

개인정보 보호법 시행령

<목 차>

1. 개인정보 보호 인증심사 방법

소관부처 및 작성자 인적사항	소관부처	개인정보보호위원회	작 성 자	이름	최화평
	담당부서 (과)	자율보호정책과		직급	행정주사
	국장	고낙준		연락처	02-2100-3048
	과장	황지은		이메일	chpjjan@mail.g o.kr

2026. 09. 09. 작성

정 책 책 임 자 직 위 : 국 장 성 명 : 고낙준 (서 명)

< 규제 개요 >

기본 정보	1.규제사무명	개인정보 보호 인증심사 방법		
	2.규제조문	개인정보 보호법 시행령 제34조의 2 제34조의 5		
	3.위임법령	개인정보 보호법 제32조의 2		
	4.유형	강화	5.입법예고	2026.09.16~2026.10.26
규제의 필요성	6.추진배경 및 정부개입 필요성	○ 추진배경 - 정보보호 및 개인정보보호 관리체계 인증(ISMS-P 인증)은 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 개인정보 보호법에 부합하는지 등에 관하여 인증하는 제도로써, 보안수준 향상 등의 목적으로 운영 중 - ISMS-P 인증의 긍정적 효과에도 불구하고 인증을 취득한 기업의 연이은 개인정보 유출사고로, 인증심사원에 의한 서면 위주의 인증심사 방식에 대한 제도적 한계가 지적됨에 따라 기술적 현장 검증 강화 필요성 대두 ○ 정부개입 필요성 - 국민 생활 파급력이 큰 대규모 기업 및 침해·유출사고 발생 기업에 대해 일정 이상의 기술자격을 보유한 자가 취약점 점검을 수행할 수 있도록 하여 현장심사를 강화할 필요 - 아울러, 인증 취득 이후 실시하는 사후관리 심사 시에도 동일한 방법과 기준이 적용되도록 할 필요		
	7.규제내용	○ 서면심사와 현장심사를 병행할 수 있도록 규정을 정비하고, 대규모 기업 및 사고 기업 등에 대해서는 전문 기술인력이 취약점 점검을 수행할 수 있는 근거 마련		
	8.피규제집단 및 이해관계자	○(피규제집단) 정보통신망법상 강화인증 적용 대상 사업자, 인증의 유효기간 내 침해사고 발생 또는 유출등을 신고한 자 ○(이해관계자) 인증심사를 수행하는 인증심사원, 심사수행기관, 인증결과를 심의·의결하는 인증위원회 위		
	9.규제목표	○ 강화인증 대상, 침해사고 발생 기업 및 개인정보 유출등을 신고한 자에 대한 전문 기술인력의 현장 검증을 통하여 형식적 인증을 방지하고 실질적인 개인정보 보호 수준 향상 도모		
규제의 적정성	10.영향평가 여부	기술영향평가	경쟁영향평가	중기영향평가
		해당없음	해당없음	해당있음

	11.비용편익 분석 (정성분석)	o 법 제32조의2에 따른 인증의 방법·절차 등을 구체화한 것으로, 서면심사와 현장심사를 병행할 수 있도록 규정을 정비하여 의미를 명확히 하였으며 사회적으로 파급력이 큰 대규모 기업, 침해·유출사고 발생 기업에 대한 인증심사 시, 기존 인증심사원 외 전문 기술인력이 취약점 점검을 실시할 수 있도록 기술인력의 요건을 명확히 규정한 것으로 일부 수수료 상승을 제외하고 추가 발생하는 비용은 없을 것으로 판단됨. 전문 기술인력을 활용한 인증심사의 전문성 제고를 통해 인증에 대한 신뢰성·실효성을 강화하여 국민의 안전한 개인정보 보호 환경 조성에 기여하는 편익 발생		
기타	12.규제일몰제	대분류	소분류	
		일몰설정에외기준	1. 국제조약 등에 따라 동일하게 적용 되어야 하는 규제	미해당
			2. 국가의 질서 유지 및 국민생명·안전과 직접 관련된 규제	미해당
			3. 사회통념상 보편적으로 통용되는 규범적 성격의 규제	미해당
		경제규제 여부기준	4. 국민과 기업의 경제활동에 대한 규제	미해당
			5. 경제활동에 직접영향을 주는 규제	미해당
		일몰설정 세부기준	6. 피규제자의 규제부담이 매우 큰 규제	미해당
			7. 한시적 목적을 위한 규제이거나 주기적인 검토가 필요한 규제	미해당
		일몰설정여부	일몰조문	연장여부
		일몰유형	일몰설정기간	일몰주기
	13. 우선허용·사후 규제 적용여부	해당 없음		

〈조문 대비표〉

현 행	개 정 안
제34조의2(개인정보 보호 인증의 기준·방법·절차 등) ④ 법 제32조의2제1항에 따른 개인정보 보호 인증심사는 제34조의8에 따른 개인정보 보호 인증심사원이 <u>서면심사 또는 현장심사의 방법으로</u> 실시한다. <u>〈단서 신설〉</u>	제34조의2(개인정보 보호 인증의 기준·방법·절차 등) ④ ----- ----- ----- ----- ----- <u>서면심사와 현장심사의 방법을 병행하여</u> <u>---. 다만, 다음 각 호의 어느 하나에 해당하는 자에 대하여 현장심사를 실시하는 경우 「정보보호산업의 진흥에 관한 법률 시행규칙」 별표 1에 따른 중급 이상의 자격기준을 갖춘 기술인력이 취약점 점검을 수행할 수 있다.</u>
<u>〈신 설〉</u>	1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제49조의2제3항 각 호의 어느 하나에 해당하는 자로서 법 제32조의2제1항에 따른 인증을 받으려는 자
<u>〈신 설〉</u>	2. 법 제32조의2에 따른 인증을 받은 자로서 인증의 유효기간 내 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제7호에 따른 침해사고가 발생한 자
<u>〈신 설〉</u>	3. 법 제32조의2에 따른 인증을 받

현 행	개 정 안
제34조의5(인증의 사후관리) ① 법 제32조의2제4항에 따른 사후관리 심사는 <u>서면심사 또는 현장심사의 방법으로</u> 실시한다. <후단 신설>	<u>은 자로서 인증의 유효기간 내 법 제34조에 따른 유출등을 신고한 자</u> 제34조의5(인증의 사후관리) ① ----- ----- <u>서면심사와 현장심사의 방법을 병행하여</u> ----- ----- <u>이 경우 제34조의2제4항 단서 및 각 호는 사후관리 심사에 준용된다.</u>

I. 규제의 필요성 및 대안선택

1. 추진배경 및 정부개입 필요성

○ 추진 배경

- 정보보호 및 개인정보보호 관리체계 인증(ISMS-P 인증)은 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 개인정보 보호법에 부합하는지 등에 관하여 인증하는 제도로서, 보안 수준 향상 등의 목적으로 운영 중
- ISMS-P 인증의 긍정적 효과에도 불구하고, 인증을 취득한 기업의 연이은 개인정보 유출사고로 서면 위주의 인증심사 방식에 대한 제도적 한계가 지적됨에 따라 기술적 현장 검증 강화 필요성 대두

○ 정부개입 필요성

- 서면심사와 현장심사를 병행할 수 있도록 규정을 정비하여 의미를 명확히 하고, 국민 생활 파급력이 큰 대규모 기업 및 침해·유출 사고 발생 기업에 대해 일정 이상의 기술자격을 보유한 자가 취약점 점검을 수행할 수 있도록 하여 현장심사를 강화할 필요
- 아울러, 인증 취득 이후 실시하는 사후관리 심사 시에도 동일한 방법과 기준이 적용되도록 하여 제도 정합성을 높이고 안전한 보호 환경 조성

2. 규제 대안 검토 및 선택

① 대안의 내용 및 선택 근거

○ 대안의 내용

규제대안1	대안명	국민 생활 파급력이 큰 대규모 기업 등에 한정하여 취약점 점검 수행
	내용	사회적으로 파급력이 큰 대규모 기업, 침해·유출 사고 발생 기업에 대한 인증심사 시, 기존 인증심사원 외 전문 기술인력이 취약점 점검 수행
규제대안2	대안명	취약점 점검 미수행(일반 서면·현장점검 수행)
	내용	현행과 같이 인증심사원만이 서면·현장심사를 수

		행하며 취약점 점검원 참여는 인정하지 않음
--	--	-------------------------

o 규제대안의 비교

구분	장점	단점
규제대안1	실제 시스템 기술 취약점 발굴 가능, 인증 신뢰성 제고, 침해사고 예방 효과 기대	현장심사 시 취약점 점검원 추가 투입으로 피규제자의 시간 부담 일부 증가
규제대안2	피규제자 부담 현행 유지	서면·일반 현장심사만으로는 기술적 취약점 검증에 한계, 침해사고 재발 방지 효과 미흡

- 서면심사와 현장심사를 병행할 수 있도록 규정을 정비하고, 국민 생활에 큰 영향을 미치는 대규모 기업, 침해·유출사고 발생 기업에 대해서는 기존 인증심사원 외 전문 기술인력이 취약점 점검을 수행할 수 있는 근거 마련

o 선택 근거

- 현행 인증제도에서 인증심사원 증원을 통해 심사 강도를 높이는 방안도 가능할 수 있으나, 이는 기존 관리체계 점검(서면심사) 방식의 연장에 불과하여 정보시스템에 대한 기술적 취약점을 직접 확인하는 것과는 본질적으로 다름
- 전문 기술인력(취약점 점검원)은 다수의 서버·네트워크 장비·애플리케이션을 직접 스캐닝·분석하는 전문가로서, 동일한 심사 기간 내에 인증심사원만으로는 검토하기 어려운 많은 수량의 정보시스템에 대한 실사가 가능함. 즉, 취약점 점검원의 투입을 통해 실질적으로 점검할 수 있는 시스템 대상이 크게 확대 가능함
- 관리체계 전반을 검토하는 인증심사원은 ISMS-P 인증의 근간으로서 여전히 핵심적 역할을 담당함. 다만, 사이버 보안위협이 고도화·지능화 됨에 따라 AI 공격, 시스템 취약점 악용 등 기술적 실사가 요구되는 위협이 급증하고 있어, 대규모 정보시스템 보유 사업자에 대한 심사에서는 기술적 점검 전문인력의 참여 없이 인증의 실효성을 담보하기 어려운 상황임
- 심사원 증원이라는 기존 방식으로는 달성하기 어려운 기술적 취

약점 실사의 범위 확대와 심사 실효성 제고를 위하여, 대규모 기업 등 일정 대상자에 한하여 취약점 점검원을 현장심사에 투입하는 것이 합리적일 것으로 판단됨

② 이해관계자 의견수렴

이해관계자명	일시 · 장소 · 방법	제시의견	조치결과
	○ 입법예고 예정 (‘26.9.16.~’26.10.26.)		

3. 규제목표

사회적 파급력이 큰 대규모 기업, 침해·유출사고 기업에 대하여 취약점 점검원이 직접 현장심사에 참여하는 기술적 검증 절차를 제도화함으로써 형식적 인증을 방지하고 실질적인 개인 정보보호 수준을 향상시킴

II. 규제의 적정성

1. 목적·수단 간 비례적 타당성

- 이 규제의 목적은 인증심사시 현장심사를 병행할 수 있는 근거를 마련하고, 국민 생활 파급력이 큰 대규모 사업자 및 침해·유출사고 발생 기업에 대한 인증심사 방식을 강화하여 인증의 실효성과 개인정보 보호 수준을 제고하기 위한 것임
- 현장점검은 ISMS-P 인증심사 대상자 모두에게 적용되나, 현재도 인증심사는 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제25조제1항에 따라 서면심사와 현장심사를 병행하고 있어 목적과 수단간 비례성을 확보함
- 전문인력에 의한 취약점 점검 적용 대상을 정보통신망법상 강화인증 대상자(정보통신망법 시행령 개정안 제49조의2제3항 각 호) 및 인증 유효기간 내 침해사고가 발생한 자, 유출등을 신고한 자로 한정하여 부담을 최소화하였음
- 취약점 점검원의 참여를 의무가 아닌 “수행할 수 있다”는 허용 형식으로 규정하되 현장심사의 일환으로 사실상 이행을 유도함으로써 비례원칙에 부합함

구분	피규제자
현장심사 병행	ISMS-P 인증심사 대상 기업(기관)
취약점 점검	ISMS-P 인증심사 대상 기업(기관) 중 사회적으로 파급력이 큰 대규모 기업, 침해·유출사고 발생 기업

- 기술적 검증 수단(취약점 점검원 참여)은 인증 실효성 확보라는 목적에 직결되는 최소한의 수단으로서 목적과 수단 간 비례성이 확보된 것으로 판단됨

2. 영향평가 필요성 등 고려사항

영향평가		
기술	경쟁	중기
해당없음	해당없음	해당있음

○ 영향평가 - 기술규제영향평가 해당없음 - 경쟁영향평가 해당없음

경쟁영향평가 점검항목	해당 여부
(A) 사업자의 수 또는 범위 제한	해당없음
(B) 사업자의 경쟁능력 제한	해당없음
(C) 사업자의 경쟁유인 감소	해당없음
(D) 소비자에게 제공되는 선택과 정보의 제한	해당없음

- 중기영향평가

해당있음

- 규제 차등화 예비분석 결과표

① 규제 영역		해당없음
② 규제 방식		해당없음
③ 예비분석모델		해당없음
	판단 근거	해당없음
④ 대상 업종		해당없음
⑤ 예비분석내용		해당없음
⑥ 차등화적용 여부		해당없음

○ 기타 고려사항

- 고용친화적 규제설계

해당없음

- 시장유인적 규제설계

해당없음

- 일몰설정 여부

해당없음

- 우선허용·사후규제 적용 여부

해당없음

분류	적용여부	적용내용/미적용사유
포괄적 개념 정의		서면심사와 현장심사를 병행할 수 있음을 명확히 하고, 취약점 점검원의 기준을 타법을 인용하여 정한 것으로 포괄적 개념 정의에 해당하지 않음
유연한 분류 체계		특정 대상에 인증심사방식 강화를 위한 취약점 점검원을 인증심사에 투입하는 것으로 유연한 분류체계에 해당하지 않음
네거티브 리스트		허용 대상을 한정하거나, 금지 대상을 열거하고 나머지는 허용하는 등의 네거티브 리스트에 해당하지 않음
사후 평가관리		신기술·신산업 관련 사규제샌드박스 적용대상이 아님전 심의·검사 또는 사후 평가·관리와 무관한 사안임
규제 샌드박스		규제샌드박스 적용대상이 아님

3. 해외 및 유사입법사례

○ 해외사례

① 미국 NIST 사이버보안 프레임워크(CSF) 2.0 및 NIST SP 800-53 Rev.5

- NIST CSF 2.0(2024.2.26. 발간)은 연방정부·주요기업을 대상으로, 사이버 보안 위협관리의 전 생애주기를 체계화한 국제 표준 프레임워크임
- 동 프레임워크의 위협평가(ID.RA) 및 탐지·모니터링(DE.CM) 범주는 자산 취약점의 기술적 식별·검증을 핵심 요소로 규정하며, 이를 구현하는 통제 기준인 NIST SP 800-53 Rev.5는 침투 테스트 (CA-8) 및 취약점 스캐닝(RA-5)을 독립 통제항목으로 의무화함
- NIST 체계는 관리체계(ISMS-P) 점검만으로는 달성할 수 없는 기술적 취약점의 식별·검증을 위해 자격 있는 독립 인력에 의한 기술적 실사를 별도 통제 항목으로 규정하고 있음. 이는 본 개정안의 취약점 점검원 투입과 직접 대응하는 선행 제도임

구분	원문 (영문)	한국어 번역
ID.RA-01 (위험 평가)	“Vulnerabilities in assets are identified, validated, and recorded.”	“자산의 취약점을 식별·검증·기록한다.” → 관리체계 서류 확인만으로는 불충분하며, 자산별 취약점을 기술적 방법으로 실제 확인·검증하도록 요구
ID.RA-05 (위험 평가)	“Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent and residual cybersecurity risk and inform risk response prioritization.”	“위협·취약점·발생가능성·영향을 활용하여 내재적·잔존 사이버보안 위험을 파악하고 위험 대응 우선순위를 결정한다.” → 기술적 취약점 데이터 없이는 실질적인 위험 우선순위 결정이 불가능함을 명시
DE.CM-09 (탐지·모니터링)	“Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.”	“컴퓨팅 하드웨어·소프트웨어·실행 환경 및 데이터를 모니터링하여 잠재적 이상 이벤트를 탐지한다.” → 시스템 단위의 실시간·직접 점검을 요구하며, 문서 검토 방식과 차별화

CA-8 (침투 테스트)	[SP 800-53 Rev.5] “Employ an independent penetration agent or penetration team to perform penetration testing on the system or system components at [organization-defined frequency].“	[SP 800-53 Rev.5] “독립적인 침투 테스트 담당자 또는 팀이 조직이 정한 주기에 따라 시스템 및 구성요소에 대한 침투 테스트를 수행하도록 한다.“ → 자격을 갖춘 독립 인력(취약점 점검원)의 기술적 실사를 명시적으로 규정
RA-5 (취약점 스캐닝)	[SP 800-53 Rev.5] “Monitor and scan for vulnerabilities in the system and hosted applications [at organization-defined frequency] and when new vulnerabilities potentially affecting the system are identified and reported.“	[SP 800-53 Rev.5] “조직이 정한 주기에 따라, 그리고 새로운 취약점이 식별·보고될 때 시스템 및 호스팅 애플리케이션의 취약점을 모니터링하고 스캔한다.“ → 정기적이고 전문적인 기술 점검을 의무화하여 관리체계 점검과의 이중 구조를 확립

② EU NIS2 지침 (2022/2555/EU)

- EU NIS2 지침(Directive 2022/2555/EU)은 유럽연합 역내 필수기업(Essential Entities) 및 중요기업(Important Entities)에 대해 사이버보안 위험 관리 조치를 의무화하는 구속력 있는 규범임
- 특히 제21조는 기업 스스로 사이버보안 위험 관리 조치의 실효성을 평가할 의무를 부과하고, 제32조는 소관 당국이 해당 기업에 현장 검사·원격 보안 스캔·기술적 감사를 실시할 수 있도록 권한을 부여함
- EU NIS2 지침은 기술적 취약점 점검(보안 스캔)·현장 검사·실효성 평가를 규범적 의무로 명시함으로써, 관리체계 서류 심사 방식과 구별되는 기술적 현장 실사의 제도화를 선도하고 있음
- 본 개정안이 취약점 점검원을 인증심사에 편입하는 방식은 EU NIS2의 기술 인력(trained professionals) 활용 원칙과 맥락을 같이하며, 선진 규범과 정합적인 입법 방향임

구분	원문 (영문)	한국어 번역
Art. 21(1) (위)	“Member States shall ensure that	“회원국은 필수기업 및 중요기업

구분	원문 (영문)	한국어 번역
위험 관리 조치 의무)	essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for the provision of their services or for the carrying out of their activities.“	이 서비스 제공 또는 활동 수행에 사용하는 네트워크 및 정보시스템의 보안에 대한 위험을 관리하기 위해 적절하고 비례적인 기술적·운영적·조직적 조치를 취하도록 보장하여야 한다.“ → 기술적 조치(technical measures)를 관리적 조치와 함께 명시적으로 요구
Art. 21(2)(e) (취약점 처리 및 공개)	“The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following: [...] (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;“	“제1항의 조치는 [...] 최소한 다음을 포함한다: [...] (e) 취약점 처리 및 공개를 포함하여 네트워크 및 정보시스템의 취득·개발·유지보수 시 보안 확보;“ → 취약점 처리(vulnerability handling)를 위험 관리 조치의 필수 구성요소로 법제화
Art. 21(2)(f) (사이버보안 조치 실효성 평가)	“The measures referred to in paragraph 1 shall [...] include at least the following: [...] (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;“	“제1항의 조치는 [...] 최소한 다음을 포함한다: [...] (f) 사이버보안 위험 관리 조치의 실효성을 평가하기 위한 정책 및 절차;“ → 단순 도입에 그치지 않고, 실효성 검증 절차를 제도적으로 내재화할 의무 부과
Art. 32(2)(a) (현장 검사 및 원격 감독)	“For the purposes of paragraph 1, competent authorities shall have the power at least to: (a) conduct on-site inspections and off-site supervision, including random checks carried out by trained professionals;“	“소관 당국은 최소한 다음의 권한을 보유한다: (a) 훈련된 전문가에 의한 불시점검을 포함하여 현장 검사 및 원격 감독을 실시하는 것;“ → 자격을 갖춘 전문인력(trained professionals)에 의한 현장 기술 검사를 당국 권한으로 명시

구분	원문 (영문)	한국어 번역
Art. 32(2)(d) (보안 스캔)	“(d) to carry out security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary in cooperation with the entity concerned;“	“(d) 객관적 · 비차별적 · 공정하고 투명한 위험 평가 기준에 따라 보안 스캔을 실시하고, 필요한 경우 해당 기업과 협력하여 수행하는 것;“ → 보안 스캔(security scan)을 감독 수단으로 법제화하여 문서 심사 외 기술적 실사 권한을 부여
Art. 32(4) (기술 감사 비용 부담)	“Where targeted security audits are ordered in accordance with paragraph 2, point (d), of this Article, the costs shall be borne by the entity, unless the competent authority decides otherwise in exceptional circumstances.“	“이 조 제2항 (d)에 따라 지정 보안 감사가 명령된 경우, 소관 당국이 예외적 사정에 따라 달리 결정하지 않는 한 그 비용은 해당 기업이 부담한다.“ → 기술적 보안 감사를 규범적 의무로 확립하고 비용 부담 원칙까지 명시함으로써 실효성 담보

③ 국제 금융 보안 표준 PCI DSS v4.0.1

- PCI DSS(Payment Card Industry Data Security Standard)는 카드사(Visa·Mastercard·AMEX 등)가 공동 설립한 PCI SSC가 관리하는 국제 금융 보안 표준으로, 카드 데이터를 처리·보유·전송하는 모든 사업자(대형 결제사·금융기관 포함)에게 적용됨
- 시스템 및 네트워크의 보안을 정기적으로 테스트·검증할 것을 의무화하며, 자격을 갖춘 인력(Qualified Personnel)에 의한 침투 테스트·취약점 스캐닝을 명문화하고 있음
- PCI DSS는 자격을 갖춘 인력에 의한 기술적 스캐닝과 침투 테스트를 정기 의무로 부과하며, 단순 문서·인터뷰 심사와 명확히 구분하고 있음. 이는 취약점 점검원이라는 자격 인력을 심사 절차에 제도적으로 편입하는 본 개정안의 방향과 동일한 국제적 흐름임

구분	원문 (영문)	한국어 번역
Req. 11.3.1 (내부 취약점)	“Internal vulnerability scans are performed as follows: - At least	“내부 취약점 스캔은 다음과 같이 수행한다: - 최소 3개월마다

스캔)	once every three months. - High-risk and critical vulnerabilities (per Requirement 6.3.1) are resolved. - Scans are performed by qualified personnel. - Rescans are performed that confirm all high-risk and critical vulnerabilities have been resolved.“	1회 이상. - 고위험 및 심각한 취약점(요구사항 6.3.1 기준)을 해소한다. - 스캔은 자격을 갖춘 인력이 수행한다. - 고위험 · 심각 취약점 해소 확인을 위한 재스캔을 실시한다.“ → 주기적 기술 스캔과 자격 인력 요건을 동시에 명시
Req. 11.4.1 (침투 테스트 방법론)	“A penetration testing methodology is defined, documented, and implemented by the entity, and includes: - Industry-accepted penetration testing approaches (e.g., NIST SP800-115). - Coverage for the entire CDE perimeter and critical systems. - Testing from both inside and outside the network. - Network-layer penetration tests that encompass all components that support network functions as well as operating systems.“	“침투 테스트 방법론을 정의 · 문서화 · 이행하며, 다음을 포함한다: - 업계에서 인정하는 침투 테스트 방식(예: NIST SP800-115). - 전체 카드 데이터 환경(CDE) 경계 및 중요 시스템 포함. - 네트워크 내부 · 외부 양방향 테스트. - 네트워크 기능 지원 구성요소 및 운영체제를 대상으로 하는 네트워크 계층 침투 테스트.“ → OS · 네트워크 장비 수준의 기술적 실사를 방법론으로 의무화
Req. 11.4.3 (외부 침투 테스트)	“External penetration testing is performed: - At least once every 12 months. - After any significant infrastructure or application upgrade or change. - By a qualified internal resource or qualified external third party. - Organizational independence of the tester exists.“	“외부 침투 테스트는 다음과 같이 수행한다: - 최소 12개월마다 1회 이상. - 중요 인프라 또는 애플리케이션 업그레이드 · 변경 이후. - 자격을 갖춘 내부 인력 또는 외부 전문 업체가 수행. - 테스터의 조직 독립성을 확보한다.“ → 독립적 기술 인력에 의한 정기 · 변경 후 필수 테스트 규정
Req. 11.4.4 (발견 취약점 조치)	“Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: - In accordance with the entity’s assessment of the risk posed by the security issue as defined in Requirement 6.3.1. - Penetration testing is repeated to verify the corrections.“	“침투 테스트에서 발견된 악용 가능 취약점 및 보안 약점을 다음과 같이 조치한다: - 요구사항 6.3.1에 따른 위험 평가 결과에 따라 조치. - 조치 완료 확인을 위한 재테스트를 수행한다.“ → 취약점 발견에서 조치 · 재확인까지 기술 인력의 연속 관여를 제도화

○ 타법사례

① 「정보통신기반 보호법」 제9조

- 주요정보통신기반시설 취약점 분석·평가 의무를 규정하고, 기술인력에 의한 취약점 점검을 실시하도록 하고 있음

「정보통신기반 보호법」 제9조
제9조(취약점의 분석·평가) ①관리기관의 장은 대통령령으로 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다. ② 중앙행정기관의 장은 다음 각 호의 어느 하나에 해당하는 경우 해당 관리기관의 장에게 주요정보통신기반시설의 취약점을 분석·평가하도록 명령할 수 있다. 1. 새로운 형태의 전자적 침해행위로부터 주요정보통신기반시설을 보호하기 위하여 필요한 경우 2. 주요정보통신기반시설에 중대한 변화가 발생하여 별도의 취약점 분석·평가가 필요한 경우 ③관리기관의 장은 제1항 또는 제2항에 따라 취약점을 분석·평가하고자 하는 경우에는 대통령령이 정하는 바에 따라 취약점을 분석·평가하는 전담반을 구성하여야 한다. ④관리기관의 장은 제1항 또는 제2항에 따라 취약점을 분석·평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있다. 다만, 이 경우 제3항에 따른 전담반을 구성하지 아니할 수 있다. 1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조의 규정에 의한 한국인터넷진흥원(이하 “인터넷진흥원”이라 한다) 2. 제16조의 규정에 의한 정보공유·분석센터(대통령령이 정하는 기준을 충족하는 정보공유·분석센터에 한한다) 3. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업 4. 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조의 규정에 의한 한국전자통신연구원 ⑤과학기술정보통신부장관은 관계중앙행정기관의 장 및 국가정보원장과 협의하여 제1항 및 제2항에 따른 취약점 분석·평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다. ⑥주요정보통신기반시설의 취약점 분석·평가의 방법 및 절차 등에 관하여 필요

한 사항은 대통령령으로 정한다.

② 「전자금융거래법」 제21조의3

- 금융 분야에서 정보보호 최고책임자 및 전문인력에 의한 취약점 점검을 내부적으로 의무화하고 있음

전자금융거래법 제21조의3
제21조의3(전자금융기반시설의 취약점 분석·평가) ① 금융회사 및 전자금융업자는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 전자금융기반시설에 대한 다음 각 호의 사항을 분석·평가하고 그 결과(「정보통신기반 보호법」 제9조에 따른 취약점 분석·평가를 한 경우에는 그 결과를 말한다)를 금융위원회에 보고하여야 한다.
1. 정보기술부문의 조직, 시설 및 내부통제에 관한 사항
2. 정보기술부문의 전자적 장치 및 접근매체에 관한 사항
3. 전자금융거래의 유지를 위한 침해사고 대응조치에 관한 사항
4. 그 밖에 대통령령으로 정하는 사항

4. 비용편익 분석

<규제대안 1 : 취약점 점검 미수행(일반 서면·현장점검 수행)>

① 비용편익분석 : 피규제 기업·소상공인 직접비용 0

분석기준년도	규제시행년도	분석대상기간 (년)	할인율(%)	단위
2026	2027	10	4.5	백만원, 현재가치

규제대안 1 : 취약점 점검 미수행(일반 서면·현장점검 수행)				
영향집단		비용	편익	순비용
피규제 기업 · 소상공인	직접			
	간접			
피규제 일반국민				
피규제자 이외 기업 · 소상공인				
피규제자 이외 일반 국민				
정부				
총 합계				

기업순비용		연간균등순비용	
-------	--	---------	--

III. 규제의 실효성

1. 규제의 순응도

○ 피규제자 준수 가능성

- 현재도 인증심사는 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제25조제1항에 따라 서면심사와 현장심사를 병행하고 있어, 신청인이 현장심사 병행에 대한 준수 가능성이 높을 것으로 예상됨
- 정보통신망법령상 강화인증 대상자는 매출액 1조원 이상 대기업으로 정보보호 조직·인력과 예산을 상당 규모로 보유하고 있어, 취약점 점검원이 참여하는 현장심사를 수용할 역량이 충분한 것으로 판단됨
- 침해사고 발생 및 유출등을 신고한 대상자의 경우 이미 사고 대응 과정에서 기술적 점검을 실시하는 경우가 많아 추가적인 제도 부담이 크지 않을 것으로 예상됨

구분	피규제자
현장심사 병행	ISMS-P 인증심사 대상 기업(기관)
취약점 점검	ISMS-P 인증심사 대상 기업(기관) 중 사회적으로 파급력이 큰 대규모 기업, 침해·유출사고 발생 기업

2. 규제의 집행가능성

○ 행정적 집행가능성

개인정보보호위원회 인력 및 업무 위탁기관인 한국인터넷진흥원 인력을 활용하여 행정적 집행 가능

○ 재정적 집행가능성

현장심사 병행에 대한 규정 정비, 전문 기술인력의 취약점 점검 등 인증의 방법·절차 등을 구체화하는 것으로 추가적인 예산을 투입할 필요 없음

IV. 추진계획 및 종합결론

1. 추진 경과

- 정보보호 및 개인정보보호 관리체계 인증제 실효성 강화를 위한 현장 간담회 개최('26.3.12.)
※ (주요내용) ISMS-P 인증제 실효성 강화방향 논의, 인증·심사 업무에 대한 현장의견·건의사항 청취 등
- 「정보보호 및 개인정보보호 관리체계 인증제 실효성 강화방안」 발표(경제관계장관회의, 과기정통부 합동. '26.4.10.)
※ (주요내용) 심사기관·심사원 전문성 강화, 현장·기술심사 방식 도입 등

2. 향후 평가계획

- 제도 운영 과정에서 간담회·설명회 등을 통해 제도 안내를 실시하고, 개선 필요시 적용 범위·방법 조정 등 개선 지속

3. 종합결론

- 본 개정안은 서면심사와 현장심사를 병행할 수 있음을 명확히 정비하여 규제의 불확실성을 해소함
- 아울러, 사회적 파급력이 큰 대규모 기업 및 침해사고 발생·유출등을 신고한 자에 한정하여 ISMS-P 인증심사에 기술 전문인력을 제도적으로 편입함으로서, 기존 관리체계 중심의 서면 위주 심사방식을 개선하여 기술적 취약점 실사를 결합한 이중 검증 체계로 전환하는 것임
- 이는 미국 NIST CSF 2.0, PCI DSS v4.0.1, EU NIS2 지침 등 주요 국제 규범이 공통적으로 요구하는 자격 인력에 의한 기술적 현장 검증 의무화와 정합하는 입법 방향으로, 국내 사이버보안 인증제도의 국제적 신뢰도 제고에 기여함

가. 대안별 분석 비교표

분석기준년도	규제시행년도	분석대상기간 (년)	할인율(%)	단위
2026	2027	10	4.5	백만원, 현재가치
규제대안1 : 취약점 점검 미수행(일반 서면·현장점검 수행)				
영향집단		비용	편익	순비용
피규제 기업 · 소상공인	직접			
	간접			
피규제 일반국민				
피규제자 이외 기업 · 소상공인				
피규제자 이외 일반 국민				
정부				
총 합계				
기업순비용			연간균등순비용	

정성분석 내용 및 기타 참고사항

○ 법 제32조의2에 따른 인증의 방법·절차 등을 구체화한 것으로, 서면심사와 현장심사를 병행할 수 있도록 규정을 정비하여 의미를 명확히 하였으며 사회적으로 파급력이 큰 대규모 기업, 침해·유출사고 발생 기업에 대한 인증심사 시, 기존 인증심사원 외 전문 기술인력이 취약점 점검을 실시할 수 있도록 기술인력의 요건을 명확히 규정한 것으로 일부 수수료 상승을 제외하고 추가 발생하는 비용은 없을 것으로 판단됨. 전문 기술인력을 활용한 인증심사의 전문성 제고를 통해 인증에 대한 신뢰성·실효성을 강화하여 국민의 안전한 개인정보 보호 환경 조성에 기여하는 편익 발생

나. 각 대안의 활동별 비용·편익 분석 결과

<규제대안1 : 취약점 점검 미수행(일반 서면·현장점검 수행)>

①피규제 기업소상공인 :

□간접비용

(정성)영향집단명	정보통신망법령상 강화인증 대상자(정보통신망법 시행령 개정안 제49조의2제3항 각 호), 인증 유효기간 내 침해사고가 발생한 자, 인증 유효기간 내 유출등을 신고한 자
활동제목	전문 기술인력 도입을 통한 현장심사 전문성 강화
비용항목	해당없음
일시적/반복적	반복적
근거설명	○ 법 제32조의2에 따른 인증의 방법·절차 등을 구체화한 것으로, 서면심사와 현장심사를 병행할 수 있도록 규정을 정비하여 의미를 명확히 하였으며 사회적으로 파급력이 큰 대규모 기업, 침해·유출사고 발생 기업에 대한 인증심사 시, 기존 인증심사원 외 전문 기술인력이 취약점 점검을 실시할 수 있도록 기술인력의 요건을 명확히 규정한 것으로 일부 수수료 상승을 제외하고 추가 발생하는 비용은 없을 것으로 판단됨

②피규제 일반국민 :

□편익

(정성)영향집단명	정보주체인 일반국민
활동제목	전문 기술인력 도입을 통한 현장심사 전문성 강화
편익항목	인증제 실효성 강화를 통한 개인정보 보호
일시적/반복적	반복적
근거설명	○ 전문 기술인력을 활용한 인증심사의 전문성 제고를 통해 인증에 대한 신뢰성·실효성을 강화하여 국민의 안전한 개인정보 보호 환경 조성에 기여하는 편익 발생