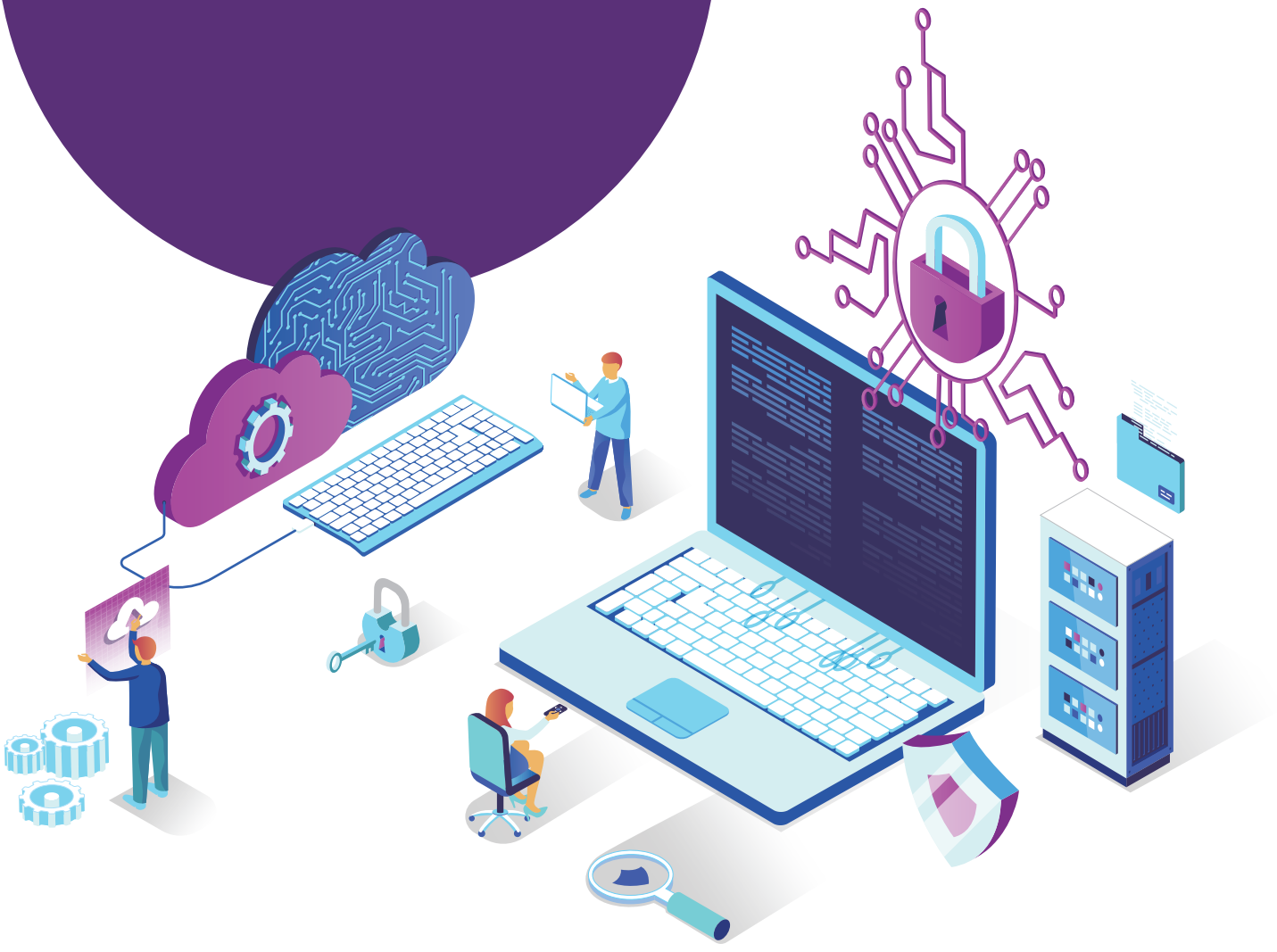
2024. 7.

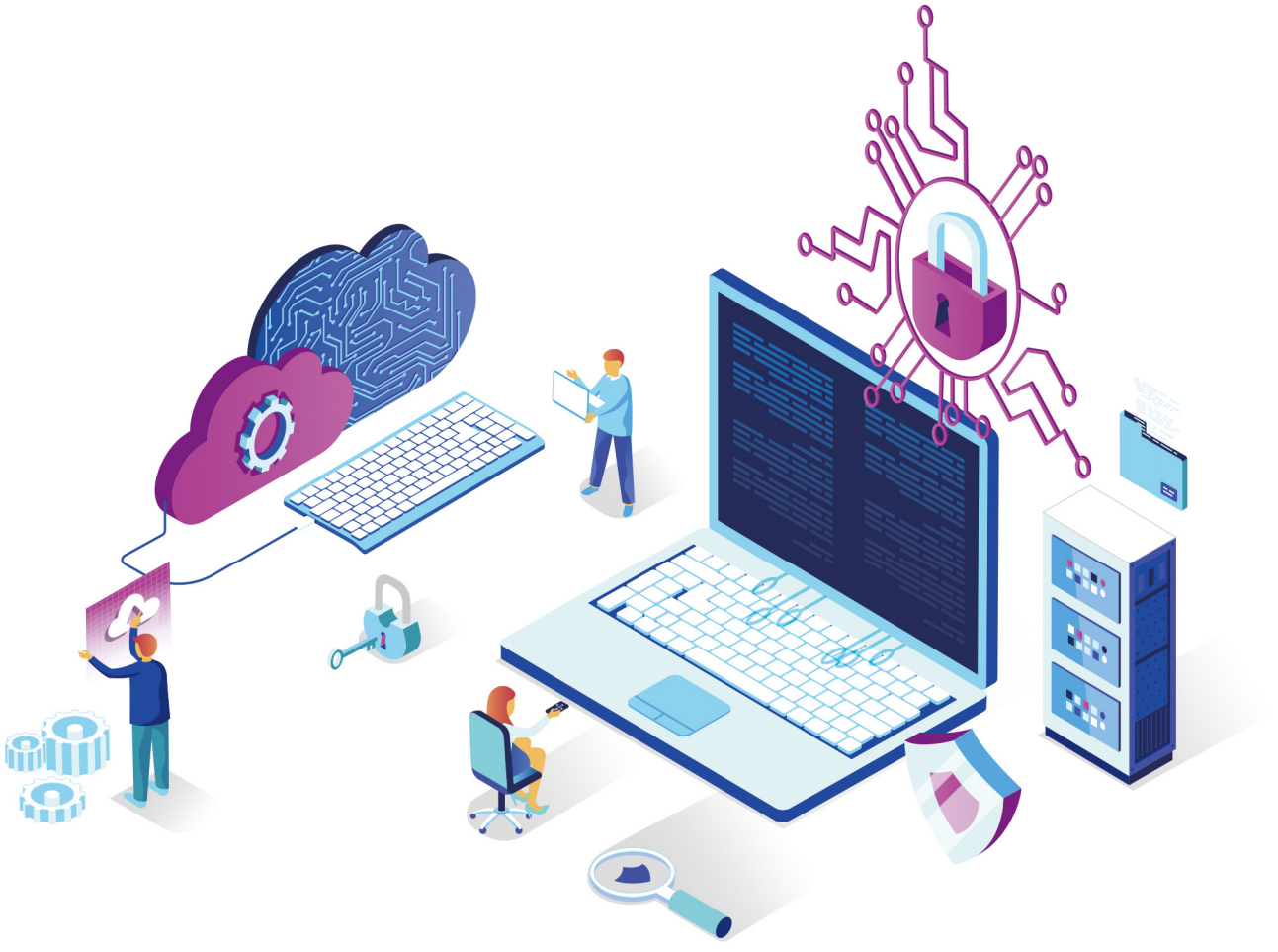
정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증제도 안내서



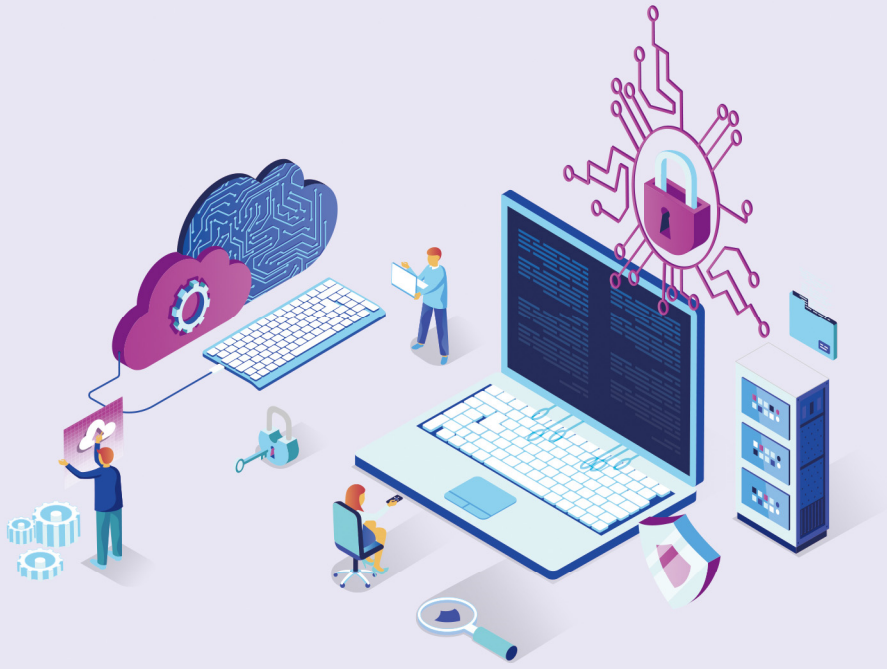
과학기술정보통신부 개인정보보호위원회 KISA 한국인터넷진흥원

정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도 안내서

2024. 7.



과학기술정보통신부 개인정보보호위원회 KISA 한국인터넷진흥원



정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도 안내서

• 들어가기 •

「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」(2018년 11월) 시행으로 정보보호 관리체계(ISMS)와 개인정보보호 관리체계(PIMS) 인증제도가 통합되었다.

본 안내서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조(정보보호 관리체계의 인증) 및 「개인정보보호법」 제32조의2(개인정보 보호 인증), 같은 법 시행령, 고시 등에서 규정하고 있는 사항에 대하여 구체적으로 설명하고자 한다. 안내서는 ISMS-P 인증을 취득하고자 하는 기관과 기업 관계자의 이해를 돕기 위하여 작성되었으며, 이외에도 ISMS-P 구축 및 운영에 관심이 있는 다양한 산업 분야에서 활용할 수 있다.

제1장에서는 ISMS-P 인증제도에 대하여 소개하고 있으며, 제2장에서는 ISMS-P 인증대상과 범위를 안내하고, 제3장에서는 ISMS-P 인증심사의 절차를 안내하고 있다. 단, 본 안내서에서 제시하는 예시는 인증 신청인의 내·외부 환경과 다를 수 있으므로 이를 충분히 고려하고 적용하여야 한다.

본 안내서에 제시된 법령, 고시, 참고자료 등은 안내서가 발행되는 시점(2024년 7월)을 기준으로 작성되었으며, 관련 법령 개정 및 기술·환경 변화를 반영하여 지속적인 보완 작업을 할 예정이므로 항상 최신 발행본 여부를 확인 후 사용해야 한다. 안내서 최신 버전은 ISMS-P 홈페이지(https://isms-p.kisa.or.kr)을 통해 확인할 수 있으며, 기타 문의사항은 아래 메일을 통해 문의할 수 있다.

E-mail : isms-p@kisa.or.kr

정보보호 및 개인정보보호 관리체계(ISMS-P)
인증제도 안내서

정보보호 및 개인정보보호 관리체계(ISMS-P)
인증제도 안내서

정보보호 및 개인정보보호 관리체계(ISMS-P)
인증제도 안내서

제1장

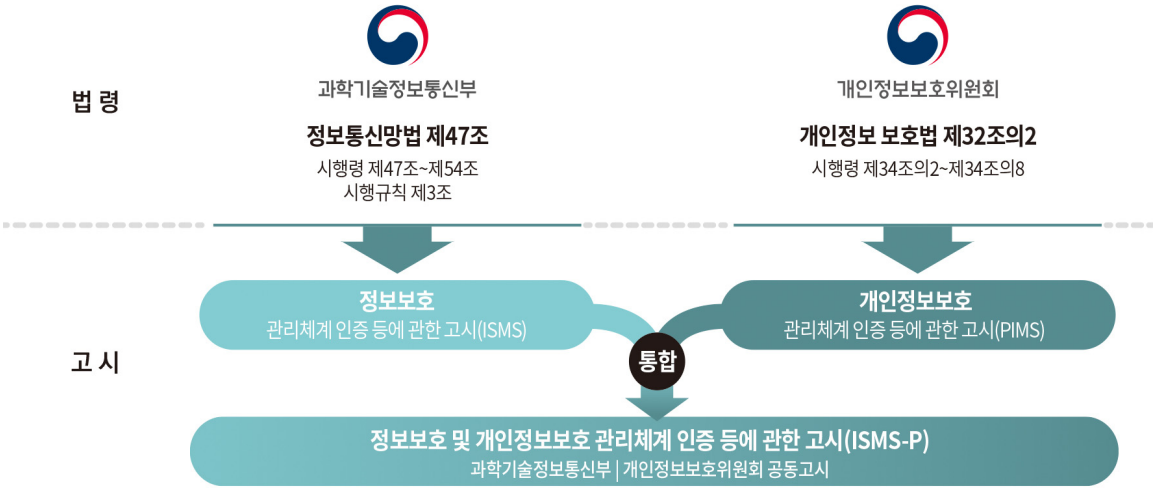
ISMS-P 인증제도 개요

1 ISMS-P 인증제도 개요

1.1. ISMS-P 인증의 법적 근거

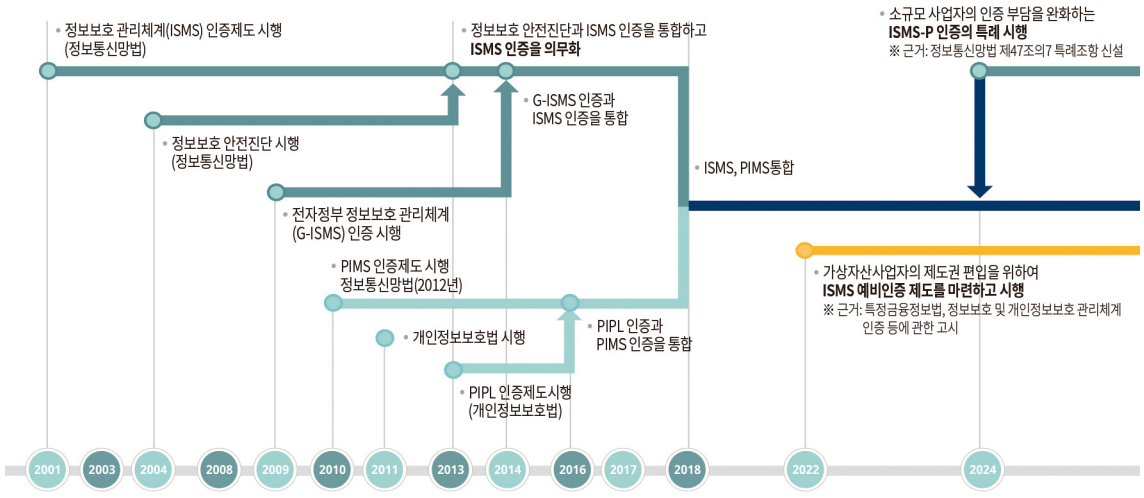
정보보호 및 개인정보보호 관리체계 인증제도는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 함) 제47조, 제47조의2 및 제47조의7, 같은 법 시행령 제47조부터 제54조의 규정 및 같은 법 시행규칙 제3조에 따른 정보보호 관리체계 인증과 「개인정보 보호법」 제32조의2, 같은 법 시행령 제34조의2부터 제34조의8의 규정에 따른 개인정보보호 관리체계 인증을 법적근거로 하고 있다.

- 법령에서 정한 인증의 통합을 위해 과학기술정보통신부와 개인정보보호위원회는 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」를 공동으로 개정하여 시행하고 있다.



〈그림 1〉 법령·고시와의 관계

1.2. ISMS-P 인증제도 추진경과



〈그림 2〉 인증제도 추진경과

- 정보보호 관리체계(ISMS) 인증제도는 국내 기업 스스로 정보보호 관리체계를 구축·운영하는데 활용할 수 있도록 관리체계 모델을 개발하고, 「정보통신망법」 개정을 통하여 도입되었다(2001년 7월 시행).
- 개인정보보호 관리체계(PIMS) 인증제도는 2010년 11월, 방송통신위원회 의결(제2010-66-273호)로 2011년부터 주요 정보통신서비스 제공 사업자 대상으로 인증심사를 우선 시행하였으며, 이후 PIMS 인증제도의 법률적 근거를 마련하였다(2013년 2월 시행).
- 정보통신망서비스제공자(ISP), 집적정보통신시설사업자(IDC), 정보통신서비스제공자 중 매출액, 이용자 수 등 일정 기준에 해당하는 기업들은 ISMS 인증을 의무적으로 받도록 「정보통신망법」이 개정되었다(2013년 2월 시행).
- 「개인정보 보호법」 개정을 통해 개인정보보호 인증(PIPL) 제도 시행의 법적 근거를 마련하였다(2013년 11월 시행).
- 인증 의무제도 시행 이후 인증 대상 기업이 늘어남에 따라 한국정보통신진흥협회(KAIT, 2014년 4월), 한국정보통신기술협회(TTA, 2015년 2월)를 ISMS 심사기관으로, 금융보안원(FSI, 2015년 7월)을 ISMS 인증기관으로 추가 지정하였다.
- 개인정보보호 관련 인증제도의 이원화 운영에 따른 기업의 혼란 해소를 위해 행정안전부와 방송통신위원회가 공동고시를 마련하여 개인정보보호 인증(PIPL) 제도와 PIMS 인증제도를 통합하였다(2016년 1월 시행).
- 정보통신망에 대한 의존도가 높고 개인정보 등 다량의 민감정보를 다루는 기관들이 ISMS 인증대상에서 제외되는 문제를 해결하기 위해 연간 매출액 또는 세입 등이 1,500억 원 이상인 자 중 일정 요건에 해당하는 기업들이 인증 의무대상에 포함되도록 「정보통신망법」이 개정되었다(2016년 6월 시행).
- 정보보호 및 개인정보보호 영역에서 각각의 인증제도 운영에 따른 기업의 혼란 해소 및 융합·고도화되는 침해위협에 효과적으로 대응하기 위해 과학기술정보통신부와 행정안전부 및 방송통신위원회가

공동고시를 마련하여 ISMS 인증제도와 PIMS 인증제도를 통합하였다(2018년 11월 시행).

- ISMS-P 통합 인증 출범에 따라 기존 ISMS 인증기관인 금융보안원(FSI)을 ISMS-P 인증기관으로 확대 지정하였으며, 또한 기존 ISMS 심사기관인 한국정보통신기술협회(TTA)와 한국정보통신진흥협회(KAIT)를 ISMS-P 심사기관으로 확대 지정하였다.(2019년 7월)
- 사회적 요구와 외부 환경 변화에 따라 ISMS-P 심사기관 상시지정, 사후관리, 재해재난 발생 시 예외조항을 신설하는 등 제도를 개선(2021년 3월)하였으며, 수요 증가에 따라 개인정보보호협회(OPA, 2020년 2월) 및 차세대정보보안인증원(NISC, 2023년 2월)을 심사기관으로 추가 지정하였다.
- 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제7조제1항에 따라 신고를 희망하는 가상자산사업자는 정보보호 관리체계 인증 취득을 요하며, 신규 가상자산사업자의 제도권 편입을 위하여 ISMS-P 고시 내 가상자산사업자에 대한 인증 특례조항을 신설하여 'ISMS 예비인증' 제도를 시행하고 있다(2022년 7월 시행).
- 「정보통신망법」 제47조의7(정보보호 관리체계 인증의 특례) 신설하여 인증에 어려움을 겪는 중소기업의 부담을 완화하고 제도권 편입을 촉진하기 위하여 완화된 인증기준과 비용으로 심사를 진행하는 'ISMS-P 인증의 특례'를 시행하고 있다(2024년 7월 시행).

1.3. ISMS-P 인증의 유형

[표 1] ISMS-P 인증의 유형

인증의 유형		주요내용
정보보호 관리체계 인증 (ISMS)	정보보호 관리체계 인증 ISMS Information Security Management System	**정보보호 중심으로 인증하는 경우** 기존의 ISMS 의무대상 기업·기관, 개인정보를 보유하지 않거나 개인정보 흐름의 보호가 불필요한 조직 등
정보보호 및 개인정보보호 관리체계 인증 (ISMS-P)	정보보호 및 개인정보보호 관리체계 인증 ISMS-P Personal information & Information Security Management System	**개인정보의 흐름과 정보보호 영역을 모두 인증하는 경우** 보호하고자 하는 정보서비스가 개인정보의 흐름을 가지고 있어 개인정보 처리 단계별 보안강화가 필요한 조직
정보보호 관리체계 예비인증	예비인증 정보보호 관리체계 인증 ISMS Information Security Management System	**가상자산사업자가 실제 서비스 운영 전 임시적으로 시스템을 구축·운영한 경우** 「특정금융정보법」에 따라 사업 영위를 위하여 신고를 해야 하지만, 2개월 이상의 운영 이력이 없어 ISMS 인증 심사를 진행할 수 없는 신규 가상자산사업자

- 조직의 정보보호를 위해 인증을 취득하고자 하는 조직은 ISMS 인증을 받고, 정보서비스에 개인정보 흐름이 포함되어 개인정보 처리 단계별 보안을 강화하고자 한다면 ISMS 인증범위에 '개인정보 처리단계별 요구사항' 분야를 포함하여 ISMS-P 인증을 취득할 수 있다.
- 「특정금융정보법」제7조제1항(신고)을 이행하고자 하나 2개월 이상의 운영 이력이 없어 본인증 취득에 어려움을 겪는 신규 가상자산산사업자는 시스템(임시)에 대하여 ISMS 예비인증을 취득할 수 있다.
- 「정보통신망법」제47조의7(정보보호 관리체계 인증의 특례)에 따라 제1항 각 호에 해당하는 기관은 완화된 기준과 절차로 ISMS 또는 ISMS-P를 취득할 수 있다.

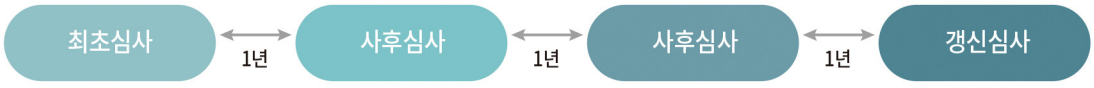
☞ 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시

고시 제2조(용어의 정의)

1. "정보보호 및 개인정보보호 관리체계 인증"이란 인증 신청인의 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다) 또는 인증기관이 증명하는 것을 말한다.
2. "정보보호 관리체계 인증"이란 인증 신청인의 정보보호 관련 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 것을 말한다.

1.4. ISMS-P 인증심사의 종류

- ISMS-P 인증심사의 종류는 '최초심사', '사후심사', '갱신심사'가 있다.



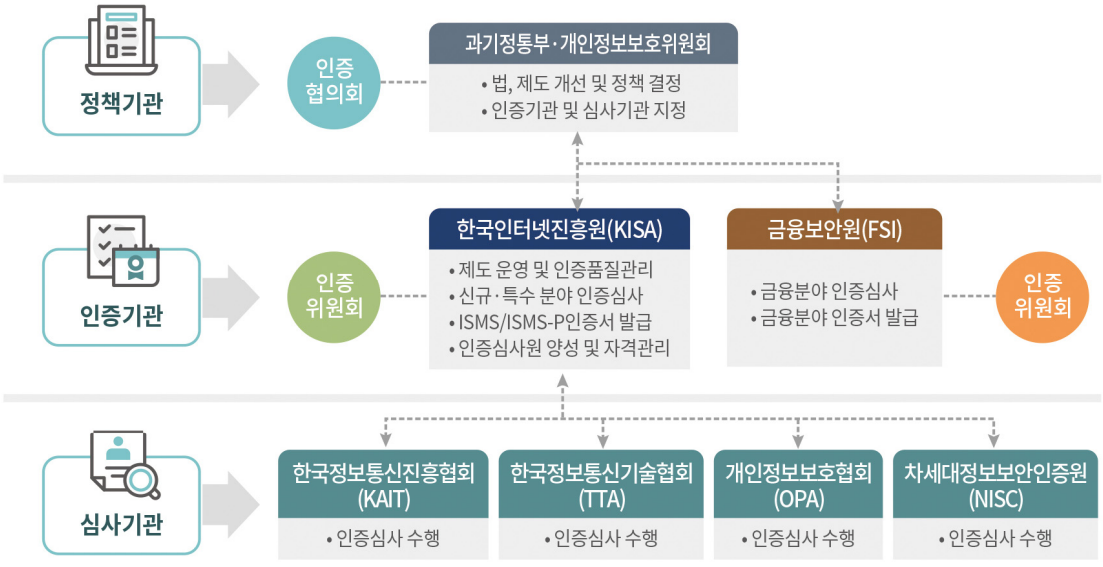
〈그림 3〉 인증심사의 종류

- '최초심사'는 ISMS-P 인증을 처음으로 취득하고자 할 때 수행하는 심사이며, 인증범위에 중요한 변경이 있어 다시 인증을 신청할 경우에도 같은 심사를 받아야 한다. 최초심사를 통해 인증을 취득하면 3년의 유효기간이 부여된다.
- '사후심사'는 인증을 취득한 이후 ISMS-P가 지속적으로 유지되고 있는지 확인하는 것을 목적으로 인증 유효기간 중 매년 1회 이상 실시하는 인증심사를 말한다.
  - 고시 제27조(사후관리)제3항에 따라 인증 취득한 범위와 관련하여 침해사고 또는 개인정보 유출사고가 발생한 경우 한국인터넷진흥원은 필요에 따라 인증관련 항목의 보안향상을 위한 필요한 지원 등을 할 수 있다.
  - 고시 제35조(인증의 취소)에 따라 사후심사를 실시하지 않는 경우 한국인터넷진흥원은 인증위원회

심의·의결을 거쳐 인증을 취소할 수 있다.

- ‘갱신심사’는 ISMS-P 인증의 유효기간 갱신을 위해 실시하는 인증심사를 말한다.
  - ISMS-P 인증은 인증 유효기간 만료 이전에 갱신심사를 통해 유효기간을 갱신하여야 하며, 유효기간이 경과한 때에는 인증의 효력이 상실된다.

2 ISMS-P 인증 추진체계



〈그림 4〉 담당기관 및 체계

2.1. 정책기관(협의회)

- 과학기술정보통신부장관과 개인정보보호위원회는 ISMS-P 인증 운영에 관한 정책 사항을 협의하기 위하여 ISMS-P 인증 협의회(이하 “협의회”이라 한다)를 구성하여 운영한다.
- 협의회는 인증제도와 관련한 법제도 개선, 정책 결정, 인증기관 및 심사기관 지정 등의 업무를 수행한다.

2.2. 인증기관

- 법정 인증기관인 한국인터넷진흥원 또는 과학기술정보통신부장관과 개인정보보호위원회가 지정한 인증기관은 인증에 관한 업무를 수행한다.
- 한국인터넷진흥원은 인증위원회 운영, 인증심사원 양성 및 자격관리, 인증제도 및 기준 개선 등 ISMS-P 인증제도 전반에 걸친 업무를 수행한다.
- 인증기관은 신청기관이 수립·운영하는 관리체계를 인증기준에 따라 심사하고, 인증위원회를 운영하여 인증기준에 적합한 기관에게 인증서를 발급한다.
- 과학기술정보통신부장관, 개인정보보호위원회가 2019년 7월 지정한 인증기관인 금융보안원(FSI)은 금융 분야 인증위원회를 구성·운영하고, 인증심사 및 인증서 발급 업무를 수행한다.

2.3. 인증위원회

- 인증위원회는 인증심사 결과가 인증기준에 적합한지 여부, 인증 취소에 관한 사항, 이의신청에 관한 사항 등을 심의·의결한다.
- 인증위원회는 35명 이하의 위원으로 구성하며, 위원은 정보보호 또는 개인정보보호 분야에 학식과 경험이 있는 전문가 중에서 한국인터넷진흥원 또는 인증기관의 장이 위촉한다.

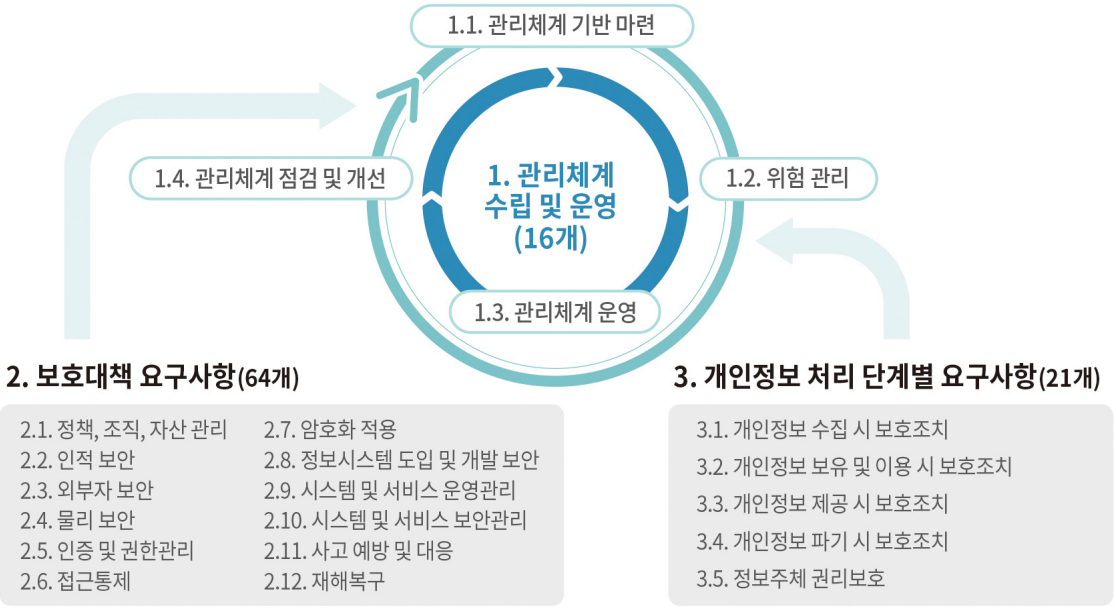
2.4. 심사기관

- 심사기관은 인증심사 일정이 확정될 시 한국인터넷진흥원에 심사원 모집을 요청하여 심사팀을 구성하고, 신청기관이 수립·운영하는 정보보호 및 개인정보보호 관리체계를 인증기준에 따라 심사하며, 심사기간에 발견된 결함사항의 보완조치 이행 여부 확인 등 인증심사 업무를 수행한다.

2.5. 신청기관

- 신청기관은 정보보호 및 개인정보보호 활동이 체계적이고 지속적으로 관리되고 있는지를 객관적으로 검증 받기 위하여 ISMS-P 인증을 취득하고자 신청하는 자를 의미한다.

3 ISMS-P 인증기준



〈그림 5〉 ISMS-P 인증기준

- ISMS-P 인증기준은 '1.관리체계 수립 및 운영(16개)', '2.보호대책 요구사항(64개)', '3.개인정보 처리 단계별 요구사항(21개)'으로 구성되어 있다.
- '1.관리체계 수립 및 운영'은 관리체계의 메인프레임으로서 전반적인 관리체계 운영 라이프사이클을 구성하고 있다. '2.보호대책 요구사항'은 총 12개 분야에 대한 인증기준으로서 정책, 조직, 자산, 교육 등 관리적 부문과 개발, 접근통제, 운영·보안관리 등 물리적·기술적 부문의 보호대책에 관한 사항으로 구성되어 있다. '3.개인정보 처리 단계별 요구사항'은 개인정보 생명주기에 따른 보호조치 사항으로 구성되어 있다.

3.1. 인증유형에 따른 인증기준

[표 2] ISMS, ISMS-P 인증기준 항목

인증 영역	인증기준	항목 수	적용 여부	
			ISMS	ISMS-P
1. 관리체계 수립 및 운영(16개)	1.1 관리체계 기반 마련	6	○	○
	1.2 위험 관리	4	○	○
	1.3 관리체계 운영	3	○	○
	1.4 관리체계 점검 및 개선	3	○	○
2. 보호대책 요구사항(64개)	2.1 정책, 조직, 자산 관리	3	○	○
	2.2 인적 보안	6	○	○
	2.3 외부자 보안	4	○	○
	2.4 물리 보안	7	○	○
	2.5 인증 및 권한관리	6	○	○
	2.6 접근통제	7	○	○
	2.7 암호화 적용	2	○	○
	2.8 정보시스템 도입 및 개발 보안	6	○	○
	2.9 시스템 및 서비스 운영관리	7	○	○
	2.10 시스템 및 서비스 보안관리	9	○	○
	2.11 사고 예방 및 대응	5	○	○
	2.12 재해 복구	2	○	○
3. 개인정보 처리 단계별 요구사항(21개)	3.1 개인정보 수집 시 보호조치	7	-	○
	3.2 개인정보 보유 및 이용 시 보호조치	5	-	○
	3.3 개인정보 제공 시 보호조치	4	-	○
	3.4 개인정보 파기 시 보호조치	2	-	○
	3.5 정보주체 권리보호	3	-	○
합계		101	80	101

- ISMS, ISMS-P 인증의 구분에 따라 인증심사 시 주안점에 차이가 있으므로, 아래의 예시를 참고하여 관리체계를 수립하여야 한다.
  - 단, ISMS 인증을 취득하고자 하는 신청기관의 경우에도 개인정보보호와 관련한 법적요구사항을 준수하여 개인정보를 안전하게 관리·운영하여야 한다.

[표 3] 인증의 구분에 따른 심사 주안점 차이(예시)

항목	인증기준	ISMS 심사 주안점	ISMS-P 심사 주안점
1.1.2 최고 책임자 지정	최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.	정보보호 최고책임자 지정에 대해 확인	정보보호 최고책임자, 개인정보보호 책임자 지정에 대해 확인
1.1.3 조직 구성	최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호 담당자로 구성된 협의체를 구성하여 운영하여야 한다.	정보보호 관련 조직 구성 및 운영 현황에 대해 확인	정보보호와 개인정보보호 관련 조직 구성 및 운영 현황에 대해 확인
1.2.1 정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.	정보자산 식별·분류의 기준 및 현황에 대해 확인	정보자산 식별·분류의 기준 및 현황에 대해 확인하며, 정보자산 중 개인정보 현황 및 분류기준을 필수로 확인
1.2.2 현황 및 흐름분석	관리체계 전 영역에 대한 정보서비스 및 개인정보처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.	정보서비스의 처리에 관한 현황 및 흐름분석	정보서비스 및 개인정보처리에 관한 현황 및 흐름분석

4 기대 효과

4.1. ISMS-P 인증의 기대 효과

- 일회성 정보보호 대책에서 벗어나 체계적, 종합적인 정보보호 관리체계를 구현함으로써 기업의 정보보호 및 개인정보보호 관리수준을 향상 시킬 수 있다.
- 기업은 지속적이고 체계적인 ISMS-P 구축을 통해 해킹, DDoS 등의 침해사고 및 개인정보 유출사고 발생 시 신속하게 대응할 수 있는 관리체계를 마련할 수 있다.
- 기업 경영진이 직접 정보보호 의사결정에 참여함으로써 정보보호 및 개인정보보호 업무에 대한 책임성과 신뢰성을 향상시킬 수 있다.
- ISMS-P 인증을 취득한 기관은 정보보호 및 개인정보보호에 대한 신뢰성을 높여 대외 이미지를 제고할 수 있다.
- ISMS-P 인증을 취득한 기관은 공공부문 사업 입찰 시 가산점 등의 인센티브를 얻을 수 있다.

☞ 인증을 취득하면 침해사고로부터 100% 안전한가?

- ISMS-P 인증을 받은 기업(조직)이 정보보안 침해사고로부터 100% 안전하다는 것을 보장하지는 못한다.
- 다만 인증취득을 통해 정보보호 침해사고 발생 가능성을 낮출 수 있으며, 침해사고가 발생하더라도 안전한 정보보호 관리체계 운영으로 서비스 복구 등에 소요되는 시간을 최소화할 수 있다.
- 이는 주기적인 운동, 식이요법, 예방 접종 등으로 꾸준히 건강을 관리한 사람도 100% 질병이 걸리지 않음을 보장할 수 없는 것과 유사한 이치다.

4.2. 인증의 홍보

- ISMS-P 인증을 취득한 자는 과학기술정보통신부장관, 개인정보보호위원회가 정하여 고시하는 ISMS-P 인증표시를 사용할 수 있다. 이 경우 인증의 범위와 유효기간을 함께 표시하여야 한다.

☞ 관련 법령

- 「정보통신망법」 시행령 제52조(인증표시 및 홍보)
- 「개인정보 보호법」 시행령 제34조의7(인증의 표시 및 홍보)

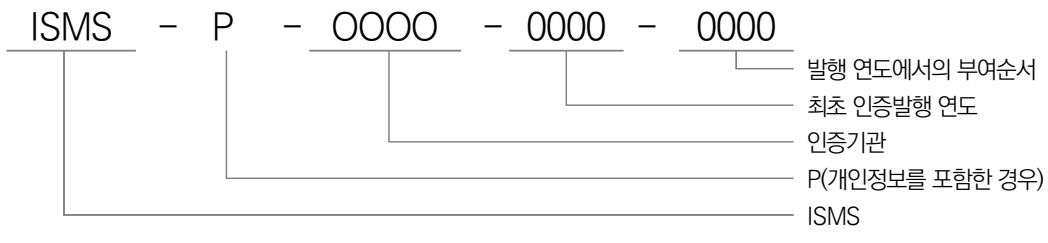
[표 4] ISMS-P 인증 도안 모형

정보보호 관리체계 인증	정보보호 및 개인정보보호 관리체계 인증	정보보호 관리체계 예비인증
		

- 인증표시를 사용하는 경우 인증의 범위와 유효기간을 함께 표시하여야 하며, 고시에 지정된 색상 등 사용방법을 준수해야 한다.
- 인증표시의 크기는 표시물 대상의 크기나 표시장소의 여건에 따라 조정할 수 있으며, 같은 비율로 축소 또는 확대하여 표시할 수 있다.
- ISMS 및 ISMS-P 인증취득 사실의 홍보는 인증서 발급일로부터 인증의 효력이 유지되는 동안에만 사용 가능하며 인증이 취소된 경우에는 인증에 대한 홍보, 인증서 사용을 중지해야 한다.
- 인증마크는 기관의 홈페이지 또는 인증을 취득한 서비스 제공 등에 필요한 경우와 일반문서, 봉투, 홍보 책자 등에 사용할 수 있다.

4.3. 인증번호의 부여

- 인증번호는 유일성, 간결성, 관리의 용이성 등을 고려하여 최초심사, 갱신심사의 구분 없이 최초 발급순서별로 부여한다.
- 인증번호는 아래와 같은 형식으로 부여한다.



정보보호 및 개인정보보호 관리체계(ISMS-P)
인증제도 안내서

제2장

ISMS-P 인증대상 및 범위

1. ISMS-P 인증대상
2. ISMS-P 인증범위

1 ISMS-P 인증대상

〈그림 6〉 ISMS-P 인증대상

1.1. 임의신청자

- ISMS-P를 구축·운영하여 적합성 여부를 판단하고자 하는 모든 개인정보처리자(공공기관, 민간기업, 법인, 단체 및 개인)와 정보통신서비스 제공자는 자율적으로 인증을 신청할 수 있다.
  - 임의신청자의 경우 인증범위를 신청기관이 정하여 신청할 수 있으며, 심사기준 및 심사절차는 의무대상자와 동일하다.

1.2. 의무대상자

- 인증 의무대상자는 ①정보통신망서비스를 제공하는 자(ISP) ②집적정보통신시설사업자(IDC) ③전년도 매출액 또는 세입 등이 1,500억 원 이상이거나 정보통신서비스 부문의 전년도 매출액이 100억 원 이상 또는 전년도 일일평균 이용자 수 100만 명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자이다.
  - 인증 의무대상자는 ISMS 인증을 받아야 하며 ISMS-P 인증을 받은 경우에도 인증의무를 이행한 것으로 본다.

[표 5] ISMS 의무대상자 기준

구분	의무대상자 기준
정보통신망서비스 제공자(ISP)	「전기통신사업법」 제6조 제1항에 따른 등록을 한 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
집적정보통신시설 사업자(IDC)	「정보통신망법」 제46조에 따른 집적정보통신시설 사업자
매출액 또는 이용자수 요건에 따른 대상자	정보통신서비스 부문 전년도 매출액이 100억 원 이상인 자
	전년도 일일평균 정보통신서비스 이용자 수가 100만 명 이상인 자
	전년도 매출액 또는 세입이 1,500억 원 이상인 자 중에서 다음에 해당되는 경우 - 「의료법」 제3조의4에 따른 상급종합병원 - 직전연도 12월 31일 기준으로 재학생 수가 1만 명 이상인 「고등교육법」 제2조에 따른 학교

※ 관계법령: 「정보통신망법」 제47조제2항 및 같은 법 시행령 제49조

① 정보통신망서비스를 제공하는 자

- 정보통신망서비스를 제공하는 자(ISP)란 「전기통신사업법」 제6조제1항 각 호의 사항을 과학기술정보통신부장관에게 등록을 한 자 중 '서울특별시 및 모든 광역시'에서 정보통신망 서비스를 제공하는 사업자를 말한다.

☞「정보통신망법」 및 같은 법 시행령

「정보통신망법」 제47조(정보보호 관리체계의 인증)

② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

1. 「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망 서비스를 제공하는 자

「정보통신망법」 시행령 제49조(정보보호 관리체계 인증 대상자의 범위)

① 법 제47조제2항제1호에서 "대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자"란 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자를 말한다.

※ 정보통신망서비스 제공자의 경우, 매출액과 이용자 수에 관계없이 인증 의무대상자에 해당함

[표 6] 정보통신망서비스(예시)

구분	서비스	세부 서비스
정보통신망서비스 제공자 (ISP)	기간통신서비스	인터넷 접속 서비스 (초고속망 서비스)
		인터넷전화 서비스(VoIP)
		이동통신 서비스 (셀룰라, PCS, 3G, 4G/LTE, 5G)

※ '서울특별시 및 모든 광역시'에서 서비스를 제공하지 않는 정보통신망서비스 제공자의 경우, 「정보통신망법」 제47조제2항제3호의 기준을 적용함

※ 불특정 다수가 이용하는 정보통신망인 경우, 인증 의무대상자에 해당함

② 집적정보통신시설사업자

■ 집적정보통신시설사업자(IDC)란 「정보통신망법」 제46조제1항의 규정에 따라 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자를 말한다.

☞「정보통신망법」

제47조(정보보호 관리체계의 인증)

② 전기통신사업법 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

2. 집적정보통신시설 사업자

※ 집적정보통신시설사업자의 경우, 매출액과 이용자 수에 관계없이 인증 의무대상자에 해당함

- 정보통신서비스 제공을 위해 자체적으로 시설을 구축하여 운영하는 자로서, 공간 임대서비스 (Co-location) 또는 서버 임대(서버호스팅) 서비스 및 네트워크 서비스 등을 제공하는 사업자를 말한다.
- 타인에 의해 구축된 집적정보통신시설의 일부를 임대하여 서비스를 재판매하는 사업자(이하 "VIDC"이라 한다)의 경우에는 「정보통신망법」 시행령 제49조제2항에 따라 전년도 매출액 또는 이용자 수 기준을 적용한다.

☞ 고시

제19조(정보보호 관리체계 인증 의무대상자) ① 정보보호 관리체계 인증 의무대상자(이하 "의무대상자"라 한다)란 정보통신망법 제47조제2항, 같은 법 시행령 제49조에 해당하는 자를 말한다.

② 제1항에 해당하는 자 중 집적정보통신시설 사업자가 마련한 시설의 일부를 임대하여 집적정보통신시설 사업을 하는 자에 대하여는 정보통신망법 시행령 제49조제2항의 기준을 준용한다.

[표 7] 집적정보통신시설 서비스(예시)

구분	서비스	세부 서비스
집적정보통신시설사업자 (IDC)	부가통신서비스	서버 호스팅
		스토리지 호스팅
		코로케이션(Co-location)
		네트워크 제공 서비스(회선 임대 포함), 보안관리 서비스, 도메인관리 서비스

③ 전년도 매출액 또는 세입 등이 (1)1,500억 원 이상이거나 (2)정보통신서비스 부문 전년도 매출액이 100억 원 이상 또는 (3)전년도 일일평균 이용자 수가 100만 명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

☞ 「정보통신망법」 및 같은 법 시행령

「정보통신망법」 제47조(정보보호 관리체계의 인증)

② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억월 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

「정보통신망법」 시행령 제49조(정보보호 관리체계 인증 대상자의 범위)

② 법 제47조제2항제3호에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 전년도 매출액 또는 세입이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자
   가. 「의료법」 제3조의4에 따른 상급종합병원
   나. 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.
3. 전년도 일일평균 이용자 수가 100만명 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.

(1) 전년도 매출액 또는 세입 등이 1,500억 원 이상인 자 중 대통령령으로 정하는 기준에 해당하는 자

- 전년도 매출액 또는 세입 등이 1,500억 원 이상인 자 중 「의료법」 제3조의4에 따른 '상급종합병원'과 직전연도 12월 31일 기준으로 재학생 수가 1만 명 이상인 「고등교육법」 제2조에 따른 '학교'는 인증의무대상에 포함된다.

  ※ '상급종합병원'은 매 3년마다 평가를 실시하여 재지정 하거나 지정이 최소 될 수 있음

  ※ 「고등교육법」 제2조에 따른 학교는 대학, 산업대학, 교육대학, 전문대학, 방송대학·통신대학·방송통신대학 및 사이버대학, 기술대학, 각종학교를 포함

(2) 정보통신서비스 부문 전년도 매출액 100억 원 이상인 자

- 정보통신서비스 부문 매출액은 정보통신서비스 제공을 통해 발생하는 연간 총 매출액의 합으로 산정하며, 여러 가지 정보통신서비스를 제공할 경우에는 해당 서비스의 매출액을 모두 합하여 계산한다.

  ※ 매출액은 국세청 등에 신고된 금액, 공인회계사 등의 검증을 거친 내부 결산자료 등 객관적 자료를 이용

[표 8] 주요 정보통신서비스 매출액 구분(예시)

구분	서비스 설명	정보통신서비스 부문 매출액 내역
신용카드 검색(CCIS)서비스	정보통신망으로 신용카드의 도난분실, 한도초과, 연체 등을 실시간으로 확인하는 서비스를 제공하는 사업자	카드조회수수료, 서비스매출, 회원수익매출, 부가수익 등
컴퓨터 예약(CRS)서비스	정보통신망을 통해 서비스나 상품에 대한 예약서비스를 제공하는 사업자	상품 및 서비스 판매매출, 수수료, 회원수익매출, 광고매출, 부가수익 등
전자문서교환(EDI)서비스	정보통신망을 통해 전자문서교환서비스를 제공하는 사업자	콘텐츠 판매매출, 수수료, 광고매출, 회원수익매출, 부가수익 등
전자지불(PG)서비스	정보통신망을 통해 지불중계역무를 제공하는 사업자	지불중계수수료, 서비스매출, 회원수익매출, 부가수익 등
인터넷 포털 서비스	정보통신망 유·무선 포털 사이트를 제공하는 사업자	온라인 광고매출, 정보제공 수수료, 중계수수료, 콘텐츠, 이용매출, 부가수익 등

구분	서비스 설명	정보통신서비스 부문 매출액 내역
인터넷 전자상거래	쇼핑몰 역무를 제공하는 사업자	판매 매출, 수수료, 광고매출, 부가수익 등
인터넷 방송	정보통신망을 통해 신문기사나 방송 프로그램을 제공하는 사업자	콘텐츠 판매매출, 수수료, 광고매출, 회원 수익매출, 부가수익 등
인터넷 게임	인터넷게임서비스를 제공하는 사업자	게임이용매출, 아이템 판매매출, 광고매출, 수수료, 부가수익 등
금융 관련 서비스	정보통신망을 통한 금융업, 연금업, 보험 관련 서비스업 등을 제공하는 사업자	인터넷 뱅킹·주식 거래·선물 거래 수수료, 인터넷 증권 중개, 홈트레이딩 기타 인터넷 금융 및 보험업 등
콘텐츠 제공 서비스	정보통신망을 통한 교육서비스를 제공하는 사업자	콘텐츠 이용매출, 수수료, 광고매출, 회원 수익매출, 부가수익 등
	정보통신망을 통한 실시간 음악 감상 서비스를 제공하는 사업자	
	정보통신망을 통한 기타 콘텐츠제공 서비스를 제공하는 사업자	
유선방송 서비스 (Cable-SO)	종합유선 방송서비스와 종합유선전송 서비스를 제공하는 사업자	방송중계서비스 매출을 제외한 초고속 인터넷서비스 매출액 등
기타	정보통신망을 통한 기타 정보통신서비스를 제공하는 사업자	

※ 정보통신서비스 온라인 판매, 광고, 콘텐츠 이용 등으로 발생한 매출액과 부가수익, 수수료, 세금 등을 포함한 총 합계액

※ 정보통신서비스 제공을 통해 직·간접으로 발생하는 연간 국내·외 매출액

[표 9] 쇼핑몰 유형 별 매출 구분(예시)

판매 유형	정보통신서비스 부문에 해당되는 매출액
자체 쇼핑몰 운영	자체 쇼핑몰을 통한 제품 판매액
중개 쇼핑몰 이용	해당사항 없음
중개 쇼핑몰 운영	판매 중개수수료 + 입점료(해당하는 경우)
자체 쇼핑몰 운영 + 중개 쇼핑몰 이용	자체 쇼핑몰을 통한 제품 판매액
중개 쇼핑몰 운영 + 자체 쇼핑몰 운영	판매 중개수수료 + 입점료(해당하는 경우) + 자체 쇼핑몰을 통한 제품 판매액
포인트 쇼핑몰	가맹점 수수료 + 고객 수수료 + 판매 수수료 + 기프티콘

(3) 전년도 일일평균 이용자 수 100만 명 이상

- 일일평균 이용자 수는 일정 기간 동안의 정보통신서비스제공자의 홈페이지 방문자 수 등을 일평균으로 환산한 이용자 수를 말하며, 여러 가지 정보통신서비스를 제공할 경우에는 해당 서비스의 이용자 수를 모두 합하여 계산한다.

  ※ 자체적 또는 공식적으로 이용자 수 확인이 어려운 경우, 민간 통계기관 등의 데이터 활용

1.3. 가상자산사업자

- 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제7조에 따라 가상자산사업자는 정보보호 관리체계 인증을 받고 금융정보분석원장에게 신고하여야 하며, 인증을 획득하지 못한 경우 금융정보분석원장은 신고를 수리하지 않을 수 있다.

☞「특정금융정보법」 및 같은 법 시행령

「특정금융정보법」 제7조(신고)

① 가상자산사업자(이를 운영하려는 자를 포함한다. 이하 이 조에서 같다)는 대통령령으로 정하는 바에 따라 다음 각 호의 사항을 금융정보분석원장에게 신고하여야 한다.

③ 금융정보분석원장은 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자에 대해서는 대통령령으로 정하는 바에 따라 가상자산사업자의 신고를 수리하지 아니할 수 있다.

1. 정보보호 관리체계 인증을 획득하지 못한 자

「특정금융정보법」 시행령 제10조의11(가상자산사업자의 신고)

① 법 제7조제1항에 따라 신고를 하려는 자는 금융정보분석원장이 정하여 고시하는 신고서에 다음 각 호의 서류를 첨부하여 금융정보분석원장에게 제출해야 한다.

3. 법 제5조의2제1항제3호마목2)에 따른 정보보호 관리체계 인증(이하 "정보보호관리체계인증"이라 한다)에 관한 자료

[참고] 「특정금융정보법」 제5조의2(금융회사등의 고객 확인의무)

① 금융회사등은 금융거래등을 이용한 자금세탁행위 및 공중협박자금조달행위를 방지하기 위하여 합당한 주의(注意)로서 다음 각 호의 구분에 따른 조치를 하여야 한다. 이 경우 금융회사 등은 이를 위한 업무 지침을 작성하고 운영하여야 한다.

3. 고객이 가상자산 사업자인 경우: 다음 각 목의 사항을 확인

마. 다음 1) 또는 2)에 해당하는 사항의 이행에 관한 사항

2) 「정보통신망 이용촉진 및 정보(보호 등에 관한 법률」 제47조 또는 「개인정보 보호법」 제32조의2에 따른 정보보호 관리체계 인증(이하 "정보보호 관리체계 인증"이라 한다)의 획득

■ 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제18조의2(가상자산사업자에 대한 인증) 제1항제1호에 따라, 정상적인 사업을 운영할 수 없는 신규 가상자산사업자는 시험 운영 환경에서의 정보보호 관리체계에 대하여 '정보보호 관리체계 예비인증'('예비인증')을 신청할 수 있다.

▶ 예비인증은 고시 제18조2제1항제2호에 따른 본인증을 받기 위한 조건부 인증으로, 예비인증을 취득한 날부터 3개월 이내에 금융분석원장에게 신고하여야 하며, 신고가 수리된 날부터 6개월 이내에 본인증을 취득하여야 한다.

☞ 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 및 같은 법 시행령

제18조의2(가상자산사업자에 대한 인증)

① 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제7조제1항에 따라 신고를 하려는 가상자산사업자 (가상자산사업을 운영하려는 자를 포함한다. 이하 이 조에서 같다)에 대한 제18조제1항제2호의 인증은 다음 각 호로 구분한다.

1. 예비인증: 가상자산사업자 중 본인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 2개월 이상 운영하지 못한 자가 실제 서비스 운영 전 임시적으로 관련 시스템을 구축·운영(이하 "시험운영"이라 한다)하여 받는 인증으로서 제2호에 따른 본인증을 받기 위한 조건부 인증
2. 본인증: 예비인증을 취득한 자로서 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 2개월 이상 운영한 자를 대상으로 하는 인증

② 인터넷진흥원 또는 인증기관은 가상자산사업자에게 제1항제1호에 따른 예비인증을 부여할 때에는 다음 각 호의 조건을 붙여야 한다.

1. 예비인증 취득한 날부터 3개월 이내에 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제7조에 따른 신고를 할 것
2. 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제7조에 따라 신고가 수리된 날부터 6개월 이내에 제1항제2호에 따른 본인증을 취득할 것(다만, 본인증 절차가 완료 될 때까지는 예비인증의 효력은 유효한 것으로 본다.)

1.4. 중소기업

■ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의7에 해당하는 자는 완화된 인증기준 및 절차에 따라 정보보호 관리체계 인증을 신청할 수 있다.

■ 의무대상자인 동시에 인증의 특례 대상에 해당하는 자는 인증의 특례에 따라 인증을 받은 경우에도 인증의무를 이행한 것으로 본다.

☞「정보통신망법」 및 같은 법 시행령

「정보통신망법」 제47조의7(정보보호 관리체계 인증의 특례)

① 과학기술정보통신부장관은 제47조제1항 및 제2항에 따른 인증을 받으려는 자 중 다음 각 호의 어느 하나에 해당하는 자에 대하여 제47조에 따른 인증기준 및 절차 등을 완화하여 적용할 수 있다.

1. 「중소기업기본법」 제2조제2항에 따른 소기업
2. 그 밖에 정보통신서비스의 규모 및 특성에 따라 대통령령으로 정하는 기준에 해당하는 자

「정보통신망법」 시행령 제49조의2(정보보호 관리체계 인증의 특례 대상자의 범위)

① 법 제47조의7제1항제2호에 따른 정보보호 관리체계 인증의 특례 대상은 「중소기업기본법」 제2조제2항에 따른 중기업으로서 다음 각 호의 어느 하나에 해당하는 자로 한다.

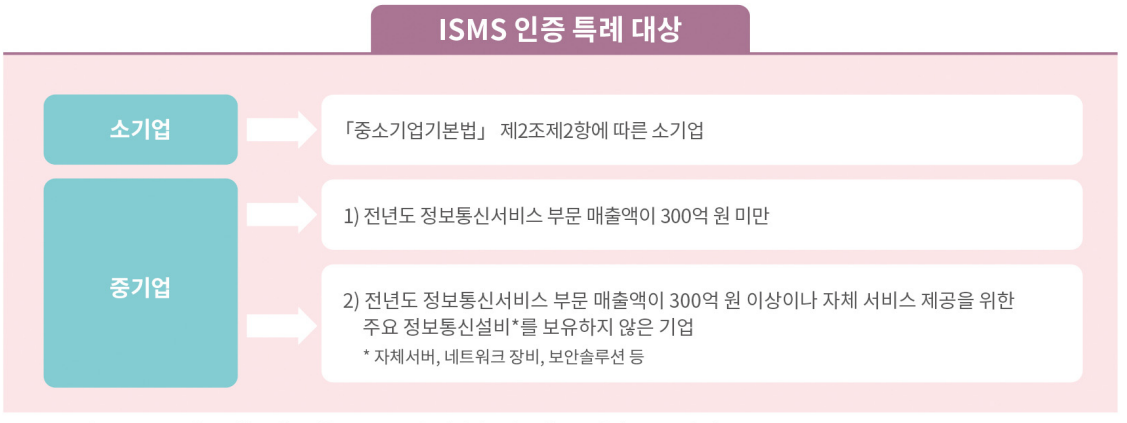
1. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 300억 원 미만인 자
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 300억 원 이상인 자이고 주요 정보통신설비를 직접 설치·운영하지 아니한 자로서 다음 각 목의 어느 하나에 해당하는 서비스(법 제47조제1항에 따른 인증 또는 「개인정보 보호법」 제32조의2제1항에 따른 인증 또는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조의2제1항에 따른 인증을 받은 자의 서비스로 한정)를 이용하는 자

가. 호스팅 서비스(인터넷 전용회선을 갖추고 웹서버·메일서버 등을 제공하거나 도메인등록 및 유지보수 등의 업무를 대행해 주는 서비스를 말한다)

나. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제3조제2호 및 제2호에 따른 클라우드컴퓨팅 서비스

② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자는 법 제47조의7제1항제2호에 따른 정보보호 관리체계 인증의 특례 대상에서 제외한다.

1. 법 제47조제2항제1호 또는 제2호에 해당하는 자
2. 제49조제2항제1호 또는 제3호에 해당하는 자
3. 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제2조제1호하목에 따른 가상자산사업자
4. 「전자금융거래법」 제2조제3호에 따른 금융회사



※ 단, ISP, IDC, 상급종합병원, 대학교, 금융회사, 가상자산사업자는 대상에 해당하지 않음

〈그림 7〉 ISMS 인증의 특례 대상

① 소기업

- 소기업이란 「중소기업기본법」 제2조제2항과 같은 법 시행령 제8조제1항에서 정의하는 기업을 의미한다.

☞「중소기업기본법」 및 같은 법 시행령

「중소기업기본법」제2조(중소기업자의 범위)

② 중소기업은 대통령령으로 정하는 구분기준에 따라 소기업(小企業)과 중기업(中企業)으로 구분한다.

「중소기업기본법」시행령 제8조(소기업과 중기업의 구분)

① 법 제2조제2항에 따른 소기업(小企業)은 중소기업 중 해당 기업이 영위하는 주된 업종별 평균매출액 등이 별표 3의 기준에 맞는 기업으로 한다.

② 중기업

(1) 정보통신서비스 부문 매출액이 300억 원 미만인 경우

- 중기업이란 「중소기업기본법」 제2조제2항과 같은 법 시행령 제8조제2항에서 정의하는 기업을 의미하며, 해당 기업 중 정보통신서비스 부문 매출액이 300억 원 미만인 경우에 해당한다.

☞「중소기업기본법」 및 같은 법 시행령

「중소기업기본법」제2조(중소기업자의 범위)

② 중소기업은 대통령령으로 정하는 구분기준에 따라 소기업(小企業)과 중기업(中企業)으로 구분한다.

「중소기업기본법」시행령 제8조(소기업과 중기업의 구분)

② 법 제2조제2항에 따른 중기업(中企業)은 중소기업 중 제1항에 따른 소기업을 제외한 기업으로 한다.

(2) 정보통신서비스 부문 매출액이 300억 원 이상인 경우

- 정보통신서비스 부문 매출액이 300억 원 이상이더라도 자체 서비스 제공을 위한 주요 정보통신설비를 보유하지 않은 중기업의 경우 인증의 특례 대상에 해당한다.
  - 다른 법인이 제공하는 웹호스팅 서비스 또는 클라우드 서비스를 이용함에 따라 별도 서버(VM, EC2 등 가상서버를 포함)가 없거나, 서버 운영체제(Windows, Linux 등), 데이터베이스시스템(Oracle, MS-SQL 등)에 대한 관리 책임이 없는 경우*를 의미한다.

    * 시스템 default 계정(root/administrator) 접근권한, 취약점 및 패치관리 등
  - 외부 서비스망 연결 또는 내부 시스템 운영을 위해 정보통신설비(외부 IDC, 클라우드 서비스 등)는 주요 정보통신설비에 해당하지 않는다.

- 웹호스팅 서비스 또는 클라우드 서비스(SaaS, PaaS)를 이용하는 경우 ISMS, ISMS-P, CSAP 인증을 취득한 서비스를 이용하여야 한다.
- 단, ISP, IDC, 상급 종합 병원, 대학교, 금융회사, 가상자산사업자는 특례 대상에서 제외한다.

1.5. 인증 대상별 유의사항

- 인증 의무대상자 중 정보통신망서비스제공자와 집적정보통신시설 사업자는 매출액 및 이용자 수와 관계없이 인증 의무대상자에 해당된다.
  - 단, 집적정보통신시설의 일부를 임대하여 서비스를 재판매하는 사업자(VIDC)는 매출액 및 이용자 수 기준을 따른다.
- 인증 의무대상자 기준 중에서 「정보통신망법」 제47조제2항의 어느 한 가지 이상의 기준에 해당할 경우, 인증 의무대상자가 된다.
- 인증 의무대상자는 법에서 정한 인증 의무대상자 기준에 해당하는지 여부를 스스로 확인하여 인증을 받아야 하며, 의무대상자임에도 불구하고 인증을 취득하지 않는 경우 과태료 부과 대상이 될 수 있다.
- 예비인증 신청기관은 정보보호 관리체계 구축 후 시험운영 결과를 토대로 준비사항을 제출하여야 한다.
- 인증의 특례에 따라 인증심사를 수행하고자 하는 경우, 신청기관은 중소기업 확인서, 정보통신서비스 부문 매출액 자료, 주요 정보통신설비 미보유 증명 자료 등의 서류를 함께 제출하여 스스로 인증의 특례 대상임을 증명하여야 한다.
- 구축 및 운영에 필요한 소요기간을 확인하여 인증심사에 차질이 없도록 준비해야 한다.
  - 준비부터 인증취득까지는 약 6개월 이상이 소요되고, 인증 신청을 위해서는 최소 2개월 이상의 운영 기간이 필요하다.

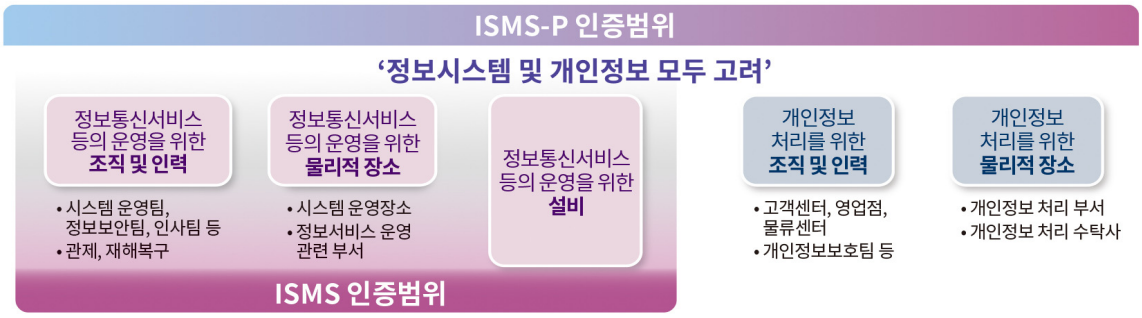
[표 10] 인증 절차 및 단계별 소요기간

	① 준비		② 심사					③ 인증	
인증 절차 내용	ISMS 구축	인증 신청	심사 준비	인증 심사	보완 조치	조치 확인	심사 결과 보고서 작성	인증 위원회 심의	인증 위원회 심의 및 인증서 교부
소요 기간	2개월 이상	심사 8주 전	심사 6주 전	1~2주	100일 이내		30일 이내	1일	인증 위원회 심의· 의결 후 2주 이내

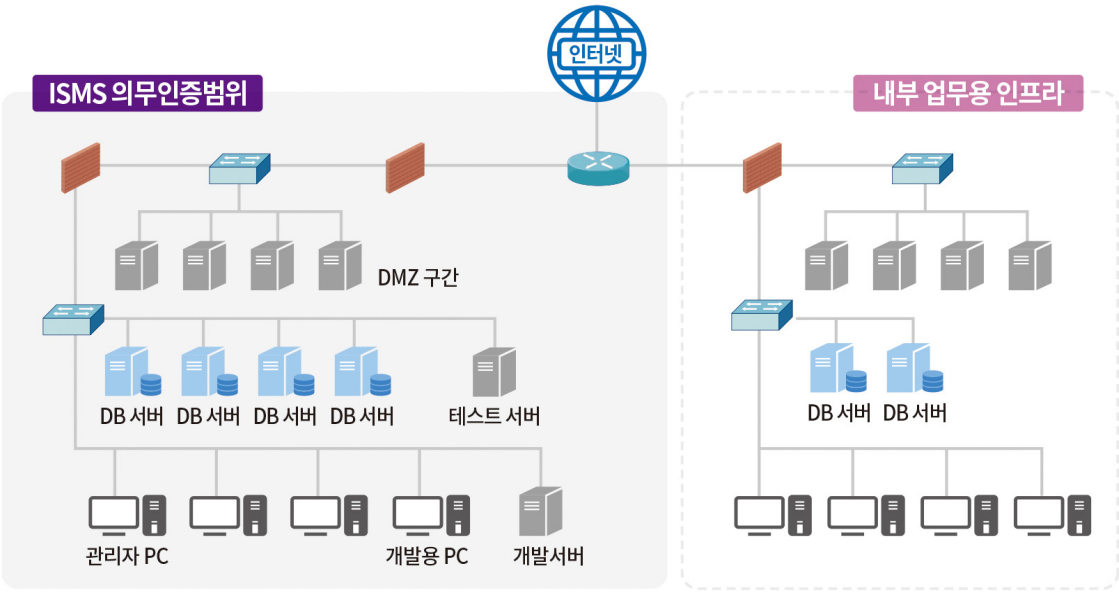
※ 신청기관의 규모 및 인증범위, 결함사항의 보완조치 확인, 인증위원회 인증결정 여부 등에 따라 소요기간이 변동될 수 있음

2 ISMS-P 인증범위

2.1. ISMS의 인증범위



- 일반적으로 ISMS 인증범위는 정보통신서비스를 기준으로 관련된 정보시스템, 장소, 조직 및 인력을 포함하게 된다. 반면에 ISMS-P 인증범위는 이에 더하여 해당 서비스에서 처리되는 개인정보의 흐름에 따라 해당 개인정보를 처리하는 정보시스템, 조직 및 인력, 물리적 장소 등을 모두 포함하여야 한다.
- 이에 따라 ISMS 인증 의무대상자가 ISMS 의무인증 범위를 포함하여 ISMS-P 인증을 신청하는 경우 ISMS-P 단일심사로 진행 가능하며 또한 ISMS 의무인증 범위에 대해서는 ISMS 인증을 신청하고 일부 서비스에 대해서는 개인정보 영역을 포함한 ISMS-P 인증을 신청하여 2개의 심사를 동시에 진행하는 것도 가능하다.



〈그림 8〉 ISMS 인증범위 설정(예시)

2.1.1. 의무대상자 인증범위 기준

- 인증 의무대상자인 경우, 인증범위는 신청기관의 정보통신서비스를 모두 포함하여 설정해야 한다.
  - 정보통신서비스란 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 서비스를 말한다.
  - 인증범위는 신청기관이 제공하는 정보통신서비스를 기준으로, 해당 서비스에 포함되거나 관련 있는 자산(시스템, 설비, 시설 등), 조직 등을 모두 포함하다.
  - 해당 서비스의 직접적인 운영 및 관리를 위한 백오피스 시스템은 인증범위에 포함되며, 해당 서비스와 관련이 없더라도 그 서비스의 핵심정보자산에 접근 가능하다면 포함한다.
  - ISMS 의무인증범위 내에 있는 서비스, 자산, 조직(인력)을 보호하기 위한 보안시스템은 인증범위에 모두 포함한다.
  - 정보통신서비스와 직접적인 관련성이 낮은 전사적자원관리시스템(ERP), 분석용데이터베이스(DW), 그룹웨어 등 기업 내부 시스템, 영업/마케팅 조직은 일반적으로 인증범위에서 제외한다.

2.1.2. 서비스 유형별 인증범위

- 인증범위를 설정하기 위해서는 신청기관이 제공하는 정보통신서비스를 분류하고, 해당 서비스를 위한 자산 및 조직을 모두 식별해야 한다.
  - 인증범위 대상으로 식별된 모든 자산 및 조직에 대해 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제23조에 따른 [별표 7] '가. 관리체계 수립 및 운영'과 '나. 보호대책 요구사항'을 준수하여 보호조치를 취해야 한다.
- 정보통신망서비스제공자(ISP)

인증범위	설명
서비스	전국망(서울특별시 및 모든 광역시)을 통한 정보통신망 서비스
설비	IP기반의 인터넷 연결을 위한 정보통신설비 및 관련 서비스를 제공하기 위한 정보통신설비

- 집적정보통신시설사업자(IDC 사업자)

인증 범위	설명
서비스	정보통신서비스를 제공하는 고객의 위탁을 받아 컴퓨터 장치 및 정보시스템을 구성하는 일정한 공간에 집중하여 시설을 운영·관리하는 서비스(공간 임대서비스, 서버호스팅, 네트워크 서비스 등)
설비	집적정보통신시설의 관리운영 용도로 설치된 컴퓨터 장치 및 네트워크 장비 등의 정보통신설비

■ 전년도 매출액, 이용자 수 등이 「정보통신망법」 및 시행령 기준에 해당하는 자

인증범위	설명
서비스	불특정 다수의 이용자가 접근 가능한 모든 정보통신서비스
설비	해당 정보통신서비스의 제공 또는 운영을 위해 필요한 정보통신설비

▶ 정보통신서비스 부문 매출액 또는 일일평균 이용자 수 요건에 해당하여 의무대상으로 포함된 경우는 정보통신서비스가 외부 정보통신망을 통해 접근 가능한지의 여부에 따른 의무 심사범위를 구분할 수 있다.

[표 11] 외부 정보통신망 공개 여부에 따른 의무 심사범위

인터넷 공개여부	설명	의무 범위
공개	- 외부 정보통신망을 통해 불특정 다수 또는 권한을 가지고 있는 자가 직접적으로 접근이 가능한 서비스 - 인증 의무대상인 신청기관이 다수의 정보통신서비스를 운영하는 경우, 개별 정보통신서비스가 인증 의무대상에 포함되지 않아도 모두 인증범위에 포함 - IP주소 제한을 통해 특정 위치 및 단말에서만 접속이 가능하도록 접근제어가 되어 있다 하더라도, 외부 정보통신망을 통해 직접 연결이 되어 있다면 인증범위에 포함 - 웹기반 서비스 뿐 아니라, 모바일 기반 서비스도 동일한 기준이 적용됨	○
미공개	- 외부 정보통신망을 통해 직접 접속이 불가능한 내부용 서비스	×

▶ 영리를 목적으로 하지 않더라도 정보통신망을 통해 정보를 제공하거나 정보의 제공을 매개하는 서비스는 모두 인증범위에 포함한다.

[표 12] 심사 의무대상자 정보통신서비스(예시)

유형	설명	예시
대표홈페이지	- 기업(기관)의 대표홈페이지	- 단순 홈페이지 포함
채용사이트	- 인터넷을 통하여 채용공고, 입사지원 등 채용 절차를 수행하는 시스템	- 온라인 채용시스템
비영리 사이트	- 비영리 목적으로 운영하는 인터넷 사이트	- 공익 사이트(자원봉사 등) - 학교 홈페이지(포털)
기타	- 임직원 복지를 위한 인터넷 시스템	- 임직원 복지몰
	- 기타 대외 서비스 및 업무처리를 위해 인터넷에 공개된 시스템	- 인터넷 방문예약 - 인터넷 신문고 등

※ 단, 정보통신망에 공개되어 있는 경우에만 해당함

2.1.3. 시스템 유형별 인증범위 고려사항

- 응용프로그램(Application)
  - 정보통신망을 통해 이용자에게 직접 노출되거나 접점이 되는 응용시스템은 심사범위에 포함
  - 정보통신서비스의 제공 또는 운영을 위하여 직접적으로 관련된 서비스 제공시스템, 서비스 관리용 시스템, 백오피스 시스템 등은 심사범위에 포함
  - 정보통신서비스의 데이터베이스를 직접 이용하지 않고, 복제 등의 방법으로 별도 데이터베이스를 구성한 후 이를 분석, 마케팅 등의 용도로 사용하는 응용시스템(DW, CRM 등)은 심사범위에서 제외
  - 정보통신서비스 관련 이용자 상담, 문의 대응 등을 위해 콜센터를 운영하는 경우, 콜센터 관련 시스템(교환기, CTI, IVR 등)은 의무 심사범위에서 제외
  - 정보통신서비스와 직접적인 관련 없이 내부업무 처리가 주목적인 그룹웨어, ERP 등은 심사범위에서 제외
- 데이터베이스(Database)
  - 인증 대상 서비스 및 응용시스템을 위해 필요한 데이터가 저장·관리되는 데이터베이스는 심사범위에 포함(회원DB, 운영DB, 백업DB 등)
- 서버(Server)
  - 인증범위에 포함된 서비스 및 응용시스템이 설치되어 운영되는 서버는 심사범위에 포함(운영서버, 연계서버 등)
  - 인증범위에 포함된 서비스 및 응용프로그램의 개발 및 운영·보안 관리를 위해 필요한 서버는 심사범위에 포함(개발서버, 시험서버, 형상관리서버, 모니터링서버, 백업서버, 로그서버, 보안관리서버, 패치관리서버 등)
  - 임대장비 등 소유자가 해당 기업이 아니더라도, 데이터 등 실질적인 운영 또는 서비스에 이용(지배권 소유)하고 있는 경우에는 심사범위에 포함
- 네트워크(Network) 장비
  - 인증 대상 서비스와 직접적으로 관련된 네트워크 장비는 모두 포함(DMZ 등 정보통신서비스 구간에 설치된 네트워크 장비 등)
  - 인증범위에 포함된 정보자산(응용시스템, 서버, 보안시스템 등) 및 물리적 시설(전산실 등)의 연결 및 구성을 위한 네트워크 장비는 포함
  - 인증범위에 포함된 조직 및 인력이 인터넷 사용, 원격접속 등을 위해 필요한 네트워크 장비는 포함
  - 단, 별도의 보안설정 없는 더미(Dummy) 역할을 하는 스위치는 심사범위에서 제외 가능
- 정보보호시스템(Security System)
  - 내·외부 침해로부터 인증 대상 서비스 및 관련 자산을 보호하기 위한 정보보호시스템은 심사범위에 포함
  - 인증범위에 포함된 조직 및 인력을 대상으로 적용된 정보보호시스템은 심사범위에 포함(DRM, DLP, PC보안, 백신, 패치관리시스템 등)

■ 클라우드서비스 이용 시

▶ 신청기관이 클라우드서비스를 이용하여 정보통신서비스를 제공하는 경우, 신청기관이 관리 가능한 운영체제, DB, 응용프로그램 등은 인증범위에 포함

▶ 단, 클라우드서비스 형태에 따라 심사범위가 달라질 수 있으므로 관리 범위, 지배권 소유 여부, 책임 소재 등에 따라 심사범위를 판단해야 함

[표 13] 클라우드서비스 형태에 따른 심사범위(예시)

구분	대상 서비스 및 자산	심사 범위
IaaS (Infrastructure as a Service)	- 신청기관이 직접 관리하는 서버OS(Guest OS), 미들웨어(WAS 등), 응용프로그램, DBMS	○
PaaS (Platform as a Service)	- 신청기관이 직접 관리하는 응용프로그램 - 단, 클라우드서비스 제공자로부터 계정 및 권한을 할당받아 사용하는 영역은 인증범위에 포함(미들웨어 계정·권한 및 비밀번호 등)	○
SaaS (Software as a Service	- 응용프로그램 관련하여 신청기관이 관리 가능한 영역에 한해 심사 수행(응용프로그램 계정·권한 관리 및 비밀번호 등)	○

※ 국내 및 해외 클라우드서비스 모두 해당 범위에 포함됨

※ 클라우드서비스 이용 시 안전성 및 신뢰성이 검증된 클라우드서비스 제공자를 이용할 것을 권고함

2.1.4. 세부 업종별 인증범위

세부 업종별 인증범위 예시는 업종별로 반드시 인증범위에 포함해야 하는 범위를 나타낸 것이며, 본 사례에 포함되지 않았다고 해서 인증범위에서 제외된다는 의미는 아님

■ 정보통신망서비스제공자(ISP) 인증범위(예시)

대분류	중분류	소분류	
ISP	유선	인터넷 접속서비스	
		인터넷 전화(VoIP)	
		인터넷 프로토콜 TV(IPTV)	
		전용 회선	
		유선 전화	시내/시외 전화
			국제전화

대분류	중분류	소분류	
			구내전화
			지능망서비스
			문자서비스
	무선	이동통신	2G
			3G/4G(LTE)
			5G

- 인터넷 접속 서비스 : 초고속 인터넷서비스, 전화선 또는 광대역 연결(케이블 또는 DSL 등)을 사용한 인터넷서비스
- 인터넷전화(VoIP) : 인터넷망을 통해 제공되는 전화서비스
- 인터넷 프로토콜 TV(IPTV) : 디지털 방송서비스, VOD서비스
- 전용회선 : 기업 등을 대상으로 제공되는 IP기반 전용망서비스
- 이동통신서비스(무선) : 모바일 등을 이용한 음성통화, 데이터통신서비스

■ 집적정보통신시설사업자(IDC) 인증범위(예시)

대분류	소분류
집적정보통신시설 사업자 (IDC)	코로케이션(Co-location)
	네트워크 제공 서비스(회선 임대 포함)
	호스팅서비스
	클라우드서비스
	보안관제서비스
	CDN서비스
	재해복구서비스

- 코로케이션서비스(Co-location) : IT시스템을 설치·운영할 수 있는 상면 공간 임대 및 전기, 시설, 설비 등 관리서비스
- 네트워크 제공 서비스(회선 임대) : 인터넷 네트워크 회선을 제공하는 서비스
- 호스팅서비스 : 인터넷 비즈니스를 위해 필요한 서버, 네트워크, 스위치, 스토리지 등을 임대하거나 운영을 대행하는 서비스
- 클라우드서비스 : 클리우드 기반의 IT 인프라 통합 운영·관리 서비스
- 보안관제서비스 : 서버 및 네트워크 보호를 위한 실시간 모니터링 및 분석서비스
- CDN서비스 : 인터넷 서비스 제공자에 직접 연결하여 콘텐츠 전송 네트워크 제공 서비스

■ 인터넷 쇼핑 인증범위(예시)

구분	설명
통신판매 (인터넷 상품판매)	- 인터넷 등을 이용하여 재화 또는 용역의 판매에 관한 정보를 제공하고 소비자의 청약을 받아 재화 또는 용역을 판매
통신판매 중계 (오픈마켓)	- 사이버몰(컴퓨터 등과 정보통신설비를 이용하여 재화 등을 거래할 수 있도록 설정된 가상의 영업장)의 이용을 허가하는 등의 방법으로 거래 당사자 간의 통신판매를 알선
MRO 쇼핑몰	- 기업에서 제품 생산과 직접 관련된 원자재를 제외한 소모성 자재를 인터넷을 통해 거래
임직원 몰	- 임직원 대상 쇼핑몰 ※ 인터넷을 통해 외부에서 접근 가능한 경우에 인증대상

■ 인터넷 게임 인증범위(예시)

구분	설명
게임 포털 (퍼블리싱)	- 게임 포털서비스 제공 - 퍼블리싱서비스
게임 개발사	- 자체 게임에 대한 개발, 운영을 모두 하는 경우

※ 순수하게 게임 개발만을 하는 개발사나 단순 채널링 되는 서비스는 인증 의무 범위 아님

- 퍼블리싱서비스 : 자체 포털을 이용하여 타사에서 개발한 게임을 운영 대행
- 자체 게임 개발 : 자체 시스템을 이용하여 게임 개발 및 운영

■ 의료 분야 인증범위(예시)

구분	설명	
의료정보 시스템	EMR	전자의무기록(Electronic Medical Record), 진료, 진료지원, 원무 등 병원 업무 전반을 포괄하는 시스템
	OCS	처방전달시스템(Order Communication System), EMR과 별도의 OCS 운영할 경우 포함
원격의료 시스템	u-헬스케어 등	컴퓨터, 화상통신 등 정보통신 기술을 활용하여 먼 곳에 있는 의료인에게 의료지식이나 기술을 지원하는 의료 활동
홈페이지	정보 제공	의료 기관 소개, 이용안내, 건강정보 제공 등
	진료 예약/조회	온라인 진료 예약, 현황 조회 등
	진단검사 결과 조회	혈압, 혈당, 맥박, 키, 체중 등 건강진단 검사 결과 조회
	증명서 발급/출력	진단서, 소견서, 입원사실증명서, 의료비 납입증명서 등
	기타	온라인 상담, 민원 처리 등

■ 대학 분야 인증범위(예시)

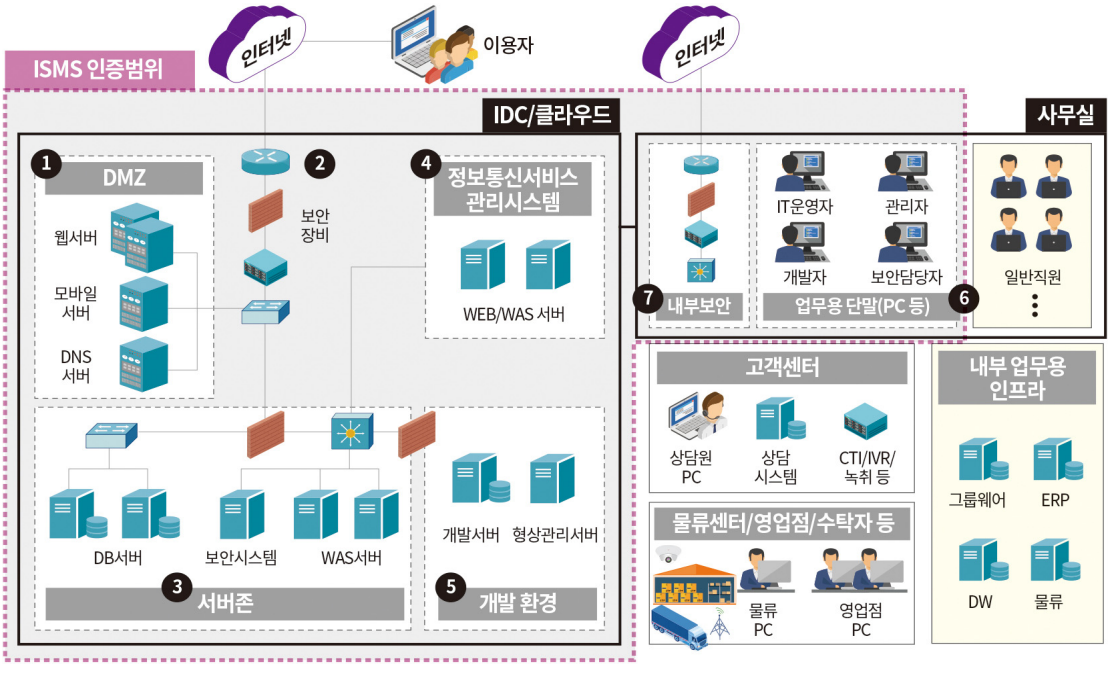
구분	설명	
학사 정보 시스템	포털	학사정보 관련 학생 및 교직원 포털 등
	교무	학사일정, 학과관리, 교육과정 관리 등
	학적관리	학적 기초정보, 신입학/등록, 진급, 전공/부전공/복구전공, 동문, 휴복학, 제적 등
	수업/수강 관리	교육과정, 수업개설, 수강신청, 학기운영, 교·강사 관리, 강의실 관리 등
	장학/등록 관리	등록금, 대상자 관리, 수납, 정산, 장학 기초정보, 장학생관리, 학자금 관리 등
	성적관리/증명서	제증명 발급 및 관리, 성적관리, 강의평가, 시험관리 등
	교직관리	기본정보, 교직이수 관리, 교직사정, 교육실습 등
	졸업/취업	졸업기준, 졸업대상자, 취업정보, 채용 관리, 취업상담 등

■ 금융 분야 인증범위(예시)

구분	설명
은행	인터넷 뱅킹(웹/모바일)을 포함하여 인터넷에서 접근 가능한 대고객 서비스
증권	트레이딩 시스템 (HTS/MTS/WTS)을 포함하여 인터넷에서 접근 가능한 대고객 서비스
보험	다이렉트 보험을 포함하여 인터넷에서 접근 가능한 대고객 서비스
카드	카드 홈페이지를 포함하여 인터넷에서 접근 가능한 대고객 서비스

※ 단, 금융 분야는 ISMS 의무대상에서 제외되므로 자율적으로 인증범위 설정이 가능함

2.1.5. 정보통신서비스 매출액·이용자 수 기준 ISMS 의무대상자 인증범위 설정



〈그림 9〉 ISMS 인증의무자 인증범위 설정(예시)

■ 정보통신서비스 부문 매출액 또는 이용자 수 기준으로 ISMS 의무대상자로 지정된 경우 다음과 같이 ISMS 인증범위를 설정할 수 있다.

▶ 단, 클라우드서비스를 이용하여 정보통신서비스를 제공하는 경우, 클라우드서비스 유형(IaaS, PaaS, SaaS) 등에 따른 책임 범위에 따라 신청기관이 직접 관리 가능한 영역에 대한 인증범위 포함이 필요하다.

[표 14] ISMS 인증범위 설정(예시)

구분	영역	설명
❶	DMZ	– 영리 여부와 상관없이 정보통신망에 공개되어 정보통신망을 통해 정보를 제공하거나 정보의 제공을 매개하는 서비스 및 관련 서버는 모두 포함 · 서비스 예시: 대표 홈페이지, 인터넷 쇼핑몰, 이용자 포털, 인터넷 채용사이트 등 · 서버 예시: 웹서버, 모바일서버, WAS서버, API서버, 연계서버, 스트리밍서버, DNS 서버 등 – 모바일 서비스가 존재하는 경우 해당 모바일 서비스 및 관련 서버도 모두 포함
❷	네트워크 및 보안 시스템	– 정보통신서비스를 위한 인터넷 구간 및 서버 구간의 네트워크시스템과 보안시스템은 모두 포함 · 네트워크시스템 예시 : 라우터, 스위치(L2, L3, L4, L7 등), TACACS, NMS 등 · 보안시스템 예시 : 방화벽, IPS/IDS, VPN, WAF(웹방화벽), DDoS 대응장비, ESM 등
❸	서버존	– 인증범위에 포함된 서비스와 관련된 서버 및 데이터베이스는 모두 포함 · 서버 예시: WAS서버, API서버, 연계서버, 백업서버, 로그서버, LDAP서버 등 · 데이터베이스 예시: 인터넷 회원DB, 온라인 구매DB, 온라인 채용DB 등 – 인증범위 내 서버 및 데이터베이스를 보호하기 위한 보안시스템도 모두 포함 · 보안시스템 예시: DB접근제어, 서버접근제어, SIEM, 통합계정관리(IM) 등
❹	정보통신서비스 관리시스템	– 인증범위에 포함된 서비스의 직접적인 운영·관리를 위해 내부 사용자 등이 접속하여 사용하는 관리시스템, 백오피스시스템 등은 모두 포함 · 관리시스템 예시: 인터넷 회원관리시스템, 온라인 쇼핑몰 백오피스시스템, 모니터링시스템(성능·용량 등) 등 – 해당 관리시스템과 관련된 웹서버, WAS서버, DB서버 등도 인증범위에 포함
❺	개발 환경	– 인증범위에 포함된 서비스 및 어플리케이션 개발과 관련된 시스템 및 장비는 모두 포함 · 개발환경 예시: 개발서버, 테스트서버, QA서버, 스테이징서버, 형상관리시스템, 개발DB, 테스트DB, 개발존 방화벽, 테스트데이터 변환시스템 등
❻	업무 환경 (업무용 PC 등)	– 인증범위에 포함된 서비스를 운영, 관리, 개발하기 위한 조직 및 인력들이 사용하는 업무용 단말 (PC, 스마트기기 등)은 인증 범위에 포함 – IT운영자, 정보통신서비스 관리시스템의 관리자 및 사용자, 정보통신서비스 관련 개발자, 보안 시스템 관리자 및 운영자 등이 관련 조직 및 인력에 해당됨 – 그 외 인력들이 사용하는 업무용 단말은 인증범위에서 제외됨

구분	영역	설명
❼	내부용 네트워크 및 보안 시스템	– 인증범위에 포함된 조직 및 인력이 인터넷 사용, 원격 접속, 유·무선 네트워크 접속 등을 위해 필요한 네트워크 장비 및 보안시스템은 인증 범위에 포함 · 네트워크시스템 예시: 인터넷 라우터, 백본 스위치, L2 스위치 등 · 보안시스템 예시: 방화벽, 차세대방화벽, IDS/IPS, WIPS, APT대응시스템, 스팸차단, 바이러스월, SSL VPN, IPSec VPN, NAC 등 ※ 별다른 보안설정 없이 더미(Dummy) 역할을 하는 스위치는 인증범위에서 제외 가능 – 인증범위에 포함된 조직 및 인력에 대대 보안통제 등의 목적으로 적용된 정보보호 시스템은 인증범위에 포함 · 보안시스템 예시: DRM, DLP, 백신, PC보안, PMS(패치관리시스템), 보안USB 등 ※ S/W형태의 보안솔루션인 경우, 관리용 서버 포함 – 인터넷 망분리가 적용된 경우, 물리적 또는 논리적 망분리와 관련된 시스템은 인증범위에 포함 · 망분리 관련 시스템 예시 : 물리적 폐쇄망 구성 장비, VDI 서버, 망연계 시스템 등 – 인증범위 내에 자체적으로 보유한 보호구역(전산실, 운영실 등)이 존재하는 경우 이에 대한 물리적· 환경적 보호를 위한 보호설비는 인증범위에 포함 · 보호설비 예시 : 출입통제시스템, DVR/NVR, 항온항습기, 소화설비 등 ※ 단, 자체적으로 보유한 시설 및 설비가 없는 경우 제외될 수 있음

의무대상자 범위 설정 팁

- 먼저 신청기관이 운영하고 있는 서비스 목록들을 나열
- "2. ISMS-P 인증범위" 내용을 참고하여 의무로 인증을 받아야 하는 서비스를 선정
- 각 서비스 별로 조직범위를 선정함. 조직범위 선정 시, 각 서비스의 개발·운영 조직(여기서의 운영은 서버 관리, 네트워크·보안장비 관리 등 시스템적 운영을 말함)을 포함
- 각 서비스의 정보통신 설비(서버, 네트워크시스템, 보안시스템 등)범위를 포함
- 신청기관의 정보보호 조직(직무자), 인적 보안 관련 직무자, 물리적 보안 관련 직무자, 관리체계 점검 수행 인력 등을 포함
- 본 안내서의 내용만으로 모호한 부분이 있으면, 인증·심사기관에 전화(메일) 또는 방문 상담 가능
- 최종적인 인증범위 내의 정보통신 설비 수, 인원 수는 인증심사팀의 예비점검 시 확정

※ 본 안내서 "2.1.4 세부 업종별 인증범위"는 일반적으로 인증범위에 포함해야 할 범위를 나열한 것임. 따라서 여기 나열된 시스템만 의무 인증범위로 해서는 안되며, "2.1.1 의무대상자 인증범위 기준", "2.1.2 서비스 유형별 인증범위" 내용을 토대로 인증범위를 설정해야 함

2.2. ISMS-P의 인증범위

2.2.1. ISMS-P 인증범위 설정 시 고려사항

- '개인정보 처리단계별 요구사항'을 포함하는 ISMS-P 인증은 의무사항이 아니므로, 신청기관이 자율적으로 인증을 받고자 하는 서비스를 지정하여 인증을 신청할 수 있다.
  - 인증 받고자 하는 서비스의 범위는 이용자 중심의 대외 서비스만 포함할 것인지 임직원이 이용하는 내부 서비스까지 포함할 것인지에 대해서 고려하여야 한다.
  - 다만, ISMS 인증 의무대상자가 ISMS-P 인증으로 대체하고자 하는 경우 ISMS-P 인증범위에는 ISMS 인증범위를 반드시 모두 포함하여야 한다.

[표 15] ISMS-P 인증대상 서비스(예시)

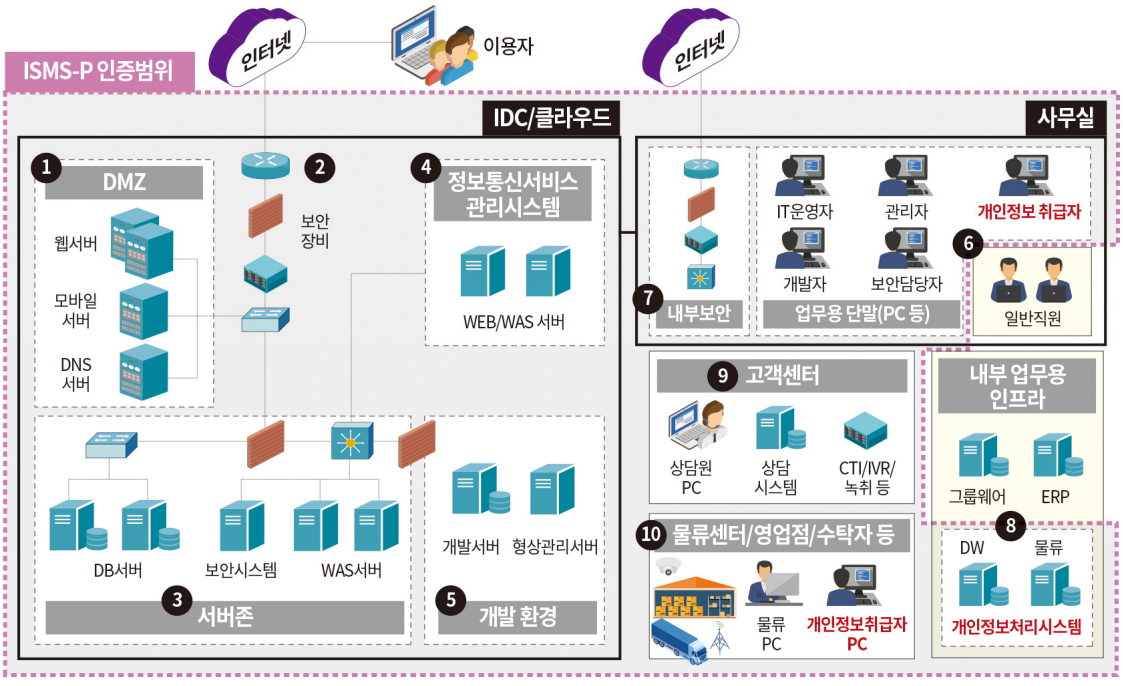
서비스 유형	서비스
대국민 또는 이용자 대상 서비스	- 인터넷 포털서비스 - 인터넷 쇼핑몰서비스 - 온라인 게임서비스 - 고객 멤버십서비스 - 대국민 온라인 민원서비스 등
임직원 또는 사내 서비스	- 출입통제서비스 - 인사·노무 관리서비스 - 재무회계서비스 - 임직원 복지몰서비스 등

- 인증을 받고자 하는 서비스 내 개인정보 처리 관련 업무를 상세하게 분석하고 개인정보의 Life-Cycle (수집·보유·이용·제공·폐기)에 따른 개인정보 흐름을 고려하여 관련된 모든 업무와 정보시스템을 식별하여야 한다.
  - 온라인 또는 오프라인 여부와 상관없이 인증을 받고자 하는 서비스에서 처리되는 개인정보를 중심으로 관련된 모든 업무 및 정보시스템을 식별하여야 한다.
- 정보시스템 및 개인정보를 모두 고려하여 서비스를 운영하기 위한 조직 및 인력, 정보시스템, 물리적 장소, 수탁자 등을 파악하고 인증범위를 설정한다.
  - ISMS-P 인증을 취득하기 위해서는 ISMS 인증에 해당하는 인증기준을 기본적으로 만족해야 하므로 '2.1 ISMS의 인증범위'를 참고하여 범위를 설정한 후 이에 더하여 개인정보 처리단계와 관련된 범위를 설정하여야 한다.

[표 16] ISMS-P 인증범위(예시)

인증 범위	설명
서비스 및 개인정보처리를 위한 조직 및 인력	개인정보보호팀, 시스템운영팀, 정보보안팀, 인사팀, 관제팀, 재해복구 관련 조직 등
개인정보 처리를 위한 조직 및 인력	고객센터, 영업점, 물류센터 등
서비스 운영을 위한 장소	사내 전산실, IDC 등 시스템 운영 장소, 정보서비스 운영관련 부서 사무실 등
개인정보 처리를 위한 물리적 장소	개인정보 취급 부서, 개인정보 취급 수탁사 등
서비스 및 개인정보 처리를 위한 정보시스템	개인정보처리시스템, 네트워크, 서버, 보안시스템, 응용프로그램, DBMS 등

2.2.2. ISMS-P 인증범위 설정



〈그림 10〉 ISMS-P 인증범위 설정(예시)

- ISMS-P는 인증대상이 되는 서비스를 중심으로 개인정보의 흐름에 따라 해당 개인정보 처리와 관련된 모든 정보시스템(개인정보처리시스템 등) 및 조직·인력을 인증범위에 포함하여야 한다.
  - 단, 클라우드서비스를 이용하여 서비스를 제공하는 경우, 클라우드 서비스 유형(IaaS, PaaS, SaaS) 등에 따른 책임 범위에 따라 신청기관이 직접 관리 가능한 영역에 대하여 인증범위에 포함한다.

[표 17] ISMS-P 인증범위 설정(예시)

구분	영역	설명
❶	DMZ	- 인증을 받고자 하는 서비스와 관련된 웹 사이트 및 관련 서버는 모두 포함 · 웹사이트 예시: 인터넷 포털사이트, 온라인 쇼핑몰사이트, 판매자사이트 등 · 서버 예시: 웹서버, 모비일서버, WAS서버, API서버, 연계서버, 스트리밍서버, DNS서버 등 - 모바일서비스가 존재하는 경우 해당 모바일서비스 및 관련 서버도 모두 포함 - 대용량 메일발송서버, 모바일 앱 푸시서버 등 개인정보가 처리되는 서버는 모두 포함 - 정보통신망에 공개되어 있더라도 인증을 받고자 하는 서비스와 관련 없는 웹사이트 및 서버는 제외 가능(예를 들어, 온라인 쇼핑몰서비스에 대하여 ISMS-P 인증을 받고자 하는 경우 인터넷 채용사이트 등 쇼핑몰 이용자의 개인정보 처리와 무관한 사이트는 제외 가능)
❷	네트워크 및 보안 시스템	- 인증을 받고자 하는 서비스를 위한 인터넷 구간 및 서버 구간의 네트워크시스템과 보안시스템은 모두 포함 · 네트워크시스템 예시: 라우터, 스위치(L2, L3, L4, L7 등), TACACS, NMS 등 · 보안시스템 예시: 방화벽, IPS/IDS, VPN, WAF(웹방화벽), DDoS대응장비, ESM 등
❸	서버존	- 인증범위에 포함된 서비스와 관련된 서버 및 데이터베이스는 모두 포함 · 서버 예시: WAS서버, API서버, 연계서버, 백업서버, 로그서버, LDAP서버 등 · 데이터베이스 예시: 인터넷 회원DB, 온라인 구매DB, 온라인 채용DB 등 - 인증범위 내 서버 및 데이터베이스를 보호하기 위한 보안시스템도 모두 포함 · 보안시스템 예시: DB접근제어, 서버접근제어, SIEM, 통합계정관리(IM) 등
❹	정보통신 서비스 관리시스템	- 인증범위에 포함된 서비스의 운영·관리를 위해 내부 사용자 등이 접속하여 사용하는 관리시스템, 백오피스시스템 등은 모두 포함 · 관리시스템 예시: 인터넷 회원관리시스템, 온라인 쇼핑몰 백오피스시스템, 모니터링 시스템(성능·용량 등) 등 - 해당 관리시스템과 관련된 웹서버, WAS서버, DB서버 등도 인증범위에 포함 - 인증범위에 포함된 서비스와 관련된 개인정보를 처리하는 정보시스템(개인정보처리시스템)은 모두 포함
❺	개발 환경	- 인증범위에 포함된 서비스 및 어플리케이션 개발과 관련된 시스템 및 장비는 모두 포함 · 개발환경 예시: 개발서버, 테스트서버, QA서버, 스테이징서버, 형상관리시스템, 개발DB, 테스트DB, 개발존 방화벽, 테스트데이터 변환시스템 등
❻	업무 환경 (업무용 PC 등)	- 인증범위에 포함된 서비스를 운영, 관리, 개발하기 위한 조직 및 인력들이 사용하는 업무용 단말(PC, 스마트기기 등)은 인증범위에 포함 - IT운영자, 정보통신서비스 관리시스템의 관리자 및 사용자, 정보통신서비스 관련 개발자, 보안시스템 관리자 및 운영자 등이 관련 조직 및 인력에 해당됨 - 인증범위에 포함된 서비스와 관련된 개인정보를 조회, 입력, 변경, 삭제, 저장, 출력 등 업무상 취급하는 인력(개인정보취급자) 및 해당 인력이 사용하는 업무용 단말은 인증범위에 포함 - 그 외 인력들이 사용하는 업무용 단말은 인증범위에서 제외됨

구분	영역	설명
❼	내부용 네트워크 및 보안 시스템	- 인증범위에 포함된 조직 및 인력이 인터넷 사용, 원격 접속, 유·무선 네트워크 접속 등을 위해 필요한 네트워크 장비 및 보안시스템은 인증범위에 포함 · 네트워크시스템 예시: 인터넷 라우터, 백본 스위치, L2 스위치 등 · 보안시스템 예시: 방화벽, 차세대방화벽, IDS/IPS, WIPS, APT대응시스템, 스팸차단, 바이러스월, SSL VPN, IPSec VPN, NAC 등 ※ 별다른 보안설정 없이 더미(Dummy) 역할을 하는 스위치는 인증범위에서 제외 가능 - 인증범위에 포함된 조직 및 인력에 대해 보안통제 등의 목적으로 적용된 정보보호 시스템은 인증범위에 포함 · 보안시스템 예시: DRM, DLP, 백신, PC보안, PMS(패치관리시스템), 보안USB 등 ※ S/W형태의 보안솔루션인 경우, 관리용 서버 포함 - 인터넷 망분리가 적용된 경우, 물리적 또는 논리적 망분리와 관련된 시스템은 인증범위에 포함 · 망분리 관련 시스템 예시 : 물리적 폐쇄망 구성 장비, VDI 서버, 망연계 시스템 등 - 인증범위 내에 자체적으로 보유한 보호구역(전산실, 운영실 등)이 존재하는 경우 이에 대한 물리적·환경적 보호를 위한 보호설비는 인증범위에 포함 · 보호설비 예시 : 출입통제시스템, DVR/NVR, 항온항습기, 소화설비 등 ※ 단, 자체적으로 보유한 시설 및 설비가 없는 경우 제외될 수 있음
❽	내부 업무용 인프라	- 인증범위에 포함된 서비스와 직접적인 관련이 없으면서 인증범위 내 개인정보의 처리 없이 내부업무 처리가 주목적인 정보시스템은 인증범위에서 제외 가능 (그룹웨어, ERP 등) - 정보통신서비스의 데이터베이스를 직접 이용하지 않고 복제 등의 방법으로 데이터베이스를 구성한 후 이를 분석, 마케팅 등의 용도로 사용하는 정보시스템의 경우 인증범위 내 개인정보를 처리하므로 인증범위에 포함: DW, CRM, 빅데이터 분석시스템 등 - 인터넷에 공개되어 있지 않으면서 오프라인 영역의 비즈니스 및 업무를 위한 정보시스템도 인증범위 내 개인정보를 처리하는 개인정보처리시스템에 해당될 경우 인증범위에 포함: 매장관리시스템, 물류시스템 등
❾	고객센터	- 인증 범위에 포함된 서비스와 관련된 이용자 상담, 문의 대응 등을 위해 고객센터를 운영하는 경우 고객센터 관련 자산 및 시스템은 인증범위에 포함 : 교환기, CTI, IVR, 녹취시스템, 상담시스템, 팩스시스템, 상담원 PC 등
❿	물류 센터, 영업점, 개인정보 수탁사 등	- 오프라인 영역에서의 비즈니스 및 업무를 위한 물류센터, 영업점, 대리점, 매장 등이 인증범위 내 개인정보를 취급할 경우 인증범위에 포함: 관련 유·무선 네트워크 장비, 물리적 보안장비(CCTV 등), POS 시스템 및 단말기, 업무용 PC 등 - 개인정보 처리업무를 위탁한 수탁자의 경우 인증범위에 포함

제3장

ISMS-P 인증심사 절차

1. ISMS-P 인증 준비단계
2. ISMS-P 인증 심사단계
3. ISMS-P 인증단계
4. ISMS-P 사후관리 단계

1 ISMS-P 인증 준비단계

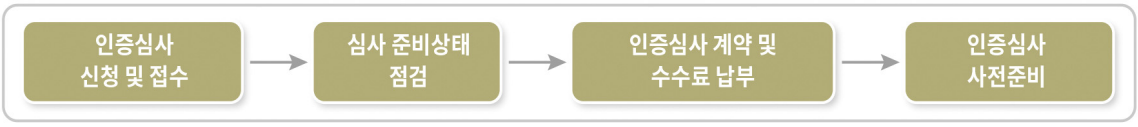
■ ISMS-P 인증심사의 전체 흐름은 다음 〈그림 11〉과 같다.

〈그림 11〉 ISMS-P 인증심사 절차

■ ISMS 인증 의무대상자의 인증 의무 취득기간(고시 제19조제4항, 부칙 제2조)

▶ ISMS 인증 의무대상자의 경우 '의무대상자'로 해당된 연도의 다음 해 8월 31일까지 인증을 취득해야 한다.

1.1. 인증심사 신청 및 접수



- 인증심사 신청 전 취득하고자 하는 인증의 종류에 따라 ISMS 혹은 ISMS-P 관리체계를 구축하고 최소 2개월 이상 운영한 증거자료를 준비하여야 한다.
- 인증심사 신청 시 다음의 서류들을 준비하여 인증 또는 심사기관에 제출한다.

☞ ISMS, ISMS-P 인증심사 신청서류

- 정보보호 및 개인정보보호 관리체계 인증신청 공문 1부
- 정보보호 및 개인정보보호 관리체계 인증신청서 1부
- 정보보호 및 개인정보보호 관리체계 운영현황 1부
- 정보보호 및 개인정보보호 관리체계 명세서 1부
- 법인/개인 사업자등록증 1부
- 법인등기부등본 1부

(참고) 인증의 특례에 따른 신청 시 추가 제출 서류

· 중소기업 확인서 1부
· 정보통신서비스 부문 매출액 자료 1부
· 주요 정보통신설비 미보유 증명 자료 1부

※ ISMS-P 인증신청서 및 명세서 양식은 인증정보를 제공하는 홈페이지(isms-p.kisa.or.kr)와 각 인증 또는 심사기관의 홈페이지에서 다운로드 가능

- 인증신청서류는 인증신청서에 안내된 이메일을 통해 제출할 수 있으며, 신청서류의 미비로 인증 또는 신청기관의 보완요청이 있을 경우 신청서류를 재구비하여 제출하여야 한다.

- 인증심사 신청 시 취득하고자 하는 인증에 따라 ISMS 단일 인증, ISMS-P 단일 인증, 다수 인증(ISMS & ISMS-P), 예비인증, 인증의 특례 중 하나를 정하여 신청할 수 있다.
  - 인증심사를 분할할 경우, 각각의 인증범위에 대하여 개별 인증신청서를 작성하고 개별 수수료를 산정하게 된다.
  - 인증을 받고자 하는 인증심사 대상 서비스가 여러 개 있는 경우 인증범위를 합치거나 분할하여 신청할 수 있으며, 인증범위를 분할할 경우, 각각의 인증범위에 대한 별도의 인증계약으로 수수료 등 추가 비용이 발생할 수 있다.

▶ 다수 인증(ISMS & ISMS-P)의 경우, 같은 관리체계 내에서 일부 서비스만 개인정보흐름을 포함하여 인증을 받고자 하는 경우로서 수수료와 심사과정을 통합하여 심사를 진행하게 되며 유효기간 및 심사주기가 동일하고 범위만 다른 2장의 인증서를 발급받게 된다.

☞ 유의사항

- 인증심사 신청부터 인증심사까지 예비점검, 계약, 심사원 모집 등 업무처리를 위한 기간이 필요하므로 희망 심사일 기준 최소 8주 전에 신청해야 함

1.2. 심사 준비상태 점검

■ 심사 준비상태 점검이란 심사팀장이 신청기관을 방문하여 정보시스템의 규모, 위험 식별 및 평가 수행 여부, 운영명세서 등 인증심사에 필요한 기초자료 구비 유무, 인증심사 준비상태 및 운영여부를 확인하는 것이다.

[표 18] 심사 준비상태 점검 시 주요 점검사항

점검 항목	세부 점검 사항
인증범위 적정성	• 전체 업무 및 인증범위 내 업무 확인 • 계약서 및 인증서 등에 반영될 인증 범위명 확인 • 인증범위 내 누락 정보자산 및 네트워크 구성 확인 ※ 정보보호 및 개인정보보호 관리체계 명세서, 운영명세서 기반으로 점검
조직(구성원) 현황	• 인증범위 내 업무, 조직 및 인원의 누락 여부 확인 • 정보보호 및 개인정보보호 전담조직 현황 확인
물리적 현황	• 인증범위 내 사무실, 전산실 등의 물리적인 위치(ISMS-P 인증의 경우 고객센터, 영업점, 물류센터 등 개인정보가 처리되는 물리적 위치 포함)
ISMS-P 운영 현황	• [정책] 정책체계 및 정책/지침/매뉴얼 운영 여부 확인 • [위험분석] 인증심사 전 위험분석 및 평가, 정보보호대책 수립 및 이행 여부 확인 • [관리체계 점검] 관리체계 점검 수행 여부 등 • [운영명세서] 운영명세서 작성 현황 및 N/A 항목 적정성 확인 • [이행증적] 관리체계 분야별 이행증적 존재 여부 확인 (2개월 이상)

■ 심사팀장은 예비점검을 통해 인증범위의 적정성, 인증심사 전 필수 수행사항 및 운영 현황 등을 확인하고 심사 진행 여부를 결정한다.

■ 심사 수행기관의 심사팀장은 신청기관의 정보보호최고책임자(CISO)와 개인정보보호책임자(CPO), 그리고 정보보호 및 개인정보보호 담당자와 예비점검 결과를 공유하고, 인증범위를 고려하여 심사일정을 확정한다.

1.3. 인증심사 계약 및 수수료 납부

- 심사진행이 결정된 이후 인증범위, 심사기간, 심사 인원, 심사팀 구성, 인증 수수료 등을 협의하고 관리체계 인증심사 계약을 체결한다.
- 인증심사 수수료는 신청기관이 인증 또는 심사기관에 납부하는 비용으로 인증심사 신청접수 및 계약, 예비점검, 현장심사, 보완조치 확인, 인증위원회 상정 등에 소요되는 제비용을 의미한다.
  - 인증범위 내 정보통신 설비 수, 인원 수, 수탁사 수 등을 기준으로 정보보호 관리체계 고시에 따라 직접인건비, 직접경비, 제경비, 기술료를 고려하여 산정한다.

[표 19] 인증심사 수수료 산정 가이드

구분		가이드
ISMS	정보통신 설비	• 범위 내 다음과 같은 서버, 네트워크 장비, 정보보호시스템 모두 포함 · 서버: 웹서버, 웹어플리케이션 서버(WAS), DB서버, APP 서버, DNS서버, 메일서버, 파일서버, 백업서버 등 · 네트워크 장비: 스위치(L4 이상), 라우터 포함 · 정보보호시스템: F/W, IPS, IDS, 웹방화벽, DLP, DRM, DB 접근제어 등 • 다음과 같은 경우 서버 수를 조정할 수 있음 · 장애 대응을 위해 서버, 네트워크 장비, 정보보호시스템 이중화 운영의 경우 1대로 산정 가능 · 로드밸런싱을 위해 다수의 서버를 운영하는 경우 1대로 산정 가능 ※ 다만 용도, OS 종류 및 버전, 소유자(관리자) 등 운영환경이 동일해야 함
	인원 수	• 범위 내 관련 조직 인원 모두 포함 ※ 내부 직원뿐만 아니라 인증범위 내 외부 인력(SM, SI 등)도 반드시 포함
ISMS-P	개인정보 수탁사 수	• 인증범위 내에서 사용되는 개인정보 수탁사 수
	개인정보 처리 서비스 수	• 개인정보를 수집하여 처리하는 서비스 수

- 신청기관은 인증심사 계약이 완료되면 계약에 따라 확정된 심사수수료를 인증심사 이전(계약 후 1개월 이내)에 완납해야 한다.
  - 인증정보를 제공하는 홈페이지(isms-p.kisa.or.kr)에 인증범위 내 정보시스템 수 및 인원 수를 기준으로 수수료 산정방법을 게시하고 있다.

    ※ 홈페이지 〉 ISMS-P(게시판) 〉 자료실 〉 'ISMS-P 인증수수료 산정내역서'

    ※ 인증·심사기관 홈페이지에서도 'ISMS-P 인증수수료 산정내역서' 확인 가능
  - 인증심사 전 수수료를 납부하지 않은 경우, 인증심사를 실시하지 않을 수 있다.

1.4. 인증심사 사전준비

- 인증심사 전 인증 또는 심사기관은 원활한 인증심사를 위해 심사계획을 수립하여 신청기관에게 안내한다.
  - 신청기관은 안내된 심사계획에 따라 심사장소, 심사대응 담당자 지정 및 심사 대응 협조 등을 사전에 준비해야 한다.

[표 20] 인증심사 전 세부 준비사항

구분	세부 내용	비고
심사 공간 확보	• 회의실(심사원 수×규모) • 빔프로젝트 및 화이트 보드 • 유선전화(내부 연락용) 및 네트워크 회선 • 기타 심사팀장이 별도로 요청한 사항	인증 심사원 수 고려
인증심사 자료 및 이행증거 자료 준비	• 각종 정책, 지침, 매뉴얼 • 정보보호 및 개인정보보호 관리체계 명세서, 운영명세서 • 자산목록대장, 네트워크 구성도 • 위험 식별 및 평가 보고서, 위험조치계획서 • 업무별 담당자 연락처	심사원별 1부
	• 인증기준별 증거 또는 이행자료 • 각종 점검 및 관리대장	원본1부, 사본1부
인적 준비사항	• 심사대응 담당자 지정, 주요 직무자 협조 요청 ※ 인증심사 기간 중 현장실사 및 인터뷰 대응, 추가자료 요청 대응 등 • 원격지에 대한 현장실사 일정 확보 • 기타 심사팀장이 별도로 요청한 사항	-

※ 출력물의 양이 많거나 여러 부를 준비하기 어려운 경우, 산출물 부수는 심사팀장과 협의하여 정할 수 있음

2 ISMS-P 인증 심사단계

2.1. 인증심사 시작회의

- 시작회의는 인증심사팀과 신청기관의 정보보호최고책임자(CISO) 또는 개인정보보호책임자(CPO), 부서장 및 주요직무자, 인증 담당자, 유관부서 관련자 등이 참석한다.
- 심사팀장은 ISMS-P 인증제도 개요, 심사원 소개, 심사 계획 등을 설명하고, 신청기관 담당자는 ISMS-P 구축 및 운영 현황 등에 대하여 간략하게 설명한다.

2.2. 인증심사

- 인증심사는 ISMS-P의 인증기준, 즉 관리체계 수립 및 운영, 보호대책 요구사항 및 개인정보 처리단계별 요구사항의 인증항목에 맞는 체계를 구축하고 적절하게 운영하고 있는지 확인한다.
- 인증심사는 서면심사와 현장심사를 병행하여 실시하며, 현장심사의 경우 서면심사 진행 현황에 맞춰 일정을 조율하여 진행한다.
- 서면심사는 ISMS-P 관련 정책, 지침, 매뉴얼(절차) 등 내부규정 존재 여부 및 해당 내부 규정이 인증기준을 충족하는지 심사한다. 또한, 신청기관에서 제출한 증적자료 확인을 통해 운영의 적정성을 확인한다.
- 현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행 여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 등의 방법으로 심사한다.

☞ 인증심사 시 유의사항

- 인증심사 시 인증준비 미흡 또는 인증심사팀 요청사항(추가자료 요청, 현장실사 및 인터뷰 요청 등) 대응이 미흡한 경우, 심사의 신뢰성을 확보할 수 없기 때문에 인증 심사팀이 철수하거나 심사를 중단할 수 있다.

2.3. 결함보고서 검토

- 인증심사팀은 서면 및 현장심사를 통하여 도출된 문제점에 대해 신청기관 담당자와의 회의를 통해 상호 간 결과를 확인한다.
  - 신청기관은 인증심사팀이 작성한 결함보고서에 사실과 다른 내용이 있는지 검토한다.
- 결함 사항: 신청기관의 정보보호 관리체계가 인증심사기준에 규정된 요구사항을 충족하지 못하는 사항이 발견되고 있으나 발견된 문제점이 정보보호 및 개인정보보호 관리체계에 중대한 영향을 미치지 않는 사항
- 중결함 사항: 신청인의 정보보호 관리체계가 인증심사기준에 규정된 요구사항을 충족하지 못하는 사항이 발견되고 있으며 발견된 문제점이 정보보호 및 개인정보보호 관리체계에 중대한 영향을 미치는 사항
- 중결함 사항이 확인된 경우 인증심사팀은 중결함이 확인된 시점부터 인증심사를 중단할 수 있다.

2.4. 인증심사 종료회의

- 종료회의에서 인증심사팀은 신청기관 임직원 및 담당자에게 심사 결과를 설명하고 보완조치요청서를 통해 결함사항들에 대한 보완조치를 요청한다.
- 인증심사팀은 보완조치 기간, 보완조치 제출방법, 인증위원회 개최 등 향후 진행 사항 및 일정에 대하여 안내하는 것으로 심사를 종료한다.

2.5. 보완조치 완료 및 결과제출

- 신청기관은 보완조치 요청을 받은 날로부터 40일 이내 보완조치를 완료하고 보완조치 사항에 대한 보완조치 내역서 및 보완조치 완료확인서를 작성하여 심사 수행기관에 제출해야 한다.
- 심사 수행기관은 신청기관이 제출한 보완조치 결과가 미흡하다고 판단하거나, 신청기관 스스로 보완조치 내용상 기한 연장이 필요하다고 판단되는 경우 공문을 통해 최대 60일 간(재조치 기간 포함) 연장할 수 있다.
  - 보완조치 기한 연장 시 보완조치요약서 및 완료된 결함사항에 대한 보완조치 내역서를 공문과 같이 제출해야 한다.
  - 총 100일의 보완조치 기한은 심사팀장이 보완조치 결과를 확인하기 위한 이행점검이 완료된 시점까지를 포함한다.
- 심사팀장은 보완조치내역서의 적절성을 판단하고 이행점검을 통해 실제 이행 여부를 확인한다.
  - 신청기관은 보완조치 전·후 내용을 확인할 수 있도록 작성하여야 하며, 보완조치의 이행계획은 보완조치가 완료되지 않은 것으로 판단한다.

- 보완조치 완료 여부가 최종 확인된 이후 심사팀장은 확인 결과를 보완조치 완료 확인서에 각각 서명 날인하고 보완조치 완료가 확인되었음을 신청기관에 안내한다.
- 연장 기한 포함하여 최대 100일 이내에 보완조치가 완료되지 않은 경우, 인증이 취소된다(최초심사의 경우, 심사 무효).

☞ 인증심사 시 유의사항

- 인증 또는 심사기관은 신청기관이 고의로 인증심사의 실시를 지연 또는 방해하거나 신청기관의 귀책으로 인증심사를 계속 진행하기가 곤란하다고 인정되는 경우 인증심사를 중단할 수 있다.

3 ISMS-P 인증단계

3.1. 인증위원회 심의·의결

- 최초심사 또는 갱신심사의 경우 인증 또는 심사기관은 보완조치가 완료된 신청기관에 대하여 "인증심사 결과보고서"를 작성하여 인증위원회 안건으로 상정한다.
  - 이는 심사결과에 대한 객관성 및 공정성 확보, 일정수준 이상의 품질을 확보하기 위함이다.
- 인증위원회는 정보보호 및 개인정보보호 관리체계 고시에 따라 관련 전문가로 구성되며 각 상정된 안건에 대하여 다음의 사항을 심의·의결한다.

☞ ISMS-P 인증위원회 심의·의결 사항

- 최초심사 또는 갱신심사 결과가 인증기준에 적합한지 여부
- 인증취소사유(정보통신망법 제47조제10항)를 발견한 경우에 그 결과의 적합성 여부
- 인증심사 결과 또는 인증 취소처분에 관하여 이의가 있는 경우 이의신청에 관한 사항
- 그 밖에 ISMS-P 인증과 관련하여 위원장이 필요하다고 인정하는 사항

- 인증위원회에서는 심의결과에 따라 보완조치를 요구할 수 있다. 이 경우 심사팀장을 통해 신청기관에게 해당사항과 보완조치 기한이 전달된다.
  - 보완조치사항을 전달받은 신청기관은 해당사항의 보완 완료 후 심사팀장에게 수정된 "보완조치 내역서"를 제출해야 한다.
  - 보완조치 이행여부를 확인한 심사팀장은 해당사항에 대한 결과보고서를 재상정하고 인증위원회는 해당 안건에 대하여 다시 심의·의결한다.

3.2. 인증결과 통보

- 인증기관의 장은 인증위원회의 심의·의결 결과를 신청기관에 통보하고 ISMS-P 인증기준에 적합한 경우 인증서를 발급하며, 부적합 통보를 받은 신청기관은 이의신청을 할 수 있다.
- 인증취득기관은 인증 유효기간 동안 정보보호 및 개인정보보호 관리체계를 지속적으로 유지하고 개선하여야 한다.

4 ISMS-P 사후관리 단계

4.1. 사후심사

- 사후심사는 인증취득기관이 수립하여 운영 중인 정보보호 및 개인정보보호 관리체계가 인증기준에 적합한 수준으로 유지되는지 확인하기 위해 인증 유효기간 중 매년 1회 이상 시행하는 인증심사를 말한다.
- 사후심사는 인증발급일 기준으로 매 1년 이전에 심사를 완료해야 하며, 인증 유효기간 내 심사를 받지 않을 경우 고시 제35조(인증의 취소)에 따라 인증이 취소될 수 있다.

4.2. 갱신심사

- ISMS-P 인증의 유효기간은 3년이며 갱신심사는 인증 유효기간이 만료될 때 유효기간 연장을 목적으로 시행하는 인증심사이다.
- 갱신심사는 유효기간(인증발급일 기준) 만료 전에 심사를 받아야 하며, 인증유효기간 내 심사를 받지 않을 경우 인증은 효력을 상실한다.
- 갱신심사를 통해 연장되는 인증 유효기간은 3년이며, 최초심사와 마찬가지로 인증위원회에서 인증 유효기간 연장에 대한 심의·의결을 받아야 한다.

과학기술정보통신부 개인정보보호위원회 KISA 한국인터넷진흥원