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** 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도

〈정보보호 관리체계 인증〉

	**정보보호 관리체계 인증** 정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도

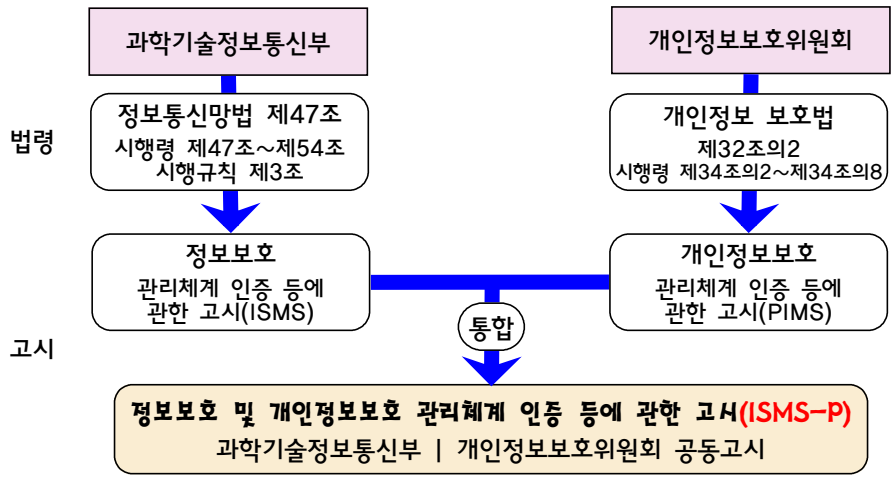
〈한국인터넷진흥원 참조〉

• 보안인증 통합으로 기업들은 기본적으로 80개 보안항목으로 ISMS 인증을 받을 수 있고,
• 추가로 21개 개인정보보호 항목을 신청해 인증받으면 ISMS-P 인증을 받을 수 있다.

• 개인정보 처리단계별 요구사항 21개만을 신청하여 인증받을 수는 없다.

1. ISMS-P 법적 근거

〈ISMS-P 법적 근거〉



〈한국인터넷진흥원 참조〉

// ISMS-P 인증의 기대 효과

- 일회성 정보보호 대책에서 벗어나 체계적, 종합적인 정보보호 관리체계를 구현함으로써 기업의 정보보호 및 개인정보보호 관리수준을 향상시킬 수 있다.
- 기업은 지속적이고 체계적인 ISMS-P 구축을 통해 해킹, DDoS 등의 침해사고 및 개인정보 유출 사고 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.

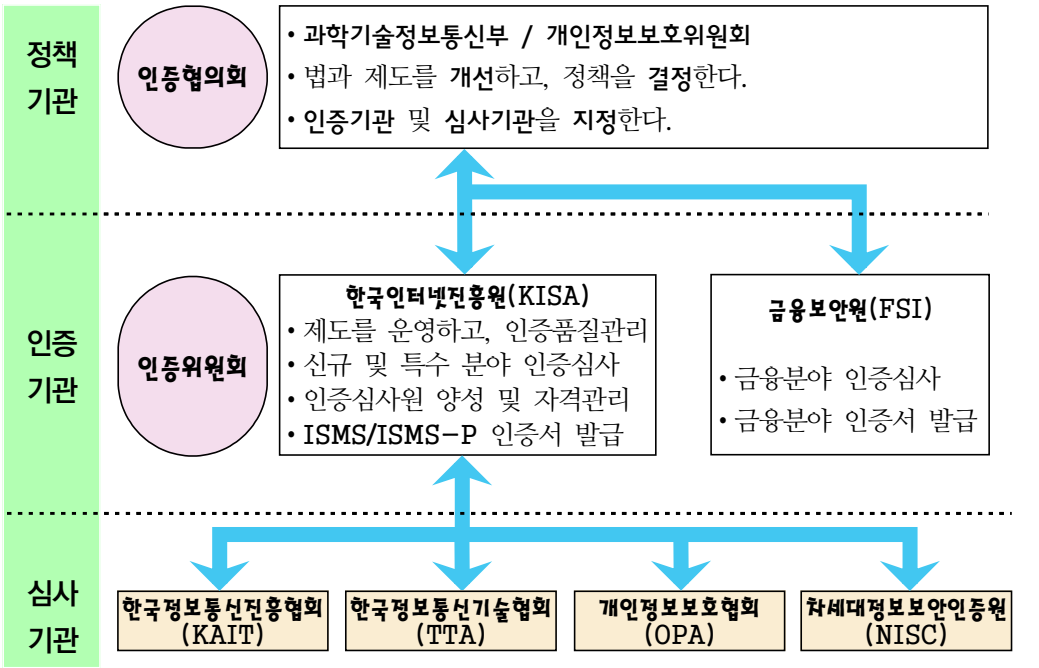
// 인증을 취득하면 침해사고로부터 100% 안전한가?

- 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.

참고	**정보통신망 이용촉진 및 정보보호 등에 관한 법률**은 약칭 **정보통신망법**이라 함

2. ISMS-P 인증 추진 체계

〈ISMS-P 인증 추진 체계〉



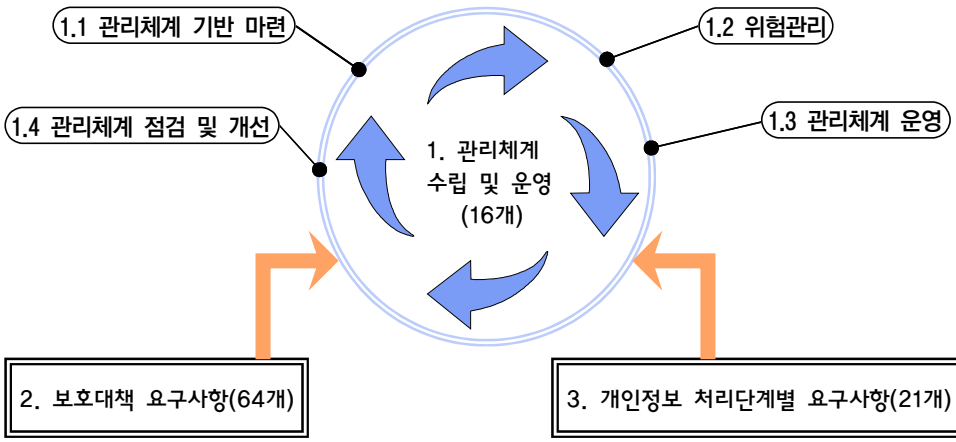
〈한국인터넷진흥원 참조〉

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.
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 금융보안원은 금융 분야 인증위원회를 구성·운영하고, 인증심사 및 인증서 발급 업무를 수행한다.
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.
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.

3. ISMS-P 인증기준

ISMS-P 인증기준은 다음과 같다.

〈ISMS-P 인증기준〉



〈한국인터넷진흥원 참조〉

↓

↓ 인증기준 세부사항

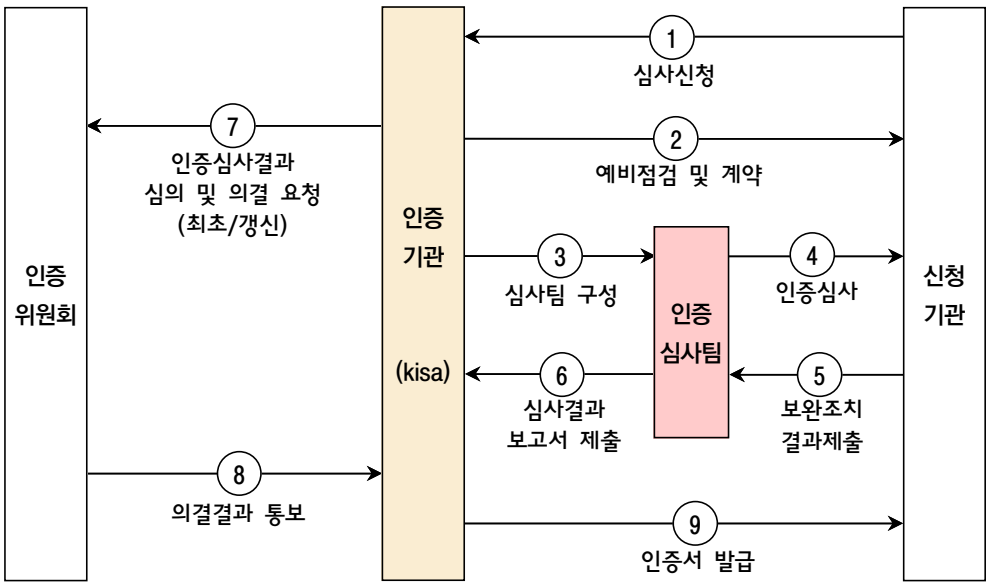
↓

구분		통합인증	분야(인증기준 개수)
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(21개) ↓ 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(2) 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

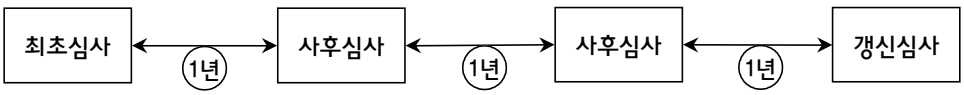
5. ISMS-P 인증범위

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 : 3천만원

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 전년도 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 일일평균 정보통신서비스 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

정보보호 등급제	정보보호 관리체계(ISMS)를 유지하는 기업 대상으로 정보보호 수준을 측정하여 '**우수**' 또는 '**최우수**' 등급을 부여하는 제도

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(101개)
유사 • 공통(82)	+	유사 • 공통(58)	⇒	정보보호(80)
고유항목(82)		고유항목(28)		개인정보보호 특화(21)

- 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 21개 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 법률에 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 인증기준에 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. ISMS-P에 대한 설명으로 옳지 않은 것은? [2020년 국가 7급]

① 인증기준은 크게 3개 영역으로 나뉘며 총 102개의 인증기준으로 구성되어 있다.
② 관리체계 수립 및 운영 영역은 4개 분야 16개 인증기준으로 구성되어 있다.
③ 보호대책 요구사항 영역은 12개 분야 64개 인증기준으로 구성되어 있다.
④ 개인정보 처리단계별 요구사항 영역은 6개 분야 24개의 인증기준으로 구성되어 있다.

인증제도 개정

♤ ISMS-P

• 개인정보 처리단계별 요구사항 영역은 6개 분야 24개의 인증기준으로 구성되어 있다.(×)
→ 개인정보 처리단계별 요구사항 영역은 5개 분야 21개의 인증기준으로 구성되어 있다.

// ISMS-P 인증기준

구분		통합인증(영역)
ISMS-P	ISMS	1. 관리체계 수립 및 운영(16)
		2. 보호대책 요구사항(64)
	–	3. 개인정보 처리단계별 요구사항(21)

인증기준 = 16 + 64 + 21 = 101

정답 : ④

4. 다음 중 국내 정보보호 관리체계 및 인증제도에 대한 설명으로 옳지 않은 것은? [2022년 군무원 7급]

① 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증을 받고자 하는 신청기관은 '관리체계 수립 및 운영', '보호대책 요구사항'의 2개 영역에서 80개의 인증기준을 적용받게 된다.
② 관리체계 수립 및 운영은 관리체계 기반마련, 위험관리, 관리체계 운영, 관리체계 점검 및 개선의 4개 분야 16개 인증기준으로 구성된다.
③ ISMS 인증은 의무 대상자가 아니더라도 자발적으로 신청하여 인증심사를 받을 수 있다.
④ 정보보호 관리체계를 유지하는 기업을 대상으로, 정보보호 수준을 측정하여 '우수', '최우수' 등급을 부여하는 정보보호 등급제 인증제도가 운영되고 있다.

♤ ISMS-P

• 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증을 받고자 하는 신청기관은 '관리체계 수립 및 운영', '보호대책 요구사항'의 2개 영역에서 80개의 인증기준을 적용받게 된다.(×)
→ ISMS-P 인증기준은 3개 영역에서 모두 101개이다.

정답 : ①

5. ISMS-P(정보보호 및 개인정보보호 관리체계 인증)의 보호대책 요구사항에 해당되지 않는 분야는? [2022년 국가 7급]

① 정책, 조직, 자산 관리 ② 외부자 보안
③ 개인정보 제공 시 보호 조치 ④ 접근통제

♤ ISMS-P

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)

• **개인정보 제공 시 보호 조치**는 **개인정보 처리단계별 요구사항**이다.

정답 : ③

6. ISMS-P 인증기준의 세 영역 중 하나인 관리체계 수립 및 운영에 해당하지 않는 것은? [2023년 지방 9급]

① 관리체계 기반 마련 ② 위험관리
③ 관리체계 점검 및 개선 ④ 정책, 조직, 자산 관리

♤ ISMS-P 인증기준

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)

• **정책, 조직, 자산 관리**는 **보호대책 요구사항**이다.

정답 : ④

7. 정보보호 및 개인정보보호 관리체계 인증에 대한 설명으로 옳은 것은? [2021년 지방 9급, 2024년 국가 7급]

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**

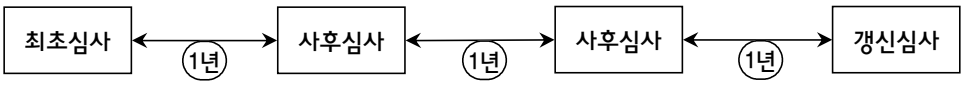
- 인증기관 지정의 유효기간은 **2**년이다.(×) → 인증기관 지정의 유효기간은 **3**년이다.
- 인증심사 기준은 **12**개 분야 **92**개 통제 사항이다.(×)
  → 인증심사 기준은 **3**개 분야, **101**개 항목(인증기준)이다.
- 인증심사원은 **2개 등급으로 구분**된다.(×)
  → 인증심사원은 **심사원보, 심사원, 선임심사원**으로 구분한다.(**3개 등급**)

// 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 3과 같다.

제13조(인증심사원 자격 신청)

① 인증심사원 자격을 신청하고자 하는 자는 별표 4의 인증심사원 자격 신청 요건을 갖추고 인터넷진흥원이 공고하는 신청기간 내에 별지 제7호 서식의 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 제8호서식의 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 **3년**으로 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 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

8. 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.

→ **인터넷진흥원**이 **인증위원회**이다.

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

9. 정보보호 및 개인정보보호 관리체계인증(ISMS-P)에 대한 설명으로 가장 옳지 않은 것은? [2019년 서울 9급]

① 정보보호 관리체계 인증만 선택적으로 받을 수 있다.
② 개인정보 제공 시뿐만 아니라 파기 시의 보호조치도 포함한다.
③ 위험관리 분야의 인증기준은 보호대책 요구사항 영역에서 규정한다.
④ 관리체계 수립 및 운영영역은 Plan, Do, Check, Act의 사이클에 따라 지속적이고 반복적으로 실행되는지 평가한다.

♤ **정보보호 및 개인정보보호 관리체계인증(ISMS-P)** - 한국인터넷진흥원 참조

영역	분야(인증기준)
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)

• ISMS : 정보보호 관리체계 인증(ISMS 인증만 선택적으로 받을 수 있다)

정답 : ③