있는가
- ☐ 취약점 점검·패치 관리 기록이 누적되어 있는가
- ☐ 물리적 접근통제(서버실·자료실)가 작동하는가

[성과평가 (조항 9)]

- ☐ 보안 KPI(예: 사고 건수·교육 이수율·패치 적용률)가 측정되고 있는가
- ☐ 내부심사가 ISMS 전 영역에 대해 1 년 이내 실시되었는가
- ☐ 내부심사에서 발견된 부적합이 시정되었는가
- ☐ 경영검토 회의가 1 년 이내 개최되고 회의록이 보관되는가

[개선 (조항 10)]

- ☐ 부적합 발생 시 근본원인 분석·예방조치 절차가 작동하는가
- ☐ 지속적 개선 활동(예: 위험평가 갱신·정책 개정)의 기록이 있는가
- ☐ 지난 심사의 부적합이 모두 종결되었는가

[2022 년판 신규 통제]

- ☐ 위협 인텔리전스 수집·공유 체계가 있는가 (A.5.7)
- ☐ 클라우드 서비스 도입·이용·종료 보안 절차가 있는가 (A.5.23)
- ☐ ICT 비즈니스 연속성 계획·시험이 있는가 (A.5.30)
- ☐ 물리적 보안 모니터링이 작동하는가 (A.7.4)
- ☐ 데이터 마스킹/유출 방지(DLP) 통제가 운영되는가 (A.8.11, A.8.12)
- ☐ 보안 코딩 가이드와 점검 절차가 있는가 (A.8.28)

15. 자주 묻는 질문 (FAQ)

Q1. 직원 5 명짜리 스타트업도 받을 수 있나요?

받을 수 있습니다. 인증 범위와 자원에 따라 통제 강도가 달라질 뿐 직원 수 제한은 없습니다. 다만 5 명 회사라면 '직무 분리(A.5.3)' 같은 통제는 현실적으로 어려우므로, SoA 에 '회사 규모상 보완 통제(이중 검토·로그 모니터링)로 대체' 식으로 합리적 사유를 기재하면 됩니다. 최근에는 B2B SaaS 스타트업의 '계약 조건' 때문에 5~10 명 회사가 ISO 27001 을 받는 사례가 늘고 있습니다.

Q2. 컨설팅 없이 자체적으로 받을 수 있나요?

이론상 가능합니다. 다만 ISO 27001 표준서·지침서의 양과 한국어 자료의 부족, 위험평가·SoA 작성의 난이도를 고려하면 '정보보안 전담 인력 1~2 명이 6 개월 풀타임 투입' 수준의 노력이 필요합니다. 최근에는 '플랫폼형 GRC 도구(Vanta, Drata, Sprinto 등)'를 활용한 자체 준비도 가능해졌지만, 한국어 심사 대응까지 고려하면 부분 컨설팅을 권장합니다.

Q3. ISMS-P 를 받으면 ISO 27001 은 자동으로 인정되나요?

아닙니다. 두 인증은 별도의 인증서이며 자동 매핑·자동 발급은 없습니다. 다만 ISMS-P 운영 자료를 ISO 27001 심사 증적으로 활용할 수는 있어, 두 인증을 통합 운영하면 컨설팅·심사 부담이 크게 줄어듭니다.

Q4. Annex A 통제 중 일부를 빼도 되나요?

네, 가능합니다. 위험평가 결과에 따라 '적용 안 함(Not Applicable)'으로 SoA 에 기재하면 됩니다. 단 사유가 합리적이어야 합니다. 예를 들어 '클라우드 전용 서비스이므로 자체 데이터센터 관련 통제 일부를 배제'는 합리적이지만, '비용이 많이 들어서 배제'는 받아들여지지 않습니다.

Q5. 심사 도중에 회사가 인수합병(M&A)되면 인증서는 어떻게 되나요?

인증서는 법인격에 종속됩니다. 합병·분할로 법인격이 바뀌면 인증기관에 '변경 신고'를 해야 하며, 사업 범위가 크게 변하면 '특별 심사(Special Audit)'가 필요할 수 있습니다. M&A 를 검토 중이라면 해당 분기의 사후심사 일정과 변경 신고 절차를 미리 인증기관과 협의하세요.

Q6. 외국 본사 인증서를 한국 법인이 그대로 쓸 수 있나요?

외국 본사 ISO 27001 인증의 '적용 범위'에 한국 법인이 명시적으로 포함되어 있다면 가능합니다. 그러나 한국 법인이 별도 시스템·서비스를 운영하고 있다면 '인증 범위 외'가 되어 활용할 수 없습니다. 한국 거래처가 인증서의 적용 범위를 확인하면 곧바로 드러나는 부분이므로, 별도 인증 또는 본사 인증의 범위 확장이 필요합니다.

Q7. ISO 27001:2013 으로 받았는데 2022 년판으로 언제까지 전환해야 하나요?

전환 마감은 2025 년 10 월 31 일이었습니다. 그 이후로 모든 신규·갱신 인증은 자동으로 2022 년판으로 발급됩니다. 2022 년판으로 전환하지 못한 인증서는 효력을 상실하므로, 만약 아직 2013 년판 보유 상태라면 즉시 인증기관에 문의하세요.

Q8. ISO 27001 외에 함께 검토할 표준은?

회사 성격에 따라 다음 표준을 함께 검토할 만합니다. (1) ISO 27017 — 클라우드 보안, (2) ISO 27018 — 클라우드 개인정보, (3) ISO 27701 — 개인정보 관리체계, (4) SOC 2 — 미국 시장 B2B SaaS 영업, (5) PCI DSS — 카드 결제 처리. 27001 인증을 '기반'으로 하면 위 표준들을 확장하기 쉽습니다.

16. 참고자료 및 공식 사이트

공식 표준·인정기구

기관/사이트	주소	용도
ISO 공식 사이트	iso.org	ISO/IEC 27001:2022 표준 원문 구매
KAB (한국인정지원센터)	kab.or.kr	국내 인정 인증기관 명단 확인
IAF (국제인정포럼)	iaf.nu	전 세계 인정기구·MLA 회원 확인
KISA ISMS-P 누리집	isms.kisa.or.kr	ISMS-P 동시 취득 시 참고

주요 인증기관 (한국 활동)

인증기관	사이트	특 징
KQA (한국품질보증원)	kqa.co.kr	국내 1 호 ISO 27001 인증기관
KSA (한국표준협회)	ksa.or.kr	ISO 표준 통합 인증
BSI Korea	bsigroup.com/ko-KR	글로벌 인지도 1 위
DNV Korea	dnv.com	다국적 기업 다수 채택
TUV Rheinland Korea	tuv.com/korea	기술 평판 우수
Bureau Veritas Korea	bureauveritas.kr	글로벌 네트워크

추천 학습자료

- ISO/IEC 27001:2022 표준서 (ISO 공식)
- ISO/IEC 27002:2022 통제 가이드 (Annex A 통제 해설)
- ISO 27001 정보보안경영시스템 인증스킴 요구사항 (KAB 발행)
- ISO 27001 Toolkit / Template Pack (Advisera, ISMS.online 등)
- 정보보호 및 개인정보보호 관리체계 인증기준 안내서 (KISA)

- Annex A 통제별 구현 가이드 (NIST SP 800-53 매핑)

맺음말

이 백서를 끝까지 읽으셨다면 'ISO 27001 은 결국 회사를 시스템적으로 운영하는 방법'이라는 점을 느끼셨을 겁니다. 인증서 한 장을 받는 것이 목적이 아니라, 그 과정에서 회사의 보안 체계가 한 단계 성숙해지는 것이 진짜 목적입니다.

운영 측면에서 한 가지 강조하고 싶은 것이 있습니다. '완벽한 첫 인증'보다 '꾸준한 개선'이 훨씬 가치 있습니다. 처음 받는 인증서는 '출발선'이고, 매년 사후심사에서 한 발짝씩 나아지는 것이 '진짜 ISMS'입니다. 이 백서가 그 출발선에 서는 데 도움이 되길 바랍니다.

— 백 지 석 —