1. 정보보호관리체계(ISMS)

- "한국인터넷진흥원(KISA) 자료" 참고

다음은 한국인터넷진흥원에서 주관하는 종합 정보보호 관리체계를 위한 **인증제도**이다.

〈정보보호 및 개인정보보호 관리체계 인증〉

정보보호 및 개인정보보호 관리체계 인증 ISMS-P Personal Information & Information Security Management System	**정보보호 및 개인정보보호 관리체계 인증** 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도

〈정보보호 관리체계 인증〉

정보보호 관리체계 인증 ISMS Information Security Management System	**정보보호 관리체계 인증** 정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도

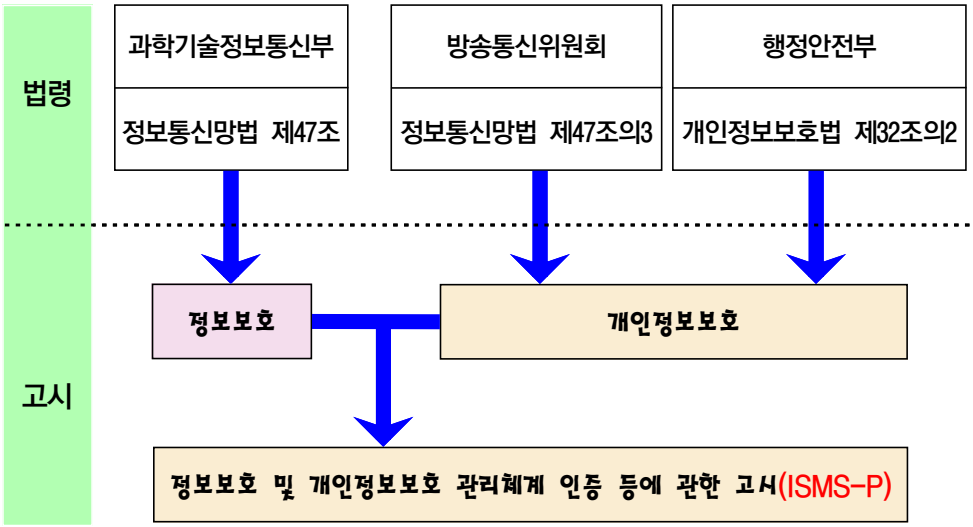
〈한국인터넷진흥원 참조〉

1. ISMS-P 법적근거

법	정보통신망법 제47조	정보통신망법 제47조의 3	개인정보보호법 제32조의 2
하위 법령	시행령 제47조~제54조 시행규칙 제3조	시행령 제54조의 2	시행령 제34조의 2~제34조의 7
고시	정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시		

• 정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭 : 정보통신망법)

〈ISMS-P 법적근거〉



〈한국인터넷진흥원 참조〉

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)

① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.
〈개정 2012. 2. 17., 2013. 3. 23., 2015. 12. 1., 2017. 7. 26.〉

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. 〈신설 2012. 2. 17., 2015. 12. 1., 2018. 12. 24.〉

1. 「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자
2. 집적정보통신시설 사업자
3. 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간의 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

③ 과학기술정보통신부장관은 제2항에 따라 인증을 받아야 하는 자가 과학기술정보통신부령으로 정하는 바에 따라 국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우에는 제1항에 따른 인증 심사의 일부를 생략할 수 있다. 이 경우 인증 심사의 세부 생략 범위에 대해서는 과학기술정보통신부장관이 정하여 고시한다. 〈신설 2015. 12. 1., 2017. 7. 26.〉

④ 과학기술정보통신부장관은 제1항에 따른 정보보호 관리체계 인증을 위하여 관리적·기술적·물리적 보호대책을 포함한 인증기준 등 그 밖에 필요한 사항을 정하여 고시할 수 있다.
〈개정 2012. 2. 17., 2013. 3. 23., 2015. 12. 1., 2017. 7. 26.〉

⑤ 제1항에 따른 정보보호 관리체계 인증의 유효기간은 3년으로 한다. 다만, 제47조의5제1항에 따라 정보보호 관리등급을 받은 경우 그 유효기간 동안 제1항의 인증을 받은 것으로 본다.
〈신설 2012. 2. 17., 2015. 12. 1.〉

⑥ 과학기술정보통신부장관은 한국인터넷진흥원 또는 과학기술정보통신부장관이 지정한 기관(이하 "정보보호 관리체계 인증기관"이라 한다)으로 하여금 제1항 및 제2항에 따른 인증에 관한 업무로서 다음 각 호의 업무를 수행하게 할 수 있다.
〈신설 2012. 2. 17., 2013. 3. 23., 2015. 12. 1., 2017. 7. 26.〉
1. 인증 신청인이 수립한 정보보호 관리체계가 제4항에 따른 인증기준에 적합한지 여부를 확인하기 위한 심사(이하 "인증심사"라 한다)
2. 인증심사 결과의 심의
3. 인증서 발급·관리
4. 인증의 사후관리
5. 정보보호 관리체계 인증심사원의 양성 및 자격관리
6. 그 밖에 정보보호 관리체계 인증에 관한 업무

⑦ 과학기술정보통신부장관은 인증에 관한 업무를 효율적으로 수행하기 위하여 필요한 경우 인증심사 업무를 수행하는 기관(이하 "정보보호 관리체계 심사기관"이라 한다)을 지정할 수 있다.
〈신설 2015. 12. 1., 2017. 7. 26.〉

⑧ 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 과학기술정보통신부장관에게 통보하여야 한다. 〈신설 2012. 2. 17., 2013. 3. 23., 2015. 12. 1., 2017. 7. 26.〉

⑨ 제1항 및 제2항에 따라 정보보호 관리체계의 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다. 〈개정 2012. 2. 17., 2015. 12. 1.〉

⑩ 과학기술정보통신부장관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우에는 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 인증을 취소하여야 한다.
〈신설 2012. 2. 17., 2013. 3. 23., 2015. 12. 1., 2017. 7. 26.〉
1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증을 받은 경우
2. 제4항에 따른 인증기준에 미달하게 된 경우
3. 제8항에 따른 사후관리를 거부 또는 방해한 경우

⑪ 제1항 및 제2항에 따른 인증의 방법·절차·범위·수수료, 제8항에 따른 사후관리의 방법·절차, 제10항에 따른 인증취소의 방법·절차, 그 밖에 필요한 사항은 대통령령으로 정한다.
〈개정 2012. 2. 17., 2015. 12. 1.〉

⑫ 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관 지정의 기준·절차·유효기간 등에 필요한 사항은 대통령령으로 정한다.
〈개정 2012. 2. 17., 2015. 12. 1.〉 [전문개정 2008. 6. 13.]

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조의 3(개인정보보호 관리체계의 인증)

① 방송통신위원회는 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "개인정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제2항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

② 방송통신위원회는 제1항에 따른 개인정보보호 관리체계 인증을 위하여 관리적·기술적·물리적 보호대책을 포함한 인증기준 등 그 밖에 필요한 사항을 정하여 고시할 수 있다.

③ 개인정보보호 관리체계의 수행기관, 사후관리 등에 대하여는 제47조제6항부터 제12항까지의 규정을 준용한다. 이 경우 "제1항 및 제2항"은 "제1항"으로 본다. 〈개정 2015. 12. 1.〉

④ 개인정보보호 관리체계 인증기관의 지정취소 등에 대하여는 제47조의2를 준용한다.
[본조신설 2012. 2. 17.]
[종전 제47조의3은 제47조의4로 이동 〈2012. 2. 17.〉]

개인정보 보호법 제32조의2(개인정보 보호 인증)

① 보호위원회는 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관하여 **인증할 수 있다**. 〈개정 2017. 7. 26., 2020. 2. 4.〉
② 제1항에 따른 인증의 유효기간은 3년으로 한다.
③ 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령으로 정하는 바에 따라 제1항에 따른 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 취소하여야 한다. 〈개정 2017. 7. 26., 2020. 2. 4.〉
1. 거짓이나 그 밖의 부정한 방법으로 개인정보 보호 인증을 받은 경우
2. 제4항에 따른 사후관리를 거부 또는 방해한 경우
3. 제8항에 따른 인증기준에 미달하게 된 경우
4. 개인정보 보호 관련 법령을 위반하고 그 위반사유가 중대한 경우
④ 보호위원회는 개인정보 보호 인증의 실효성 유지를 위하여 연 1회 이상 사후관리를 실시하여야 한다. 〈개정 2017. 7. 26., 2020. 2. 4.〉
⑤ 보호위원회는 대통령령으로 정하는 전문기관으로 하여금 제1항에 따른 인증, 제3항에 따른 인증취소, 제4항에 따른 사후관리 및 제7항에 따른 인증 심사원 관리 업무를 수행하게 할 수 있다. 〈개정 2017. 7. 26., 2020. 2. 4.〉
⑥ 제1항에 따른 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.
⑦ 제1항에 따른 인증을 위하여 필요한 심사를 수행할 심사원의 자격 및 자격 취소 요건 등에 관하여는 전문성과 경력 및 그 밖에 필요한 사항을 고려하여 대통령령으로 정한다.
⑧ 그 밖에 개인정보 관리체계, 정보주체 권리보장, 안전성 확보조치가 이 법에 부합하는지 여부 등 제1항에 따른 인증의 기준·방법·절차 등 필요한 사항은 대통령령으로 정한다.
[본조신설 2015. 7. 24.] [시행일 : 2020. 8. 5.] 제32조의2

개인정보 보호법 제7조(개인정보 보호위원회)

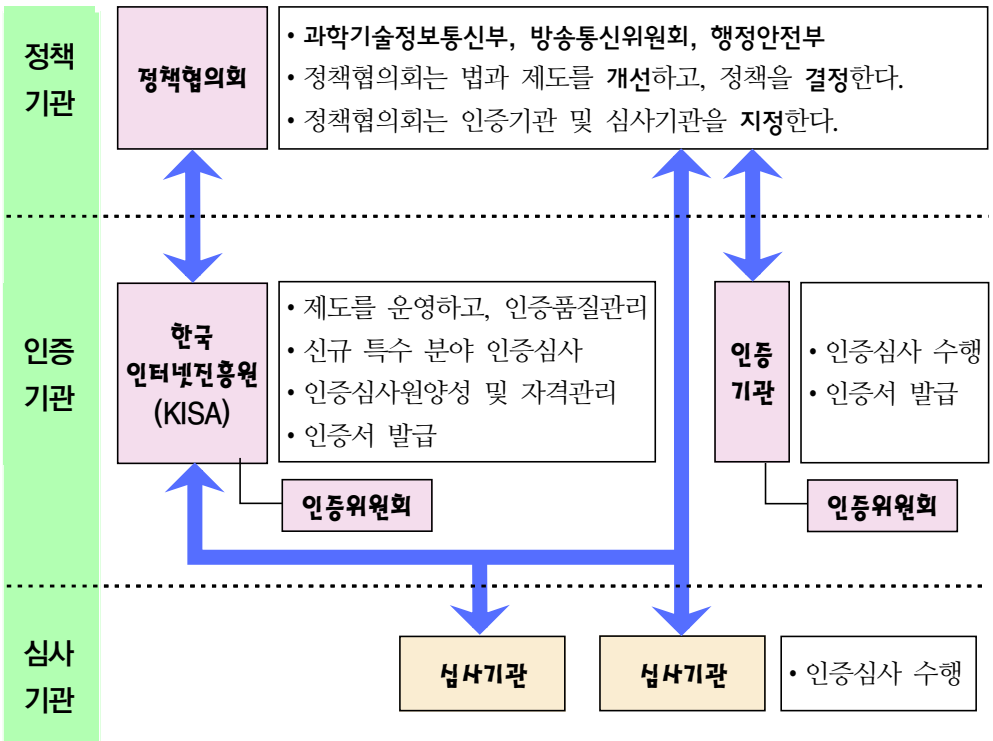
① 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 **국무총리** 소속으로 개인정보 보호위원회(이하 "보호위원회"라 한다)를 둔다. 〈개정 2020. 2. 4.〉
② 보호위원회는 「정부조직법」 제2조에 따른 중앙행정기관으로 본다. 다만, 다음 각 호의 사항에 대하여는 「정부조직법」 제18조를 적용하지 아니한다. 〈개정 2020. 2. 4.〉
1. 제7조의8제3호 및 제4호의 사무
2. 제7조의9제1항의 심의·의결 사항 중 제1호에 해당하는 사항
[시행일 : 2020. 8. 5.] 제7조

• 추가 설명 : 정부조직법에서 **개인정보 보호위원회**는 **행정안전부** 소속 위원회이다.

2. ISMS-P 인증체계

ISMS-P 인증체계는 다음과 같다.

〈ISMS-P 인증체계〉



〈한국인터넷진흥원 참조〉

- 정책기관 : 과학기술정보통신부, 방송통신위원회, 행정안전부 (정책협의회)
- 인증기관 : 한국인터넷진흥원(KISA)
- 인증심사팀은 ISMS 인증심사원 양성교육을 수료하고 자격요건을 갖춘 자들로 구성한다.

ISMS-P 인증제도는 정보보호등급제를 실시한다.**(우수와 최우수)**

〈정보보호등급제 기대효과〉

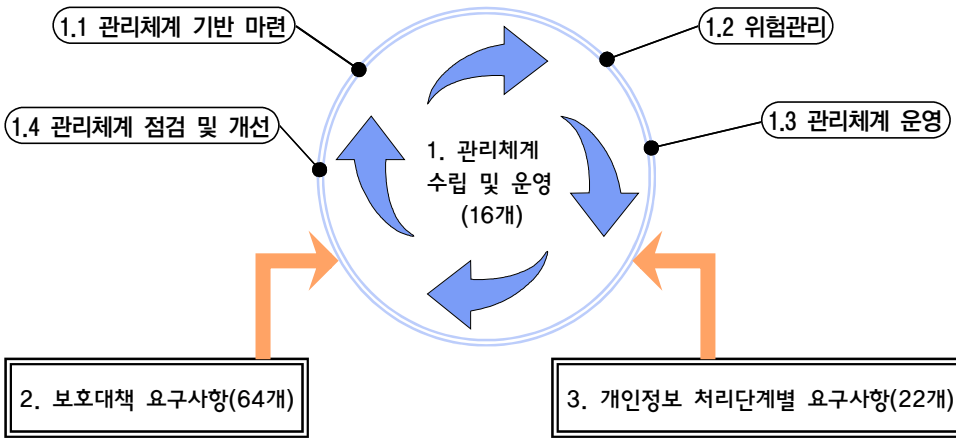
- 이용자에게 객관적인 기업 선택의 기준을 제시
- 기업의 신뢰수준 및 비교우위 경쟁력 확보 지원
- 기업의 정보보호 활동 기준 및 목표수준 마련

〈한국인터넷진흥원 참조〉

3. ISMS-P 인증기준

ISMS-P 인증기준은 다음과 같다.

〈ISMS-P 인증기준〉



〈한국인터넷진흥원 참조〉

↓

↓ 인증기준 세부사항

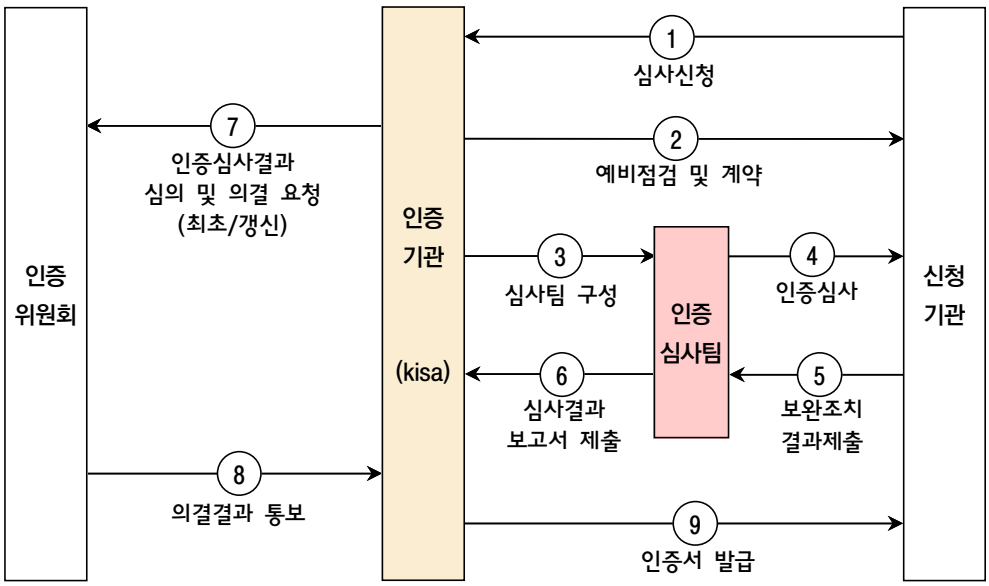
↓

구분		영역	분야(인증기준)
ISMS-P	ISMS	1. 관리체계 수립 및 운영(16개) ↓ 필수영역, PDCA 모델 적용	1.1 관리체계 기반 마련(6) 1.2 위험관리(4) 1.3 관리체계 운영(3) 1.4 관리체계 점검 및 개선(3)
		2. 보호대책 요구사항(64개) ↓ 선택영역 해당사항이 없으면 이유를 제시 (현실적으로는 모두 인증을 받음)	2.1 정책, 조직, 자산 관리(3) 2.2 인적보안(6) 2.3 외부자 보안(4) 2.4 물리보안(7) 2.5 인증 및 권한 관리(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 재해복구(2)
	–	3. 개인정보 처리단계별 요구사항 (22개) ↓ 준거성(법률)	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(3) 3.5 정보주체 권리보호(3)

4. ISMS-P 인증심사 절차

ISMS-P 인증심사 절차는 다음과 같다.

〈ISMS-P 인증심사 절차〉



〈한국인터넷진흥원 참조〉

- 신청 단계 : 신청공문 + 인증신청서, 관리체계운영명세서, 법인/개인 사업자 등록증
- 계약 단계 : 수수료 산정 〉 계약 〉 수수료 납부
- 심사 단계 : 인증심사 〉 결함보고서 〉 보완조치내역서
- 인증 단계 : 최초/갱신심사 심의 의결(인증위원회), 유지(인증기관)

◈ 인증신청 방법

- 인증심사 신청 시 다음의 서류들을 준비하여 인증 또는 심사기관에 제출한다.
- 인증 신청 공문 1부
- 인증 신청서 1부
- 인증 명세서 1부
- 법인/개인 사업자 등록증 1부

※ 인증신청서 및 명세서 양식은 홈페이지 자료실에서 다운로드 가능

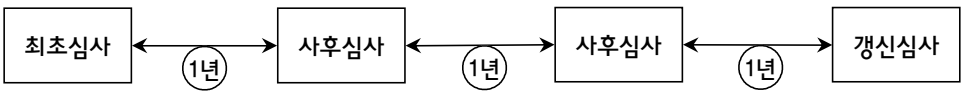
5. ISMS-P 인증범위

ISMS-P 인증범위는 다음 2가지이다.

구분		내용
ISMS-P	**정보보호 및 개인정보보호 관리체계 인증**	• 정보서비스의 운영 및 보호에 필요한 조직, 물리적 위치, 정보자산 • 개인정보 처리를 위한 수집, 보유, 이용, 제공, 파기에 관여하는 개인정보처리 시스템, 취급자를 포함
ISMS	**정보보호 관리체계 인증**	• 정보서비스의 운영 및 보호에 필요한 조직, 물리적 위치, 정보자산을 포함

6. ISMS-P 심사종류

〈ISMS-P 심사종류〉



〈한국인터넷진흥원 참조〉

↓세부적 설명

구분	설명
최초심사	• 최초심사는 인증을 처음으로 취득할 때 진행하는 심사이며 • 인증의 범위에 중요한 변경이 있어 다시 인증을 신청할 때에도 실시한다. • 최초심사를 통해 인증을 취득하면 **3년**의 유효기간이 부여
사후심사	• 사후심사는 인증을 취득한 이후 정보보호 관리체계가 지속적으로 유지되고 있는지 확인하는 것을 목적한다. • 사후심사는 인증 유효기간 중 **매년 1회 이상** 시행하는 심사이다.
갱신심사	• 갱신심사는 정보보호 관리체계 인증 유효기간 연장을 목적의 심사를 말한다.

7. ISMS-P 인증의 홍보

• 인증 표시를 사용하는 경우 인증의 범위와 유효기간을 함께 표시하여야 하며, 고시에 지정된 색상 등 사용 방법을 준수해야 한다.
• 인증 받은 내용을 거짓으로 표시하거나 홍보한 자는 과태료 부과
• 정보통신망법 : 1천만원
• 개인정보보호법 : 5천만원

8. ISMS-P 인증대상

ISMS-P 인증대상은 자율신청자와 의무대상자로 구분된다.

① 자율신청자

의무대상자 기준에 해당하지 않으나 자발적으로 정보보호 및 개인정보보호 관리체계를 구축·운영하는 기업·기관은 임의신청자로 분류되며, 임의신청자가 인증 취득을 희망할 경우 자율적으로 신청하여 인증심사를 받을 수 있다.

② ISMS인증 의무대상자(정보통신망법 제47조 2항)

인증 의무대상자는 전기통신사업법 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 표에서 기술한 의무대상자 기준에 하나라도 해당되는 자이다.

구분	의무대상자 기준
ISP	전기통신사업법 제6조제1항에 따른 허가를 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
IDC	정보통신망법 제46조에 따른 집적 정보통신시설 사업자
다음 조건 중 하나라도 해당하는 자	① 연간 매출액 또는 세입이 1,500억원 이상인 자 중에서 다음에 해당되는 경우 • 의료법」 제3조의4에 따른 상급종합병원 • 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
	② 정보통신서비스 부문 전년도 매출액이 100억원 이상인 자 (법인인 경우에는 전 사업연도를 말한다)
	③ 전년도 직전 3개월간 정보통신서비스 일일평균 이용자 수가 100만명 이상인 자

• ISP : Internet service provider 약어, 인터넷 서비스 제공자

• IDC : Internet Data Center 약어, 인터넷 데이터 센터를 의미 (수많은 서버를 관리)

◈ 의무대상자 신청

• 의무대상자는 ISMS, ISMS-P 인증 중 선택 가능

• 의무대상자가 되어 인증을 최초로 신청하는 경우 다음 해 8월 31일까지 인증 취득

※ 이미 인증을 취득한 기업의 경우 해당 없음

탐구

우리나라 정보보호 인증제도 변천사

우리나라 보안 인증제도에 대해서 살펴본다.

〈우리나라 보안 인증제도 변천사〉

인증제도	정책기관	인증기관	인증 대상
ISMS	미래창조과학부	한국인터넷진흥원	공공기관 및 기업
G-ISMS	미래창조과학부	한국인터넷진흥원	공공기관(전자정부)
PIMS	방송통신위원회	한국인터넷진흥원	개인정보를 처리하는 기업, 기관, 개인
PIPL	안전행정부	한국정보화진흥원	공공기관 • 대기업 • 중소기업 • 소상공인

• 2014년, G-ISMS는 ISMS로 통합(민간과 공공기관이 동일한 인증제도를 사용하게 됨)
• 2016년, 중복성 논란으로 PIPL(개인정보보호인증제)은 PIMS로 통합되었고
• 2017년, ISMS와 PIMS의 심사항목 중 74%가 중복 및 유사하여 ISMS-P로 통합되었다.

↓
↓ 현재, ISMS-P로 통합
↓

〈정보보호 및 개인정보보호 관리체계인증(ISMS-P)〉

구분		통합인증(영역)
ISMS-P	ISMS	1. 관리체계 수립 및 운영(16)
		2. 보호대책 요구사항(64)
	–	3. 개인정보 처리단계별 요구사항(22)

〈한국인터넷진흥원 참조〉

• ISMS-P 인증은 조직의 정보 자산을 체계적으로 보호하기 위한 종합적인 관리체계이다.
• ISMS-P 인증은 기업의 성공적인 비즈니스를 위한 필수조건이라고도 한다.

기출문제 분석

1. 국내의 기관이나 기업이 정보 및 개인정보를 체계적으로 보호할 수 있도록 통합된 관리체계 인증제도는? [2019년 지방 9급]

① PIPL-P ② ISMS-I ③ PIMS-I ④ ISMS-P

♤ ISMS-P

- 국가 보안인증이 하나로 통합 확정(2017. 12. 27) : ISMS-P(가칭)

ISMS(104개)		PIMS(86개)		통합인증(102개)
유사 • 공통(82)	+	유사 • 공통(58)	⇒	정보보호(80)
고유항목(82)		고유항목(28)		개인정보보호 특화(22)

- 중복성 논란으로, PIPL(개인정보보호인증제)은 2016년부터 PIMS로 통합되었고
- 2018부터는 ISMS와 PIMS의 심사항목 중 74%가 유사 및 중복으로 통합되었다.
- 보안인증 통합으로 기업들은 기본적으로 80개 보안항목으로 ISMS 인증을 받을 수 있고,
- 추가로 22개 개인정보보호 항목을 신청해 인증 받으면 ISMS-P 인증을 받을 수 있다.

정답 : ④

2. 현행 우리나라의 정보보호관리체계(ISMS) 인증에 대한 설명으로 옳지 않은 것은? [2016년 지방 9급]

① 정보통신망 이용촉진 및 정보보호 등에 관한 법률 에 근거를 두고 있다.
② 인증심사의 종류에는 최초심사, 사후심사, 갱신심사가 있다.
③ 인증에 유효기간은 정해져 있지 않다.
④ 정보통신망의 안정성 • 신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 인증 기준에 적합한지에 관하여 인증을 부여하는 제도이다.

♤ 정보보호관리체계(ISMS) 인증

- 인증에 유효기간은 정해져 있지 않다.(×)
- 최초심사 : 정보보호관리체계 인증 취득을 위한 심사
- 사후심사 : 정보보호관리체계를 지속적으로 유지하고 있는지에 대한 심사(연 1회 이상)
- 갱신심사 : 유효기간(3년)만료일 이전에 유효기간의 연장을 목적으로 하는 심사

정답 : ③

3. 정보보호 및 개인정보보호 관리체계 인증에 대한 설명으로 옳은 것은? [2021년 지방 9급]

① 인증기관 지정의 유효기간은 2년이다.
② 사후심사는 인증 후 매년 사후관리를 위해 실시된다.
③ 인증심사 기준은 12개 분야 92개 통제 사항이다.
④ 인증심사원은 2개 등급으로 구분된다.

♤ **정보보호 및 개인정보보호 관리체계 인증**

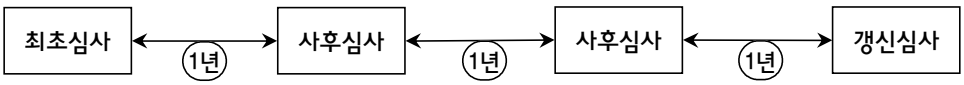
- 인증기관 지정의 유효기간은 **2**년이다.(×) → 인증기관 지정의 유효기간은 **3**년이다.
- 인증심사 기준은 12개 분야 92개 통제 사항이다.(×)
  → 인증심사 기준은 **3**개 분야, **102**개 항목(인증기준)이다.
- 인증심사원은 **2개 등급으로 구분**된다.(×)
  → 인증심사원은 **심사원보, 심사원, 선임심사원**으로 구분한다.(**3개 등급**)

// 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(※ 별표 3)

등급	자격 기준
심사원보	**인증심사원** 자격 신청 요건을 만족하는 자로서 인터넷진흥원이 수행하는 인증심사원 양성과정을 통과하여 자격을 취득한자
심사원	**심사원보** 자격 취득자로서 인증심사에 **4**회 이상 참여하고 심사일수의 합이 **20**일 이상인 자
선임심사원	**심사원** 자격 취득자로서 정보보호 및 개인정보보호 관리체계 인증심사를 **3**회 이상 참여하고 심사일수의 합이 **15**일 이상인 자

인증심사원 등급별 자격 요건(제12조 관련)

// ISMS-P 심사종류 〈한국인터넷진흥원 참조〉



↓세부적 설명

구분	설명
최초심사	• 최초심사는 인증을 처음으로 취득할 때 진행하는 심사이며 • 인증의 범위에 중요한 변경이 있어 다시 인증을 신청할 때에도 실시한다. • 최초심사를 통해 인증을 취득하면 **3년의 유효기간**이 부여
사후심사	• 사후심사는 인증을 취득한 이후 정보보호 관리체계가 지속적으로 유지되고 있는지 확인하는 것을 목적한다. • 사후심사는 인증 유효기간 중 **매년 1회 이상** 시행하는 심사이다.
갱신심사	• 갱신심사는 정보보호 관리체계 인증 유효기간 연장을 목적의 심사를 말한다.

정답 : ②

(개인정보보호위원회) 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시

제4장 인증심사원

제12조(인증심사원의 자격 요건 등)
인증심사원은 **심사원보, 심사원, 선임심사원**으로 구분하며 등급별 자격 요건은 별표 3 과 같다.
제13조(인증심사원 자격 신청)
① 인증심사원 자격을 신청하고자 하는 자는 별표 4 의 인증심사원 자격 신청 요건을 갖추고 인터넷진흥원이 공고하는 신청기간 내에 별지 제7호 서식 의 인증심사원 자격 신청서와 관련 서류를 제출하여야 한다.
② 인터넷진흥원은 제1항에 의해 제출한 신청서류가 자격 신청 요건에 적합한지를 검토하여야 한다.
③ 제2항에 따른 서류검토 결과 적합한 자는 인터넷진흥원이 시행하는 인증심사원 양성과정을 수료하여야 한다.

제14조(인증심사원 자격 발급 및 관리)
① 인터넷진흥원은 인증심사원 양성과정을 수료한 자에게 별지 제8호서식 의 정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서를 발급하여야 한다.
② 인터넷진흥원은 인증심사원의 자격 증명서 발급, 심사원등급, 인증심사 업무경력 등을 관리하여야 한다.

제15조(인증심사원 자격 유지 및 갱신)
① 인증심사원의 자격 유효기간은 자격을 부여 받은 날부터 3년으로 한다.
② 인증심사원은 자격유지를 위해 자격 유효기간 만료 전까지 인터넷진흥원이 인정하는 보수교육을 수료하여야 한다.
③ 인터넷진흥원은 자격 유효기간 동안 1회 이상의 인증심사를 참여한 인증심사원에 대하여 제2항의 보수교육 시간 중 일부를 이수한 것으로 인정할 수 있다.
④ 인터넷진흥원은 인증정보를 제공하는 홈페이지에 제2항의 보수교육 운영에 관한 세부내용을 공지하여야 한다.
⑤ 인터넷진흥원은 제2항의 요건을 충족한 인증심사원에 한하여 별지 제8호서식 의 정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서를 갱신하여 발급하고 자격 유효기간을 3년간 연장한다.
⑥ 제5항에도 불구하고 인터넷진흥원은 다음 각 호의 어느 하나에 해당하면 인증심사원 자격의 유효기간을 연장할 수 있다.
1. 제29조제2항 에 따른 인증위원회 위원으로 인정된 자
2. 「재난 및 안전관리 기본법」 제3조 에 따른 재난의 발생 등 협의회가 인정하는 불가피한 경우

4. 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시에서 인증심사원에 대한 설명으로 옳지 않은 것은? [2022년 국가 9급]

① 인증심사원의 자격 유효기간은 자격을 부여 받은 날부터 3년으로 한다.

② 인증심사 과정에서 취득한 정보 또는 서류를 관련 법령의 근거나 인증신청인의 동의 없이 누설 또는 유출하거나 업무목적 외에 이를 사용한 경우에는 인증심사원의 자격이 취소될 수 있다.

③ 인증위원회는 자격 유효기간 동안 1회 이상의 인증심사를 참여한 인증심사원에 대하여 자격유지를 위해 자격 유효기간 만료 전까지 수료하여야 하는 보수 교육시간 전부를 이수한 것으로 인정할 수 있다.

④ 인증심사원의 등급별 자격요건 중 선임심사원은 심사원 자격취득자로서 정보보호 및 개인정보보호 관리체계 인증심사를 3회 이상 참여하고 심사일수의 합이 15일 이상인 자이다.

♤ **정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 – 제15조(인증심사원 자격 유지 및 갱신)**

① **인증심사원**의 자격 유효기간은 자격을 부여 받은 날부터 **3**년으로 한다.

② **인증심사원**은 자격유지를 위해 자격 유효기간 만료 전까지 인터넷진흥원이 인정하는 보수교육을 수료하여야 한다.

③ **인터넷진흥원**은 **자격 유효기간** 동안 **1**회 이상의 인증심사를 참여한 **인증심사원**에 대하여 **제2항**의 **보수교육 시간** 중 **일부**를 **이수한 것**으로 인정할 수 있다.

④ 인터넷진흥원은 인증정보를 제공하는 홈페이지에 제2항의 보수교육 운영에 관한 세부내용을 공지하여야 한다.

⑤ 인터넷진흥원은 제2항의 요건을 충족한 인증심사원에 한하여 별지 제8호서식의 정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서를 갱신하여 발급하고 자격 유효기간을 3년간 연장한다.

⑥ 제5항에도 불구하고 인터넷진흥원은 다음 각 호의 어느 하나에 해당하면 인증심사원 자격의 유효기간을 연장할 수 있다.

1. 제29조제2항에 따른 인증위원회 위원으로 인정된 자
2. 「재난 및 안전관리 기본법」 제3조에 따른 재난의 발생 등 협의회가 인정하는 불가피한 경우

정답 : ③