무료 백서

ISMS 취득 백서

누구나 이해할 수 있는 정보보호 관리체계 인증 가이드

취득 방법 · 비용 · 기간 · 통제항목 · 결함 사례까지

백 지 석

2026

머리말 — 이 백서를 시작하며

ISMS 는 더 이상 '대기업의 일'이 아닙니다. 매출 100 억 원을 넘긴 정보통신서비스 사업자, 이용자 100 만 명을 넘긴 플랫폼, 그리고 일정 규모 이상의 병원·대학까지, 인증을 의무로 받아야 하는 기업과 기관이 매년 늘어나고 있습니다. 받지 않으면 최대 3,000 만 원의 과태료가 부과됩니다.

그런데 막상 'ISMS 를 받아야 한다'는 말을 듣고 인터넷을 검색하면 용어부터 어렵습니다. ISMS 와 ISMS-P 는 어떻게 다른지, 102 개의 통제항목이 무엇인지, 비용이 1 억 원이라는 말과 수백만 원이라는 말이 동시에 나오는 이유는 무엇인지. 정보는 많은데 정작 '처음부터 끝까지'를 한 번에 보여주는 자료는 드뭅니다.

이 백서는 그 빈틈을 채우기 위해 만들었습니다. ISMS·ISMS-P 가 무엇인지, 누가 받아야 하는지, 어떤 절차로 어떤 비용과 기간이 드는지, 인증을 받기 위해 어떤 통제항목을 만족해야 하는지, 그리고 자주 발생하는 결함은 무엇인지 — 한 권으로 정리했습니다. 정보보호 담당자뿐 아니라 경영진, 개발자, 인사·총무 담당자, 그리고 '우리 회사가 ISMS 대상인지' 가 궁금한 모든 분께 도움이 되도록 가능한 한 쉬운 표현으로 풀어 썼습니다.

이 백서는 무료입니다. 부담 없이 읽고, 동료에게 공유하고, 인증 준비의 첫걸음으로 활용해 주세요. 잘못된 점이나 보완할 점이 있다면 알려 주시면 다음 판에 반영하겠습니다.

저자 백지석

목 차

01. ISMS, 도대체 무엇인가

정보보호 관리체계, 한 문장으로 말하면

ISMS(Information Security Management System)는 '정보보호 관리체계'의 영문 약자입니다. 쉽게 말해 회사가 '우리는 정보를 안전하게 지키기 위한 절차와 기술을 갖추고, 실제로 그렇게 운영하고 있다'는 것을 국가에서 인증받는 제도입니다.

여기서 핵심 단어는 '관리체계'입니다. 방화벽 한 대 사면 보안이 끝나는 것이 아니라, 정책을 만들고(Plan) → 실제로 운영하고(Do) → 점검하고(Check) → 개선하는(Act) 사이클이 회사 안에 살아 있어야 한다는 뜻입니다. ISMS 는 그 사이클이 제대로 돌아가는지 외부 전문가가 와서 검증해 주는 제도라고 이해하면 됩니다.

PDCA 사이클이란

Plan(계획) — Do(실행) — Check(점검) — Act(개선)의 약자입니다. 품질 경영의 기본 사이클로, ISMS 인증의 '1.관리체계 수립 및 운영' 영역이 바로 이 사이클을 따르고 있습니다. 한 번 인증을 받았다고 끝이 아니라, 매년 사이클을 돌리며 개선해 나가는 것이 ISMS 의 본질입니다.

ISMS 의 법적 근거

ISMS 제도는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법) 제 47 조에 근거를 두고 있습니다. ISMS-P 인증의 'P(Personal Information)' 부분, 즉 개인정보보호 영역은「개인정보보호법」제 32 조의 2 를 근거로 합니다. 두 법을 묶어 운영하기 위해 과학기술정보통신부와 개인정보보호위원회가 공동으로 고시를 운영합니다.

다시 말해 ISMS 는 '회사가 자율적으로 받는 인증'이 아니라, 일정 요건을 충족하는 사업자에게 법으로 의무화된 인증입니다. 이 점이 ISO 27001 같은 국제 표준 인증과의 가장 큰 차이입니다.

왜 ISMS 를 받아야 하는가 — 세 가지 이유

1. 법적 의무 회피 — 대상 사업자가 인증을 받지 않으면 최대 3,000 만 원의 과태료가 부과됩니다.

2. 고객·파트너 신뢰 확보 — 공공기관 입찰, 대기업 협력사 등록, B2B SaaS 영업에서 ISMS 인증서는 사실상 표준 요구사항이 되어 있습니다.

3. 내부 보안 수준 향상 — 102 개 통제항목을 점검하면서 그동안 보이지 않던 빈틈이 드러나고, 사고 발생 시 책임 소재와 대응 절차가 명확해집니다.

02. ISMS 와 ISMS-P, 무엇이 다른가

'ISMS'와 'ISMS-P' — 한 글자 차이지만 인증 범위와 비용, 그리고 받을 수 있는 효과가 모두 다릅니다. 처음 인증을 검토하는 분들이 가장 자주 헷갈리는 부분이므로 표 한 장으로 정리하고 시작합니다.

구 분	ISMS	ISMS-P
정식 명칭	정보보호 관리체계 인증	정보보호 및 개인정보보호 관리체계 인증
통제항목 수	80 개	102 개 (ISMS 80 개 + 개인정보 22 개)
적용 영역	정보보호 전반	정보보호 + 개인정보 처리 전 단계
주요 근거 법령	정보통신망법 제 47 조	정보통신망법 + 개인정보보호법 제 32 조의 2
권장 대상	개인정보 처리량이 적은 일반 IT 서비스	이커머스·SNS·핀테크 등 개인정보 대량 처리
심사 수수료(일반)	약 800~1,400 만 원	약 1,000~1,800 만 원
심사 기간	통상 5 일 내외	통상 7~10 일

어느 쪽을 받아야 하나

법적 의무 대상자는 'ISMS 와 ISMS-P 중 하나'를 선택해서 받으면 됩니다. 즉, ISMS-P 를 받았다면 ISMS 는 별도로 받지 않아도 됩니다. 다만 다음과 같은 경우에는 ISMS-P 를 권장합니다.

- 회원가입형 서비스를 운영해 개인정보를 다량 수집·보관하는 경우
- 결제 정보, 실명·주민번호 등 민감한 식별정보를 처리하는 경우
- 글로벌 시장 진출, 대기업·금융기관 납품을 염두에 둔 경우 (개인정보 보호 수준을 더 강하게 어필 가능)

반대로 자체 서비스에 회원가입이 없거나 개인정보 처리가 매우 제한적인 경우, ISMS 만으로도 충분합니다. 통제항목 22 개 차이가 그대로 컨설팅 공수와 비용 차이로 이어지므로, 무리해서 ISMS-P 를 받을 필요는 없습니다.

한 번에 끝내고 싶다면

처음부터 ISMS-P 를 받는 것을 권장합니다. ISMS 를 받은 뒤 1~2 년 후 ISMS-P 로 확장하는 경우 통제항목 매핑·문서 재작성·재심사가 다시 필요해 오히려 총비용이 더 들 수 있습니다.

03. 누가 받아야 하는가 — 의무대상 완전 정리

정보통신망법 제 47 조 제 2 항은 다음 다섯 가지 조건 중 하나라도 해당하면 ISMS(또는 ISMS-P) 인증을 의무적으로 받아야 한다고 규정하고 있습니다. 자기 회사가 어디에 해당하는지 빠짐없이 체크해 보세요.

구분	세부 기준	비고
① ISP	정보통신망 서비스 제공자(KT·SKT·LG U+ 등)	회선임대·인터넷접속서비스 사업자
② IDC	집적정보통신시설 사업자	데이터센터 운영사
③ 매출액 1,500 억 원 이상	전년도 연간 매출액 또는 세입 1,500 억 원 이상	단, 상급종합병원·재학생 1 만 명 이상 학교 포함
④ 정보통신 매출 100 억	정보통신서비스 부문 전년도 매출 100 억 원 이상	온라인 쇼핑몰·플랫폼·SaaS 등
⑤ 이용자 100 만 명	전년도 말 직전 3 개월간 일평균 이용자 100 만 명 이상	월간이 아닌 일평균 기준

‘정보통신서비스 매출 100 억 원’의 함정

④번 기준은 가장 자주 오해가 발생하는 항목입니다. ‘회사 전체 매출’이 아니라 ‘정보통신서비스 부문 매출’이라는 점을 반드시 기억해야 합니다. 예를 들어 제조업체가 총 매출 500 억 원을 올리고 그중 자사 쇼핑몰 매출이 50 억 원이라면, 정보통신서비스 매출은 100 억 원 미만이므로 의무대상이 아닐 수 있습니다.

반면 SaaS 스타트업의 매출 대부분이 구독료·서비스 이용료라면 그 전액이 정보통신서비스 매출로 잡혀, 100 억 원을 넘는 시점에 의무대상이 됩니다. 매출 산정 기준이 모호한 경우 KISA 에 사전 유권해석을 요청하는 것이 안전합니다.

‘일평균 이용자 100 만 명’ 산정 방법

⑤번 기준은 월간 이용자(MAU)가 아닌 '일평균 이용자'를 봅니다. 직전 3 개월간 일평균 방문자(또는 로그인 사용자) 수를 평균낸 값으로, 보통 자체 분석 도구(GA, Amplitude 등)의 DAU 통계로 확인합니다. 일회성 이벤트로 트래픽이 폭발한 달은 평균에 큰 영향을 주지만, 3 개월 평균이라는 점에서 이벤트 한 번으로 의무대상이 되지는 않습니다.

이행 기한을 놓치지 마세요

의무대상에 해당하는 해(예: 매출 100 억을 넘은 해)의 다음 해 8 월 31 일까지 인증을 받아야 합니다. 준비 기간이 평균 6 개월 이상 걸리는 점을 고려하면, 의무대상이 된 시점부터 즉시 준비를 시작해야 마감을 맞출 수 있습니다.

04. 인증을 받지 않으면 어떻게 되는가

정보통신망법 제 76 조는 ISMS 의무대상이 인증을 받지 않은 경우에 부과되는 과태료를 명시하고 있습니다. 2021 년 법 개정으로 상한이 1,000 만 원에서 3,000 만 원으로 세 배 인상되었으며, 이는 단순한 '권고'가 아닌 강한 강제 수단으로 자리잡았습니다.

위반 행위	과태료 상한	근거
ISMS 의무대상이 인증 미취득	3,000 만 원	정보통신망법 제 76 조
인증서 거짓 발급·표시	3,000 만 원	정보통신망법 제 76 조
사후심사 미이행	1,000 만 원	정보통신망법 시행령

물론 과태료 자체보다 더 무서운 것은 '평판 리스크'입니다. 매년 KISA 가 미인증 의무대상 명단을 공공데이터 형태로 공개하기 때문에, 이름이 한 번 오르면 회사 신뢰도에 직접적인 타격을 줍니다. 또한 보안 사고가 발생했을 때 'ISMS 인증조차 받지 않았다'는 사실은 손해배상 소송에서 회사에 매우 불리하게 작용합니다.

'과태료가 더 싸다'는 오해

일부 기업은 '인증 비용 1 억 원보다 과태료 3,000 만 원이 싸다'고 계산합니다. 하지만 과태료는 한 번이 아니라 미이행 상태가 지속되는 한 매년 부과될 수 있으며, 정보통신망법 외에도 공정거래법·하도급법·공공조달 평가에서 패널티가 누적됩니다. 수치만 보면 함정에 빠지기 쉽습니다.

05. 인증기관과 심사기관 한눈에 보기

ISMS 제도에는 '인증기관'과 '심사기관'이 따로 있습니다. 인증기관은 제도를 운영하고 최종 인증서를 발급하는 곳이며, 심사기관은 실제로 회사를 방문해 심사를 수행하는 곳입니다. 신청자는 둘 중 어느 곳에 신청해도 결과적으로 동일한 인증서를 받게 됩니다.

인증기관 (Certification Body)

기관	역할	전담 영역
KISA (한국인터넷진흥원)	제도 운영, 인증서 발급, 인증품질관리, 심사원 양성	일반 분야 전체
FSI (금융보안원)	금융분야 인증심사·인증서 발급	은행, 보험, 증권 등 금융기관

심사기관 (Audit Body)

기관	특 징
KAIT (한국정보통신진흥협회)	통신·일반 IT 분야 다수 심사 실적 보유
TTA (한국정보통신기술협회)	기술표준 기반의 심사, 공공·연구기관 강점
OPA (개인정보보호협회)	개인정보 분야 ISMS-P 심사에 강점

심사기관 선택은 '일정'과 '업종 적합성'을 기준으로 하는 것이 일반적입니다. 일정이 빠듯하다면 각 심사기관에 동시에 견적과 심사 가용 일정을 문의해 가장 빠른 곳을 택하고, 업종이 명확하다면 해당 분야에 강점이 있는 기관을 택하는 것이 안전합니다.

06. 인증기준 102 개 — 통제항목 이해하기

ISMS-P 인증기준은 다음 세 영역, 총 102 개의 통제항목으로 구성되어 있습니다. ISMS 만 받는 경우 세 번째 영역(개인정보 처리단계별 요구사항 22 개)을 제외한 80 개를 적용받습니다.

영역	분야 수	통제항목 수	세부 점검항목
1. 관리체계 수립 및 운영	4 개	16 개	약 42 개
2. 보호대책 요구사항	12 개	64 개	약 195 개
3. 개인정보 처리단계별 요구사항	5 개	22 개	약 80 개
합 계	21 개	102 개	약 317 개

6.1 관리체계 수립 및 운영 (16 개)

PDCA 사이클을 따르는 4 개 분야로 구성됩니다. 한 번 받고 끝나는 인증이 아니라 '지속적으로 운영되는 관리체계'임을 보여주는 영역으로, 가장 먼저 점검받게 됩니다.

분야	주요 통제항목
1.1 관리체계 기반 마련	경영진 참여, 최고책임자(CISO/CPO) 지정, 조직 구성, 범위 설정, 정책 수립, 자원 할당
1.2 위험관리	정보자산 식별, 현황 분석, 위험 평가, 보호대책 선정·이행계획 수립
1.3 관리체계 운영	보호대책 구현, 보호대책 공유, 운영 현황 관리
1.4 관리체계 점검 및 개선	법적 요구사항 준수 검토, 관리체계 점검, 관리체계 개선

6.2 보호대책 요구사항 (64 개)

관리적·물리적·기술적 보호대책을 12 개 분야에 걸쳐 정의합니다. ISMS 통제항목 중 가장 양이 많고, 실무 부담도 가장 큰 영역입니다.

분야	내 용
2.1 정책·조직·자산관리	정책·지침 수립, 조직 구성, 정보자산 분류·관리
2.2 인적보안	주요 직무자 관리, 비밀유지서약, 퇴직·직무변경 절차,

	보안교육
2.3 외부자 보안	외주 인력 관리, 외부 서비스 보안, 클라우드 위탁 보안
2.4 물리보안	물리적 보호구역 설정, 출입통제, 정보시스템 보호, 매체 통제
2.5 인증 및 권한 관리	사용자 계정·접근권한 관리, 비밀번호 정책, 특수 계정 관리
2.6 접근통제	네트워크 분리, 무선 보안, 원격접속, 응용프로그램 접근통제, DB 접근통제
2.7 암호화 적용	암호 정책, 키 관리, 전송·저장 시 암호화
2.8 정보시스템 도입 및 개발 보안	보안 요구사항 정의, 개발·시험·운영 분리, 시큐어 코딩, 시험 데이터 보안
2.9 시스템 및 서비스 운영관리	변경관리, 성능·용량 관리, 백업·복구, 로그·접속기록 관리, 시각 동기화, 정보자산 관리
2.10 시스템 및 서비스 보안관리	보안시스템 운영, 클라우드 보안, 패치관리, 악성코드 통제, 검색·수집 도구 보안
2.11 사고 예방 및 대응	사고 예방·대응 체계, 취약점 점검, 이상행위 분석, 사고 대응 훈련
2.12 재해복구	재해·재난 대비, 복구 전략, 복구 시험

6.3 개인정보 처리단계별 요구사항 (22 개)

ISMS-P 전용 영역으로, 개인정보의 '수집 → 보유·이용 → 제공 → 파기' 라이프사이클과 정보주체 권리보호를 다룹니다. 개인정보보호법의 핵심 의무가 거의 그대로 통제항목으로 매핑되어 있습니다.

분야	주요 통제 내용
3.1 개인정보 수집 시 보호조치	수집 동의, 최소 수집, 민감·고유식별정보 처리, 만 14 세 미만 아동 동의
3.2 개인정보 보유·이용 시 보호조치	이용·제공 목적 외 사용 금지, 가명·익명 처리, 자동화된 의사결정
3.3 개인정보 제공 시 보호조치	국내·국외 위탁·제공 동의, 영업양도 통지
3.4 개인정보 파기 시 보호조치	보유기간 만료 시 파기, 분리보관
3.5 정보주체 권리보호	열람·정정·삭제·처리정지권 보장, 개인정보 처리방침 공개, 분쟁조정

통제항목 102 개를 모두 외울 필요는 없습니다

실무에서 중요한 것은 '우리 회사 환경에서 어떤 통제가 누락되어 있는가'를 진단하는 능력입니다.

예비점검을 통해 결함이 예상되는 항목만 집중 점검하면 충분히 합격선에 도달할 수 있습니다.

07. 취득 절차 — 신청부터 인증서까지

ISMS 인증 취득은 크게 '신청 → 계약 → 심사 → 인증'의 4 단계로 진행됩니다. 단계별로 어떤 활동이 필요한지, 어떤 산출물이 오가는지 살펴봅니다.

STEP 1. 신청 단계

심사기관에 인증을 받겠다는 의사를 공식 표명하고 서류를 제출합니다.

- 신청 공문
- 인증신청서
- 관리체계 운영명세서 (102 개 통제항목별 운영 현황을 자세히 기술)
- 법인/개인 사업자 등록증

운영명세서는 신청 당시 시점의 '현실'을 솔직하게 기술해야 합니다. 부풀려서 작성하면 심사 단계에서 결함이 무더기로 쏟아지므로, 이미 운영 중인 항목과 향후 보완 예정 항목을 구분해 적는 것이 좋습니다.

STEP 2. 계약 단계

심사기관이 신청 내용을 검토한 후, 심사 범위와 일정을 협의해 수수료를 산정합니다. 견적이 확정되면 계약을 체결하고 수수료를 납부합니다. 이 단계에서 심사팀장이 배정되며 일정 조율이 시작됩니다.

STEP 3. 심사 단계

심사 단계는 '예비점검 → 본 심사 → 결함 보완'으로 세분화됩니다.

■ 예비점검 (본 심사 6~8 주 전)

심사팀장이 신청기관을 방문해 준비 현황을 점검합니다. 미리 결함을 파악해 보완할 수 있는 '리허설' 단계로, 합격률에 큰 영향을 미칩니다. 이 단계를 형식적으로 넘기면 본 심사에서 심각한 결함이 다수 도출될 수 있습니다.

■ 본 심사 (5~10 일)

심사팀이 회사를 방문해 '문서 심사 + 인터뷰 + 시스템 점검'을 병행합니다. ISMS 는 통상 5 일 내외, ISMS-P 는 7~10 일 정도 진행됩니다. 심사 기간 동안 담당자는 거의 풀타임으로 대응에 매달려야 하므로 일정 조정이 필수입니다.

■ 결함 보고 및 보완조치 (보통 30~40 일)

심사 종료 후 '결함보고서'가 전달되면 신청기관은 '보완조치내역서'를 작성해 제출합니다. 결함은 '중결함'과 '경결함'으로 구분되며, 중결함이 있는 경우 모두 해소되어야 인증이 가능합니다. 보완 기간은 통상 30~40 일이지만, 사안에 따라 연장될 수 있습니다.

STEP 4. 인증 단계

보완조치까지 완료되면 KISA(또는 FSI)의 인증위원회에서 인증 여부를 심의·의결합니다. 최종 의결되면 인증서가 발급되며, 유효기간은 발급일로부터 3 년입니다.

단계	주요 활동	산출물	소요 기간
① 신청	공문, 신청서, 운영명세서 제출	신청 접수증	1~2 주
② 계약	수수료 산정, 계약 체결	계약서, 수수료 납입	2~3 주
③ 예비점검	심사팀장 방문 사전 점검	사전 결함 리스트	1~2 주
④ 본 심사	문서·인터뷰·시스템 심사	심사보고서·결함보고서	5~10 일
⑤ 보완조치	결함 시정·증빙 제출	보완조치내역서	30~40 일
⑥ 인증의결	인증위원회 심의·의결	인증서 발급	2~4 주

08. 비용은 얼마나 드는가

'ISMS 받는 데 1 억 든다'는 말과 'ISMS 받는 데 700 만 원이면 된다'는 말이 모두 사실입니다. 전혀 다른 항목을 두고 이야기하기 때문입니다. ISMS 취득 비용은 다음 네 가지 카테고리로 나눠 봐야 정확합니다.

비용 항목	범위	전형적 금액
① 심사 수수료	심사기관에 직접 납부 (인건비+직접경비)	ISMS 800~1,400 만 원 / ISMS-P 1,000~1,800 만 원
② 컨설팅 비용	외부 컨설팅사를 통한 사전 준비·문서화·예비점검 지원	5,000 만 원 ~ 1 억 5,000 만 원
③ 시스템 구축 비용	DLP, DRM, 통합 로그관리, NAC, 백업 등 솔루션 도입	3,000 만 원 ~ 수억 원
④ 내부 인건비·간접비	담당자 투입, 교육비, 장비 부대비용	프로젝트당 2,000 만 원 이상

심사 수수료 산정 방식

심사 수수료는 '직접인건비 + 직접경비'로 산정합니다. 직접인건비는 심사에 투입되는 심사원 수, 심사 일수, 그리고「소프트웨어산업진흥법」제 22 조 제 4 항에 따른 SW 기술자 노임단가를 곱해 계산합니다. 직접경비는 교통비·숙박비·식대 등 실제 발생 경비입니다.

즉 '회사가 크고 시스템이 복잡할수록 심사원 수와 일수가 늘어나 수수료가 비싸진다'는 단순한 구조입니다. 매년 SW 노임단가가 인상되므로 수수료도 매년 소폭 상승하는 추세입니다.

컨설팅 비용은 왜 천차만별인가

컨설팅 비용이 가장 큰 변수입니다. 같은 회사라도 컨설팅사에 따라 견적이 두 배 이상 차이날 수 있습니다. 이유는 다음과 같습니다.

- 투입 컨설턴트 인원과 등급 (선임/책임/수석)

- 투입 기간 (단기 3 개월 vs 장기 6 개월)
- 산출물 범위 (기본 정책 문서 vs 시스템 설계서까지 포함)
- 위험평가·예비점검 포함 여부
- 컨설팅사의 인증 전담 인력 보유 여부

복수의 컨설팅사로부터 동일 기준의 RFP 로 견적을 받아 비교하는 것이 가장 안전합니다. 단순히 '싼 곳'보다 '유사 업종·유사 규모 인증 실적이 많은 곳'을 우선시하는 것이 좋습니다.

시스템 구축 비용을 줄이는 법

ISMS 통제항목을 만족시키려면 '로그관리 시스템', '접근통제 솔루션', '백업 인프라' 등 다양한 보안 시스템이 필요합니다. 신규 도입 시 수억 원이 들 수 있지만, 다음과 같은 방법으로 비용을 크게 줄일 수 있습니다.

- AWS·Azure·GCP 의 관리형 보안 서비스(GuardDuty, Security Hub, Defender) 활용
- 오픈소스 SIEM (Wazuh, Graylog, OpenSearch) 도입
- 이미 보유한 도구의 통합·고도화로 신규 도입 최소화
- KISA 의 '중소기업 정보보호 컨설팅 지원사업' 등 정부 지원사업 활용

정부 지원사업을 꼭 확인하세요

KISA 는 매년 'ISMS 인증 컨설팅 비용 지원사업' 등 다양한 지원사업을 운영합니다. 매출 800 억 원 미만 중소·중견기업의 경우 컨설팅 비용의 50~70%까지 지원받을 수 있는 경우가 있으므로, 준비 시작 전 KISA 홈페이지의 '기업지원' 메뉴를 반드시 확인하세요.

09. 기간은 얼마나 걸리는가 — 6 개월 로드맵

현장 경험상 ISMS 인증은 '준비 시작'부터 '인증서 수령'까지 평균 6~8 개월이 걸립니다. 단, 인증을 신청하려면 통제항목이 '최소 2 개월 이상 운영된 증적'이 있어야 한다는 점을 반드시 기억하세요. 즉, 신청 직전에 급하게 만든 정책 문서로는 인증을 받을 수 없습니다.

월차	주요 활동	마일스톤
M1	착수, 인증범위 확정, 컨설팅사 선정	범위 확정서, 킥오프
M2	현황 분석, 위험평가, Gap 분석	위험평가 보고서
M3	정책·지침 수립, 보호대책 이행계획	정책서 v1.0
M4	통제항목 구현, 시스템 도입·설정	보호대책 운영 시작
M5	운영 증적 누적, 예비점검, 문서 보완	예비점검 보고서
M6	인증 신청, 본 심사	심사 보고서
M7	결함 보완, 보완조치 제출	보완조치내역서
M8	인증위원회 의결, 인증서 발급	인증서 ✦

'2 개월 운영 증적'이란

ISMS 인증은 '서류상 준비됨'이 아닌 '실제로 운영되고 있음'을 증명하는 인증입니다. 따라서 정책을 수립한 직후에 신청하면 곧바로 거절됩니다. 다음과 같은 운영 증적이 최소 2 개월 이상 쌓여 있어야 합니다.

- 정보보호 위원회 회의록 (월 1 회 이상)
- 보안 교육 이수 기록
- 주기적 취약점 점검 결과
- 주요 시스템 로그 (접근, 변경, 백업)
- 외부 인력·외주사 보안 점검 기록

'2 개월'은 최소치이고, 결함률을 낮추려면 '3~4 개월 이상 운영 증적'을 권장합니다. 일정이 촉박하다면 운영 증적 누적 기간을 무리하게 줄이기보다, 인증 신청 시점을 한 분기 뒤로 조정하는 편이 결과적으로 더 빠릅니다.

10. 간편인증제 — 중소기업 부담 완화

2024 년 7 월 24 일부터 'ISMS·ISMS-P 간편인증제'가 시행되어 중소기업의 인증 부담이 크게 줄었습니다. 통제항목 수와 수수료가 모두 절반 가까이 인하되어, 의무대상은 아니지만 자율 인증을 검토하던 스타트업·중소기업에게 특히 유리한 제도입니다.

간편인증 적용 대상

- 정보통신서비스 부문 매출액 300 억 원 미만의 중소기업
- 정보통신서비스 부문 매출 300 억 원 이상이지만, 회사 내 주요 정보통신설비를 보유하지 않은 중기업 (웹호스팅·클라우드 이용)

간편인증의 혜택

항목	일반 인증	간편 인증
통제항목 수 (중소기업)	80 개	40 개
통제항목 수 (중기업·설비 미보유)	80 개	44 개
ISMS 심사 수수료	800~1,400 만 원	400~700 만 원
ISMS-P 심사 수수료	1,000~1,800 만 원	600~1,100 만 원
인증서 명칭	ISMS / ISMS-P	동일 (간편인증으로 별도 표기 없음)

간편인증으로 받아도 발급되는 인증서는 일반 인증과 동일합니다. 즉 고객·파트너 입장에서 보면 'ISMS 인증을 받았다'는 사실만 보이고, 간편인증 여부는 표시되지 않습니다. 의무대상이 아닌 기업이라면 간편인증부터 시작해 인증 운영 노하우를 쌓고, 회사가 성장하면서 일반 인증으로 확장하는 전략이 효율적입니다.

간편인증, 정말 '간편'한가

통제항목이 절반으로 줄었지만, 핵심 영역(접근통제·암호화·로그관리·사고대응)은 그대로 유지됩니다. '간편'이라는 이름에 비해 실제 준비 강도는 일반 인증의 60~70% 수준이라는 평가가 많습니다. '쉬운 인증'이 아니라 '부담을 줄인 인증'으로 이해하는 것이 정확합니다.

11. 사후관리 — 사후심사와 갱신심사

ISMS 인증은 '한 번 받으면 끝'이 아닙니다. 인증서 유효기간 3 년 동안 매년 사후심사를 받아야 하고, 3 년 차에는 갱신심사를 받아 인증을 연장해야 합니다. 사후심사를 빼먹으면 인증이 효력을 상실하므로 일정 관리가 매우 중요합니다.

연차	심사 종류	주요 점검 사항	수수료 수준
1 년 차	최초심사	전 통제항목 102 개	100% (기준)
2 년 차	사후심사	운영 적정성, 변경사항, 결함 후속조치	약 50~70%
3 년 차	사후심사	운영 적정성, 변경사항, 결함 후속조치	약 50~70%
4 년 차	갱신심사	전 통제항목 재심사 (최초심사 수준)	약 80~100%

사후심사 vs 갱신심사

사후심사는 '인증 받은 체계가 잘 운영되고 있는가'를 확인하는 약식 심사입니다. 본 심사 대비 기간이 짧고 점검 깊이도 얕습니다. 반면 갱신심사는 사실상 최초심사와 동일한 수준으로 진행되며, 인증서를 새로 발급받는다고 봐도 무방합니다.

갱신심사는 인증 유효기간 만료 3 개월 전까지 신청해야 합니다. 신청을 놓치면 '인증 효력 상실 → 재신청'의 절차를 밟아야 하므로, 만료 6 개월 전부터 일정을 챙기는 것이 좋습니다.

12. 자주 발생하는 결함 사례 TOP 10

KISA 의 연도별 결함현황 자료와 컨설팅 현장의 경험을 종합해, 가장 자주 도출되는 결함 10 가지를 선정했습니다. 인증 준비 시 우선적으로 점검해야 할 '단골 결함'입니다.

▸ TOP 1. 사용자 패스워드 정책 미준수

복잡도·변경주기·재사용 제한 정책이 있어도, 실제 시스템에 강제 적용되지 않은 경우가 흔합니다. 특히 레거시 시스템이나 외주사 운영 시스템에서 자주 결함이 도출됩니다.

▸ TOP 2. 계정·권한 관리 미흡

퇴직자·직무변경자의 계정이 즉시 회수되지 않거나, 특수 계정(관리자·시스템·공용)이 통제 없이 사용되는 경우. 정기 권한 검토 기록이 없는 것도 단골 결함입니다.

▸ TOP 3. 로그 관리 부실

중요 서버의 접속·변경 로그가 안전하게 백업되지 않거나, 보관 기간이 법정 기준(개인정보처리시스템 최소 1 년)을 충족하지 않는 경우. 로그가 위·변조 가능한 상태로 방치된 경우도 결함입니다.

▸ TOP 4. 정보자산 식별 미흡

정보자산 목록은 있지만 실제 운영 자산과 일치하지 않거나, 중요도 등급이 부여되지 않은 경우. 신규 도입한 클라우드·SaaS 자산이 누락되는 사례가 가장 많습니다.

▸ TOP 5. 위원회 구성 부적절

정보보호 및 개인정보보호 위원회가 실무자급으로만 구성되어 '의사결정권'이 없는 경우. 임원·경영진이 반드시 포함되어야 하며 회의록도 정기적으로 작성되어야 합니다.

▸ TOP 6. 외부자(외주·클라우드) 보안 미흡

외주 인력에게 접근권한을 광범위하게 부여하거나, 클라우드 위탁 시 위탁 계약서에 보안 요구사항이 반영되지 않은 경우. 클라우드 보안 책임 분담 모델(공동책임)에 대한 이해 부족이 원인입니다.

▸ TOP 7. 암호화 적용 부분 누락

DB·파일 저장 시 암호화는 적용했지만, 백업·이동매체·로그 영역의 개인정보가 평문으로 저장된 경우. 암호 키 관리 절차가 없는 것도 자주 보입니다.

▸ TOP 8. 취약점 점검·패치 미흡

정기 취약점 점검은 했으나 발견된 취약점에 대한 조치 이력·재점검 기록이 없는 경우. 보안 패치 정책은 있지만 실제로는 미적용 상태로 방치된 시스템이 다수 발견됩니다.

▸ TOP 9. 개인정보 수집 동의 형식 미흡

수집 항목·이용 목적·보유 기간이 한 화면에 묶여 있어 정보주체가 '선택적 동의'를 행사할 수 없는 경우. 만 14 세 미만 아동의 법정대리인 동의 절차가 누락된 사례도 흔합니다.

▸ TOP 10. 재해복구 훈련 미실시

재해복구 계획서는 있지만 실제 훈련을 해본 적이 없거나, 훈련 결과가 보호대책에 반영되지 않은 경우. '서류상의 BCP'가 가장 자주 지적됩니다.

결함을 줄이는 가장 좋은 방법

결함은 대부분 '정책은 있는데 운영이 따라가지 않는' 상태에서 발생합니다. 거창한 정책서 분량보다 '이 정책이 매주 누구에 의해 어떻게 점검되는가'의 운영 절차를 명확히 정의하는 것이 결함을 줄이는 핵심입니다.

13. 인증 준비 체크리스트

본 심사 전 반드시 확인해야 할 항목을 영역별로 정리했습니다. 각 항목 옆에 ✅ 표시를 하며 점검해 보세요.

[조직과 거버넌스]

- ☐ 최고경영자가 정보보호 의지를 공식 문서로 표명했는가
- ☐ CISO·CPO 를 임원급으로 지정하고 신고를 완료했는가
- ☐ 정보보호 위원회에 임원이 포함되어 있고 정기적으로 개최되는가
- ☐ 정보보호 조직의 인력·예산이 확보되어 있는가

[범위와 자산]

- ☐ 인증 범위(서비스·조직·시스템·물리적 위치)가 명확히 정의되어 있는가
- ☐ 정보자산 목록이 최신 상태이며 중요도 등급이 부여되어 있는가
- ☐ 신규 도입한 클라우드·SaaS 자산이 모두 포함되어 있는가

[정책과 지침]

- ☐ 정보보호 정책서·지침서가 위원회 승인을 거쳐 시행되고 있는가
- ☐ 정책·지침이 최소 2 개월 이상 운영된 증적이 있는가
- ☐ 법령(정보통신망법·개인정보보호법) 변경이 정책에 반영되어 있는가

[기술적 보호]

- ☐ 관리자 계정에 다중 인증(MFA)이 적용되어 있는가
- ☐ 퇴직자·직무변경자의 계정이 즉시 회수되는 절차가 작동하는가
- ☐ 개인정보 저장·전송·백업 시 암호화가 모두 적용되어 있는가
- ☐ 주요 시스템의 로그가 위변조 불가 상태로 1 년 이상 보관되는가

- ☐ 정기 취약점 점검과 후속 조치 기록이 갖춰져 있는가

[외부자 관리]

- ☐ 외주 인력의 접근권한이 최소화·정기 검토되고 있는가
- ☐ 클라우드 위탁사와 보안 요구사항이 계약서에 반영되어 있는가
- ☐ 위탁사 보안 점검·평가 기록이 누적되어 있는가

[개인정보 (ISMS-P)]

- ☐ 수집 동의 화면이 항목별 선택 동의가 가능하도록 되어 있는가
- ☐ 민감정보·고유식별정보의 별도 동의가 분리되어 있는가
- ☐ 보유기간 만료 시 자동 파기 또는 분리보관이 작동하는가
- ☐ 정보주체의 열람·정정·삭제 요청 처리 기록이 보관되는가
- ☐ 개인정보 처리방침이 홈페이지 첫 화면에서 한 번에 접근되는가

[사고 대응과 BCP]

- ☐ 보안사고 대응 매뉴얼과 비상연락망이 최신 상태인가
- ☐ 최근 1 년 이내 사고 대응 모의훈련을 실시하고 결과를 기록했는가
- ☐ 재해복구 훈련을 실제로 수행하고 RTO·RPO 를 측정했는가

14. 자주 묻는 질문 (FAQ)

Q1. ISO 27001 을 이미 받았는데 ISMS 도 받아야 하나요?

네, 받아야 합니다. ISO 27001 은 국제 인증이고 ISMS 는 국내 법정 인증입니다. ISO 27001 을 보유하면 심사 시 일부 통제항목 증적으로 활용할 수는 있지만 ISMS 를 대체하지는 못합니다. 다만 ISO 27001 의 운영 노하우가 ISMS 준비 기간을 크게 단축시켜 줍니다.

Q2. 스타트업도 받아야 하나요?

법적 의무대상이 아니라면 '반드시'는 아닙니다. 다만 B2B SaaS·핀테크·이커머스 분야의 스타트업은 고객사(특히 대기업·금융기관)가 'ISMS 인증'을 도입 전 필수 요구사항으로 요구하는 경우가 많아, 사실상 영업을 위해 자율 취득하는 경우가 늘고 있습니다. 간편인증제를 활용하면 비용 부담을 절반 가까이 줄일 수 있습니다.

Q3. 인증 범위는 회사 전체로 잡아야 하나요?

아닙니다. 특정 서비스·특정 조직·특정 시스템 단위로 범위를 좁힐 수 있습니다. 다만 의무대상자는 법에서 요구하는 서비스 전체를 범위에 포함해야 하며, 임의로 범위를 축소해 회피할 수 없습니다. 범위가 좁을수록 비용·기간이 줄어들기 때문에, 의무대상이 아닌 경우 핵심 서비스부터 시작해 확장하는 전략을 권장합니다.

Q4. 컨설팅 없이 자체적으로 받을 수 있나요?

이론적으로는 가능합니다. 그러나 102 개 통제항목과 약 317 개 세부 점검항목을 자체적으로 매핑하고 결함 없이 운영 증적을 쌓는 것은 정보보호 전담 인력 3 명 이상이 6 개월 이상 풀타임으로 매달려야 겨우 가능합니다. 인증 1 회 비용 대비 인건비를 계산하면 컨설팅이 더 저렴한 경우가 많습니다.

Q5. 심사 중에 결함이 너무 많이 나오면 어떻게 되나요?

'중결함'이 다수 도출되면 보완조치 기간이 연장되거나 인증위원회에서 '부적합' 판정을 받을 수 있습니다. 부적합 판정 시 처음부터 다시 심사를 받아야 하므로 비용·시간이 두 배로 듭니다. 예비점검 단계에서 결함을 가능한 한 많이 잡아내는 것이 가장 안전한 방법입니다.

Q6. 인증서가 발급되면 무엇을 해야 하나요?

발급된 인증서는 회사 홈페이지·제안서·계약서에 게시해 공개적으로 활용할 수 있습니다. 다만 인증 받은 '범위' 내에서만 사용해야 하며, 범위 외 서비스에 인증을 적용한 것처럼 표시하면 '인증서 거짓 표시'로 과태료 부과 대상이 될 수 있습니다.

Q7. 인증을 받았는데 회사가 합병/분할되면?

인증서는 법인격에 종속됩니다. 합병·분할로 법인격이 바뀌면 '인증 승계 신고'를 KISA 에 해야 하며, 사업 범위가 크게 변경된 경우 '재심사'가 필요할 수 있습니다. M&A 를 검토 중인 회사라면 인증 유지 비용을 사전에 점검하세요.

Q8. ISMS 인증 심사원 자격증은 무엇인가요?

ISMS-P 인증심사원은 KISA 가 주관하는 자격증으로, 정보보호 분야 6 년 이상의 경력자 중 양성과정·필기·실기를 통과한 사람에게 부여됩니다. 인증을 받는 회사 입장에서는 직접 관련은 없지만, 내부에 인증심사원 자격을 가진 직원이 있으면 사후심사 대응이 훨씬 수월해집니다.

15. 참고자료 및 공식 사이트

공식 사이트

기관/사이트	주소	용도
KISA ISMS-P 누리집	isms.kisa.or.kr	제도 안내, 신청서 양식, 자료실
개인정보 포털	privacy.go.kr	ISMS-P 인증기준, 개인정보보호법 해설
KAIT 정보보호 인증	isms.kait.or.kr	한국정보통신진흥협회 심사기관
TTA 정보보호 인증	tta.or.kr	한국정보통신기술협회 심사기관
OPA 정보보호 인증	opa.or.kr	개인정보보호협회 심사기관
FSI 금융보안원	fsec.or.kr	금융분야 ISMS-P 인증기관
국가법령정보센터	law.go.kr	정보통신망법·개인정보보호법 원문

주요 법령·고시

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 47 조
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제 49 조
- 개인정보보호법 제 32 조의 2
- 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시

(과학기술정보통신부·개인정보보호위원회)

- 정보보호 및 개인정보보호 관리체계 인증기준 (KISA)

추천 KISA 자료

- ISMS-P 인증기준 안내서 (최신본)
- ISMS-P 결함 사례집 (연도별)
- ISMS·ISMS-P 간편인증제 안내서

- ISMS-P 세부 점검항목 (공공데이터포털)
- 기업을 위한 개인정보보호 가이드라인

맺음말

이 백서는 'ISMS, 도대체 뭘 어떻게 해야 하는 거야?'라는 막막함을 풀어주기 위해 만들었습니다. 물론 이 한 권으로 모든 준비가 끝나지는 않습니다. 102 개의 통제항목 하나하나에는 또 다른 디테일이 숨어 있고, 회사마다 처한 환경이 다르기 때문입니다.

다만 한 가지는 분명합니다. '제대로 된 ISMS 운영'이 자리잡으면 단순히 인증서 한 장이 아니라 회사의 보안 수준·사고 대응 능력·고객 신뢰가 함께 따라옵니다. 인증은 결과물이고, 더 큰 가치는 그 과정 자체에 있습니다. 이 백서가 그 길의 첫 번째 지도가 되기를 바랍니다.

— 백 지 석 —

본 백서는 무료 배포용입니다.
내용 중 오류·보완 의견은 jiseok.paik@gmail.com 으로 보내 주시면 다음 판에 반영하겠습니다.