

정보보호 및 개인정보보호 관리체계 인증제 실효성 강화방안

2026. 4.

과기정통부 · 개인정보위

I. 추진 배경

1 제도개요 및 현황

- ISMS·ISMS-P 인증은 국제표준(ISO27001:27701) 기반으로, 개인정보 보유 및 정보통신서비스 기업의 보안수준 향상과 사고예방 등 목적으로 운영 중

「“ISMS-P 본격시행 1년, 정보보호 강화 효과 확인”(전자신문 보도, '20.05.07)」

- 관리체계 구축 효과 : 직원 정보보호 인식 개선(27%), 경영진의 이해도 향상(22%) 등
- 인증 취득 효과 : 사내 정보보호 수준 강화(31%), 고객 신뢰도 확보(23%) 등

- ISMS·ISMS-P 인증의 긍정적 효과에도 불구하고 통신사·이커머스 해킹 등 인증기업의 연이은 사고로 인해 제도의 실효성 지적 심화

※ 최근 3년간 ISMS·ISMS-P 인증기업 중 179개社(약 14%)에서 침해사고 발생

- “인증받은 SKT도 뚫렸다”...한계 드러낸 ISMS (25.07.14, 이데일리)
- “ISMS는 건강검진일 뿐”... 해킹 못 막은 보안인증, 韓 보안 불감증(25.06.09, 이투데이)
- “쿠팡 정보 유출 사고로 대두한 ‘ISMS-P 인증 무용론’(25.12.01, 세계일보)

- ISMS·ISMS-P 제도가 실질적으로 작동할 수 있도록 인증체계 전반에 대한 개선, 인증 관리·감독 강화 필요성에 대한 국민의 공감대 형성

※ 중요사업자 보안기준 강화 및 ISMS-P의무화를 위한 법률 개정안, 국회 본회의 통과

- 디지털 환경변화(DX·AX), 사이버위협 고도화 상황을 고려, 인증기업의 사고예방·보안역량 강화를 위한 제도개선 필요성 대두

- AI 기반, 초연결 인프라 등 새로운 기술환경에서 기존의 인증심사 방식으로 보안수준 담보 불확실, 인증체계의 구조적 개편 필요
- 서면 위주·스냅샷 방식의 평가 등 기존 심사방식의 한계를 벗어나 실효적 사고예방 수단이 되도록 실제 운영을 추적·개선하는 체계로 전환 필요

〈 ISMS·ISMS-P 인증제 개요 〉

□ 개요

- 주요 정보자산 유출 및 피해 예방을 위해 기업이 스스로 수립·운영 중인 정보보호 및 개인정보보호 관리체계*가 적합한지를 인증하는 제도

* (관련근거) 정보통신망법 제47조, 개인정보보호법 제32조의2

□ 주요 내용

- (인증의무 부과) 침해사고 발생 시 이용자 피해가 심각할 것으로 예상되는 기업의 정보시스템·정보통신서비스에 대해 ISMS 인증의무를 부과
 - ※ ISMS-P 인증제는 그간 자율취득 방식으로 운영 중이나, 현재 의무화를 위한 법개정 완료

〈 정보보호 관리체계(ISMS) 인증 의무대상(’26.2월 기준, 593개社) 〉

- 전국에 인터넷망·무선망 등을 제공하는 정보통신망서비스 제공자(ISP)
- 기간통신사업자로부터 이동통신서비스를 제공받아 재판매하는 전기통신사업자(MMNO)
- 정보통신서비스 제공자에게 서버·시설 등을 임대하는 데이터센터(IDC)
- 세입·매출 1,500억원 이상인 재학생 수 1만명 이상의 대학 및 상급종합병원
- 정보통신서비스 연 매출액 100억원 또는 일일평균 이용자수 100만명 이상의 자

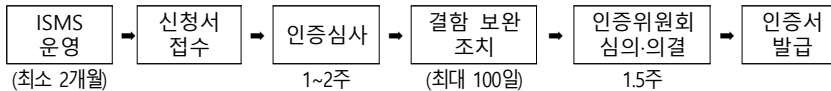
※ ISMS 인증 의무대상자가 인증을 받지 않은 경우 3,000만원의 과태료 부과

- (인증기준) 총 101개

※ ISMS 인증기준 80개 : 관리체계 수립·운영 16개, 보호대책 요구사항 64개
ISMS-P 인증기준 101개 : ISMS인증기준 80개 + 개인정보보호 요구사항 21개

- (인증·심사기관) 인증기관 2곳(한국인터넷진흥원, 금융보안원), 심사기관 5곳
(정보통신기술협회, 정보통신진흥협회, 개인정보보호협회, 차세대정보보안인증원, 한국경영인증원)

- (인증절차) 서면 및 현장심사의 방법으로 인증심사를 실시하고, 인증위원회의 심의·의결을 거쳐 인증서 부여(약 3~4개월 소요)



- (인증 유효기간) 3년 (최초인증 후 매년 사후심사 진행)
- (인증현황) 1,257건 ('26.2월말 기준, ISMS 942개, ISMS-P 315개)

2 문제점

① 대상 및 기준

- 개인정보 관리가 중요하나 그간 ISMS-P 인증은 재량이었으며, 기업의 중요도와 무관하게 인증기준을 획일적으로 적용

- ▶ (ISMS-P 자율) ISMS-P 취득이 자율에 맡겨져 있어, 대규모 개인 정보 처리 등 핵심 인프라에 대한 관리체계의 공백 발생
- ▶ (획일화된 인증기준) 동일한 인증기준으로 심사가 진행되어, 국민 생활과 직결되는 산업군에 대한 강화된 보안관리 미흡

② 심사 방식

- 한정된 인력 및 서면 위주 심사방식으로 실제 취약점 발견 미흡

- ▶ (샘플링 점검) 기업이 자체 수행한 증적·취약점에 대한 신뢰를 바탕으로 심사함에 따라 실질적인 보안취약 여부 검증 불가

③ 사후 관리

- 사고기업에 대한 사후관리 및 인증기업에 대한 지속적 관리가 부족한 상황이며, 제도 시행이래 인증 취소사례도 전무한 실정

- ▶ (관리미비) 사고기업도 일반기업과 차이가 없는 사후관리 적용 중이며, 인증기업 전반에 대한 상시 점검체계도 미흡
- ▶ (인증취소) 기업의 인증 지속 유지 및 일정 수준 이상의 보안체계 확보에 방점을 둔 제도 운영으로, 인증취소 사례 없음

④ 품질 확보

- 심사기관의 부실심사 방지 및 심사품질 확보를 위한 관리수단이 미흡하며, 인증심사원의 전문역량 개발 역시 부족한 상황

- ▶ (심사기관·심사원) 심사기관의 부실심사에 대한 제재수단 및 심사원의 신기술 발전에 부합한 점검 대응능력 부족

개선 방향

심사방식·사후관리 등 인증체계 전반에 대한 **구조적인 개편**을 통해 **인증체계의 실효성 강화** 및 정부인증제의 신뢰 제고

II. 추진 과제

1 인증 의무대상 확대 및 기준 강화

◆ 국민 파급력이 큰 대규모 개인정보처리자 등에 개인정보보호 인증 의무를 부여하고, 통신사·데이터센터 등 고위험군의 인증기준 강화

현 행 (As-Is)	개 선 (To-Be)
<ul style="list-style-type: none"> ▶ ISMS-P 인증은 자율적 취득 ▶ 기업규모 구분없이 인증기준 일원화 적용 	<ul style="list-style-type: none"> ▶ 공공민간 대규모 개인정보처리자 ISMS-P 의무화 ▶ 인증 3단계 구분하고, 인증기준 차등 적용

○ **(ISMS-P 의무화)** 개인정보의 특성·규모, 매출액 등 고려하여 공공·민간 중요 개인정보처리시스템* ISMS-P 인증 의무화 추진

* (대상안) ▲ 주요 공공시스템운영기관, ▲ 이동통신사업자, ▲ 본인확인기관, ▲ 매출액 및 처리하는 개인정보 수를 고려한 대규모 개인정보처리자

- 기존 자율적으로 운영되던 ISMS-P를 의무화*하여 주요 시스템의 상시적 개인정보 안전관리체계 구축 * 의무화 시 과징금 감경 제외

○ **(인증 차등화 적용)** 인증을 3단계로 구분하고, 국민생활 파급력이 큰 강화인증*은 기존 대비 인증기준 및 심사방식 차등 적용

* (대상안) ▲ 매출액 1조이상 주요ISP·IDC, ▲ 매출액 3조이상 정보통신서비스제공자 등

〈 인증 등급체계(안) 〉

구분	설명	인증기준
(신화) 강화인증(Advanced)	고 보안위험 대비 보안 수준 강화	20개(안) ※ 표준인증기준에 강화인증기준 추가
표준인증(Standard)	보안 기본 원칙 중심	ISMS 80개, ISMS-P 101개
간편인증(Lite)	인증 부담 완화	ISMS 44개, ISMS-P 65개

○ **(강화 인증기준)** 주요 보안위험 사례, 주요국 보안 요구 사항을 참조하여 보안을 강화한 인증기준 개발 후 강화인증군에 적용

구분	기존	[추가] 강화인증군			
		인증기준	세부점검항목	강화 인증기준(안)	세부점검 항목(안)
ISMS	관리체계 수립·운영	16	42	20	76
	보호대책 요구사항	64	195		
ISMS-P	개인정보보호 요구사항	21	91	-	-
합계		101	237	20	76

- 개발된 강화 인증기준을 사업자들에게 先 배포·적용 안내하고, 관련 고시 등 규정에 반영하여 의무 적용

〈 강화 인증기준 (예시) 〉

관련 인증기준	특화 보안요구사항(안)
최고책임자의 지정	조직 전체의 정보보호 및 개인정보보호 업무를 조정·구현할 정보보호 최고책임자, 개인정보 보호책임자를 최고경영자(CEO) 직속의 임원으로 임명하고, 실질적 보안 통제 권한을 부여
정보자산 식별 강화	자동화 도구를 활용하여 정보자산, 시스템 구성요소 목록을 관리하고, 비인가 구성요소를 탐지
무결성 검증	소프트웨어, 펌웨어 등의 비인가 변경을 탐지하기 위한 무결성 검증 도구를 운영
자동화된 계정 관리	정보시스템 계정의 생성·수정·비활성화·삭제 등 생명주기 전반을 자동화된 메커니즘으로 관리하고, 계정 상태 변경을 실시간 반영
사용자 인증 강화	중요 정보시스템 및 정보에 대한 접근 시 강화된 인증수단을 의무 적용하고, 위험 수준·접근 상황에 따른 적용형 인증을 수행
인증정보 관리	액세스 토큰, API키 등 인증정보의 전체 생명주기를 체계적으로 관리
네트워크 접근 강화	외부 네트워크의 연결 접점을 최소화 하고 외부에 노출된 기능, 서비스와 중요 네트워크망 사이에는 물리적 또는 논리적으로 분리, 분리가 불가능할 경우 중요 정보를 암호화 하는 등의 보호대책을 적용

○ **(인증기준서 개선)** 최근 주요 침해사고 원인 분석 및 기술변화를 반영하여, 기존 인증기준 안내서의 미비사항을 검토 및 보완

※ 무선 네트워크 보안강화, 주요정보 난독화, CISO-CPO 권한 강화 등

○ **(인증범위 확대)** 인증대상 서비스와 관련된 장비, 시설 등은 누락없이 모두 포함하고, 특히 외부 인터넷과 연결되는 점점 자산*은 인증범위 내 반드시 포함되도록 인증범위를 단계적으로 확대

* 인터넷과 연결되어 공격 경로로 활용될 가능성이 있는 디지털 자산

○ **(위험평가 재정의)** 기업 보안체계의 전반적인 수준을 높일 수 있도록 '위험평가(인증항목)*'의 기준이 되는 '위험수용 가이드라인'을 마련·배포

* 서비스 및 자산의 위험을 식별하고, 조직 특성에 맞게 보호대책 위험수용 기준을 자체 수립

2 인증심사 방식 강화

◆ 기존 서면 증적 확인 위주의 심사방식 내 미비점 등 보완을 위해 **심사팀 구성, 심사체계·점검방식을 개편하여 현장실증 점검 강화**

현 행 (As-Is)	개 선 (To-Be)
▶ 기업제출 자료에 대한 신뢰를 기반한 서면 증적 확인 위주의 인증심사	▶ 보안취약점 직접 점검, 시스템 접속 시연 등 현장실증형 심사체계 구축

○ **(심사팀 개편)** 심사투입 인력 및 기간 확대 등 심사팀 구성 체계 개편

- 표준인증군은 인증심사원을 추가 투입해 현장실증을 강화하고, 강화인증군은 취약점점검원을 투입해 기술심사를 정밀하게 실시

* (현재) ISMS-P 인증심사원 → (향후) ISMS-P 인증심사원 + 취약점점검원(전문기업)
 ※ **취약점점검원을 전담 투입하여 점검자산수를 대폭 확대(기존10대 → 최대 500대)**하고, 중요도(개인정보 처리, 인터넷접점, 중요서비스 등)가 높은 정보자산 우선 점검

〈 심사방식 강화 위한 심사팀 개편(안) (예시) 〉

구분	기존인증	심사방식 강화	
		표준인증	강화인증·사고기업 등 대상
ISMS	5명, 5일(팀장1,심사원4)	6명, 5일(팀장1, 심사원5)	10명, 10일(팀장1, 심사원4, 취약점점검원5)
ISMS-P	5명, 7일(팀장1,심사원4)	6명, 7일(팀장1, 심사원5)	10명, 12일(팀장1, 심사원4, 취약점점검원5)

○ **(인증심사 절차 강화)** 보안사고와 직결하는 중요 핵심항목-기술심사 先 검증 → 後 본심사를 통해 미흡한 기업 부실인증 사전 차단

구분	기존	개선(안)
인증신청	· 관리체계 운영명세서	· 관리체계 운영명세서 + 인증범위 자산-위험평가 현황 추가
예비심사	· 심사팀장 1인 방문(1일)	· ① 핵심항목 先 검증 ② 기술심사* 방식 적용(취약점진단, 모의침투 등) * 강화인증, 사고기업 등 핵심항목 미충족 → 본심사 불가 → (최초인증) 신청 반려, (사후심사) 미보완시 인증효력 취소
본심사	· 서면위주, 샘플링 점검(5일)	· 서면점검 + ⑤ 현장실증형 심사방법 추가
이행심사	· 심사팀장 1인 방문(1일)	· 심사팀장 1인 + 심사결과 미흡 수준에 따라 인력 추가 투입

※ 인증심사 절차 강화에 따른 기술료 조정(기술심사-ISMS-P 10%→20%), 투입 인력·기간 증가분, 심사원 보수 현실화(SW평균임금) 반영하여 인증수수료 상승 예정

〈인증심사 절차 강화 세부 방안〉

- (핵심항목 先검증)** 본 심사 前 예비심사 단계를 강화하여, 핵심적으로 확인해야 할 인증기준을 사전에 점검하고 본심사 진행여부 결정
 - 최근 유출사고 주요 원인 분석 및 관련 인증항목을 도출하여 서버 내 보안패치 적용 등 핵심항목* 심사 엄격화
 - * 핵심항목(안) : ① CISO-CPO의 정보보호 정책 관리 권한 여부, ② 개인정보 처리·외부 인터넷 접점 자산 식별 ③ 개인정보 처리시스템 비밀번호암호화 적용, ④ 취약점·패치관리 등
- (기술 심사)** 취약점 점검 전문인력이 점검도구(취약점 스캐너, 스크립트, 소스코드 진단툴 등)를 활용하여 취약점진단 및 모의침투 수행

〈 기술심사(취약점 점검) 수행 절차(안) 〉

정보자산 식별	점검범위 설정	취약점 점검	취약점 결과 검토
인증범위 내 모든 정보자산을 목록화	중요정보, 가용성 등을 고려한 범위 설정	①CVE, ②CCE, ③소스코드 점검, ④모의침투테스트	발굴된 취약점에 대해 종합적으로 검토 실시

〈 취약점 점검별 점검 항목(안) 〉

구분	① CVE	② CCE	③ 소스코드 점검	④ 모의침투
점검내용	자산식별, 취약점 스캔	정보시스템 보안설정(계정, 권한, 패스워드 등)	소스코드 개발유형 등 SW 보안약점 진단	시나리오기반(내외부 공격) 침투테스트, 방어체계 검증
점검항목	CVE, 보호나라(KrCERT), 국가사이버안보센터 등	기반시설 취약점분석평가, CIS 벤치마크 등	CWE, 소프트웨어 보안약점 진단가이드(KISA)	Mitre att&ck 프레임워크 등

③ **(현장실증 심사)** 심사원이 실질적 보안관리 상태를 확인할 수 있도록 실시간 시연 확인 등 현장실증 심사방법 적용

- 침해사고·개인정보 유출 원인, 최신 보안위협 등 심사기준에 반영

〈 인증심사 기준별 현장실증 방법(안) 〉

인증 기준	수행 내용	상세 절차
1.2.1 정보자산 식별	숨겨진 정보자산 식별	①인증범위 자산 확정 → ②자산관리시스템 실시 (필요 시 점검도구를 활용한 네트워크 스캔)
2.2.5 퇴직 및 직무변경 관리	계정, 권한 회수 등 즉시성 검증	①주요 계정, 권한 현황 점검 → ②테스트 계정 생성 → ③퇴직, 직무변경 상황 부여 → ④절차 검증
2.11.3 이상행위 분석 및 모니터링	대용량 유출, 관리자 접속 등 이상행위 모니터링 현황	①이상행위 기준 점검 → ②이상행위 상황 부여 → ③서버, 보안시스템 등 로그 실사
2.11.5 사고 대응 및 복구	백업데이터 무결성 검증, 실제 데이터 복구	①백업대상, 방법 등 점검 → ②테스트 파일 생성 및 백업 → ③테스트 파일 암호화 → ④복구 시연

3 인증 사후관리 강화

◆ 인증 사후에도 보안관리 유지될 수 있도록 상시 점검을 강화하고, 중대한 침해사고 기업 등에 대한 인증 엄격 관리

현 행 (As-Is)	개 선 (To-Be)
<ul style="list-style-type: none"> ▶ 특정 시점만 확인 하는 스냅샷 방식 ▶ 인증을 받았음에도 사고가 지속 발생하고, 인증을 취소한 사례가 없음 	<ul style="list-style-type: none"> ▶ 상시 자체점검 의무화로 지속적 보안관리 ▶ 사고발생 기업 사후관리 강화 ▶ 인증취소 등 인증서 엄격 관리

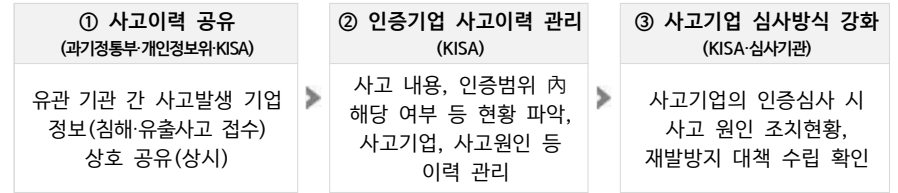
- **(상시 점검체계 확립)** 인증의 취득부터 유지·갱신에 이르는 전 과정에서 관리체계가 현장에서 연간 적정하게 운영되고 있는지를 중점 점검
 - 보안관리의 지속적인 유지 여부를 확인할 수 있도록 주기별 점검 양식을 표준화하고, 사후심사 시 이를 집중 점검
 - ※ CISO-CPO지정, 취약점 점검, 로그-접속 기록 등 핵심항목은 인증 사후에도 지속적 이행-관리하도록 점검양식 표준화-배포(KISA), 인증취득 당시 일시적 보안관리 방지
- **(중대사고 심사중단)** 중대한 침해사고 발생 시 정부의 조사·처분 종료 전까지 인증 심사심의를 잠정 중단
 - 인증기업이 사고복구 및 조치, 재발방지 대책 수립 등에 집중하도록 인증심사를 중단 (유효기간을 조건부로 일시 연장)
 - 정부조사·처분 종료 후 심사를 재개하고, 사고 조치 결과 등을 종합적으로 고려하여 인증 유지 여부를 최종 결정
- **(사고기업 관리강화)** 사고기업은 인증심사 시 심사인력·기간 투입을 확대(2배), 사고원인·조치현황 등을 집중심사하여 재발방지 강화

〈 기업 중요도별 사후심사 차등화 관리(예시) 〉

구분	기존인증	개선 표준인증	신설 사고기업 인증심사
심사방식	기본 방식	기본 방식 현장실증	현장실증-기술심사(취약점점검, 모의해킹) 사고 주요원인 집중심사(재발방지 완료시 까지)
제출서류	신청서, 운영명세서,	신청서, 운영명세서, 자산-위험평가 현황	신청서, 운영명세서, 자산-위험평가 현황, 사고 조치 현황
투입인력	5명, 5일	6명, 5일	10명, 10일(심각도에 따라 유연 조정)

- **(사고이력 관리)** 침해사고가 접수된 인증기업의 현황을 KISA에서 관리하고, 인증심사 강화대상에 편입하여 보다 엄격한 심사를 추진

〈 인증기업 사고이력 관리체계(안) 〉

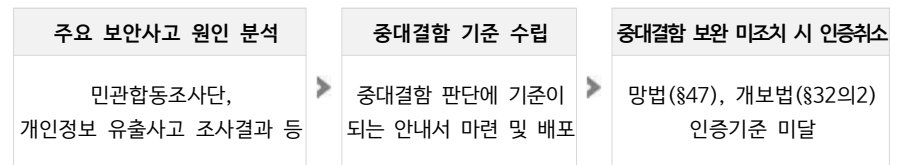


- **(인증취소)** 법령에 규정된 인증취소 사유를 구체화하고, 관련 법령에 따라 취소 절차 추진

〈 인증취소 검토 대상(안) 〉

관련 법령	인증취소 검토대상 예시
사후관리 거부·방해	사후관리* 미이행 * 사후관리 포기 의사 제출, 사후심사 미신청, 예비인증-본인증 미실시 등
	신청자료* 미제출·거부 * 운영명세서, 자산현황, 위험평가 결과 등
인증기준 미달	중대결함* 보완 미조치 * EoS, 보안패치 미적용, 로그 미보관 등
중대한 법령 위반	정보통신망법, 개인정보보호법 등에 따라 위반행위가 매우 중대한 경우

- 보안사고 원인(정부 조사결과 등), 인증기업 점검 결과 등을 토대로 인증기준 미달 판단을 위해 중대결함 기준 마련(인증기준서 명시)



※ 중대결함은 경영진의 승인에 따른 위험수용(1.2. 위험관리) 불가, 보완조치 기한 (100일) 이내 미조치 시 인증위원회에 안건으로 상정하여 인증취소 심의 추진

4 심사기관 · 심사원 전문성 강화

◆ **심사품질 제고를 위해 심사기관의 관리책임과 사후점검을 강화하고, 심사원의 전문성 향상을 위한 교육 · 관리 집중**

현 행 (As-Is)	개 선 (To-Be)
▶ 심사기관의 부실심사 등에 대한 평가기준 부재, 심사원들의 역량 부족 지적	▶ 심사기관 관리 감독을 강화하고, 심사원 역량제고 교육 강화

- **(심사품질 개선)** 심사기관의 심사품질 관리책임을 강화하여, 심사기관 스스로 심사역량 및 전문성을 관리하는 체계로 전환
 - (신뢰도 조사) 인증심사 종료 후 심사기관에 대한 신뢰도* 조사를 실시하고, 그 결과를 차년도 인증심사 배분량**에 반영
 - * 과도한 수수료를 부과하거나, 역량 없는 심사원 배정 시 신뢰도에 영향
 - ** 신뢰도 낮은 심사기관의 심사 배분량을 축소하고, 이해 상충 발생(회원사 등) 및 장기 반복 심사(유착방지) 배제하도록 심사 배분 시 검토(KISA)
- **(심사전문성 강화)** AI · 클라우드 등 전문분야별 특화 심사가 가능하도록 소속심사원을 확충 또는 전문심사원 모집을 통해 전문성 확보
 - ※ 심사팀 전문성(전문자격, 유관경력 등) 및 구성원칙(투입인력·기간) 기준 수립(KISA)
- **(심사기관 감독강화)** 부실심사 등 심사품질 하락 방지 위한 심사기관 재지정 요건, 지정 사후점검(매1년) 강화
 - (평가기준) 심사품질 관련 항목(예: 심사인력 임의축소 등)을 지정(또는 재지정(매 3년)) 평가에 반영하여 심사품질 제고 유도
 - (심사품질관리 점검) 심사기관의 심사역량관리(교육, 전문심사원 활용), 심사팀구성 원칙 준수 여부를 사후관리 점검(매1년) 통해 철저히 확인
 - (심사기관 사후점검) 매1년 심사기관 사후관리 점검에서 지정 기준 미달 확인 시 업무정지(3~6개월), 업무정지 3회 시 지정취소

< 인증·심사기관 업무수행 능력 심사 기준(고시 별표2) 개선(안) >

개선항목	현재	향후
개선 전담 인력	심사품질 관리부재	심사품질 및 기술심사(취약점점검) 관리 전담인력 보유 시 가점 부여
개선 전문성	심사팀장 전문성 부족	클라우드, AI 등 신기술 전문성 강화 노력(교육, 자격증 등) 가점 추가
신설 사고 관리	인증 사후 사고발생 시 관리책임 부재	인증심사 사후 사고 발생 시 관리 절차 수립 및 이행 관련 평가항목·배점 신설
신설 심사 품질	심사역량, 심사팀관리의 심사기관 책임 부재	심사역량, 심사팀구성 공정성·공평성 확보 ※ 이해상충 및 역량미흡 제거, 신규심사원 일정비율 배정 등
개선 감점	심사품질 부실관리 적극 제재 미이행	심사인력·기간 임의 축소, 사고기업 사후관리 미이행, 심사팀구성 원칙 위반 등

- **(심사원 역량강화)** 취약점 등 기술심사 검증 능력 제고를 위한 실무 교육을 강화하고, 심사원별 전문분야 정보를 관리하여 심사에 활용

심사원 전문분야 관리	심사원 교육 강화
· 클라우드, AI, 개인정보 등 심사원 전문분야 정보 관리, 해당분야 우선 배정권 부여	· 현장실증 심사방법(경비·서버별 취약점 점검, 운영 체제별 보안설정 확인) 등 심사원 교육 강화 · 심사기술 공유 등을 위한 심사팀장 워크숍 등 개최
심사참여 요건 개선	심사원 양성 업무협력
· 심사 참여자(연4회↑) 대상 심사 참여 · 자격시험 합격자 및 장기 미참여자는 참관(2회) ※ 형식적인 자격갱신 요건(보수교육) 폐지하되, 심사 참여 심사원 대상 교육 집중	· ICT 자격검정 전문기관 업무협력 · 역량 있는 심사원 발굴 기회 확대 ※ 자격수요는 증가하는 반면, 예산 부족으로 인한 심사원자격 응시 인원 제한 해결

- **(심사원 처우개선)** 우수 인력 이탈 방지 및 심사원 추가 확보를 위해 심사기관·심사원 인건비 현실화
 - ※ SW기술사 평균임금 공표에 따른 정보보안전문가 평균임금 연동
- **(기술심사 가이드)** 인증심사 주안점, 최신 보안위협 상황에 맞는 기술심사 방법 등 심사가이드를 제공하여 현장실증형 심사 수행능력을 제고하고 가이드에 따른 심사의 일관성 확보*
 - * 기업에서는 심사원 경력 차이에 따른 심사품질 편차 발생 지적

심사기관	인증기관(KISA)	심사팀(심사팀장, 심사원)
· 심사 시 발생하였던 주요 사례 정리 및 인증기관(KISA) 제출	· 취합된 주요 사례, 최신기술 반영한 심사방법 개발, 가이드 배포	· 가이드라인 근거, 일관성 있는 인증심사 수행

Ⅲ. 추진 일정

추진과제	시행일정	개정사항
1) 인증 의무대상 확대 및 기준 강화		
① ISMS-P 의무화	'27년. 하~	개보법 시행령 고시
② 인증 차등화 적용	'27년~	방법 시행령 고시
③ 강화 인증기준	'27년~	고시 가이드라인
④ 인증기준서 개선	'26년. 하~	가이드라인
⑤ 인증범위 확대	'27년~	고시
⑥ 위험평가 재정비	'27년~	가이드라인
2) 인증심사 방식 강화		
① 심사팀 개편	'27년~	개보법 시행령 방법 시행령 고시
② 인증심사 절차 강화	'27년~	개보법 시행령 방법 시행령 고시
3) 인증 사후관리 강화		
① 상시 점검체계 확립	'26년. 하~	가이드라인
② 중대사고 심사중단	'26년. 하~	고시
③ 사고기업 관리강화	'27년~	가이드라인
④ 사고이력 관리	'26년. 하~	가이드라인
⑤ 인증취소	'26년. 하~	가이드라인
4) 심사기관·심사원 전문성 강화		
① 심사품질 개선	'27년~	고시
② 심사전문성 강화	'27년~	고시
③ 심사기관 감독강화	'27년~	고시
④ 심사원 역량강화	'27년~	고시
⑤ 심사원 처우개선	'27년~	가이드라인
⑥ 기술심사 가이드	'27년~	가이드라인