



제 439회 국회 (정기회)
제1차 과학기술정보방송통신위원회

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

검 토 보 고

〈공공기관에 대한 정보보호 관리체계 인증 의무화〉

■ 김용만의원 대표발의(의안번호 제2218584호)

2026. 9.

과학기술정보방송통신위원회

수석전문위원 이지민

목 차

I . 제안경위	1
----------------	---

II . 제안이유 및 주요내용	1
------------------------	---

III . 검토의견	2
------------------	---

1. 공공기관에 대한 정보보호 관리체계 인증 의무화	2
------------------------------------	---

※ 참고자료

1. ISMS(ISMS-P) 제도 소개 자료	10
--------------------------------	----

I. 제안경위

가. 제 안 자 : 김용만의원 등 10인

나. 제 안 일 : 2026. 4. 23.

다. 회 부 일 : 2026. 4. 24.

II. 제안이유 및 주요내용

현행법은 정보보호 관리체계(ISMS) 인증 의무 대상을 법률에서 직접 규정하고 있으나, 개인정보 관리체계(ISMS-P)의 인증 의무 대상과 범위가 일치하지 않고, 특히 공공기관이 ISMS 인증 의무 대상에서 제외되어 정보보호의 사각지대가 발생하고 있음.

이에 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관을 ISMS 인증 의무 대상에 포함하여 정보보호 관리체계 인증의 실효성을 높이려는 것임(안 제47조제2항제4호 신설).

Ⅲ. 검토의견

1. 공공기관에 대한 정보보호 관리체계 인증 의무화

가. 개정안의 내용

- 정보보호 관리체계 인증 의무대상자에 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관을 추가함(안 제47조제2항제4호 신설).

현행	개정안
제47조(정보보호 관리체계의 인증) ① (생략) ② 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신 역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. 1. ~ 3. (생략) <u><신설></u> ③ ~ ⑫ (생략)	제47조(정보보호 관리체계의 인증) ① (현행과 같음) ② ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- 1. ~ 3. (현행과 같음) 4. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관 ③ ~ ⑫ (현행과 같음)
※ 부 칙 이 법은 공포 후 6개월이 경과한 날부터 시행한다.	

나. 검토의견

○ 정보보호 관리체계(ISMS; Information Security Management System) 인증제도는 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치 등 종합적 관리체계를 수립·운영하는 자에 대하여 과학기술정보통신부장관이 고시한 기준에 따라 그 적합성을 인증하여 주는 제도임.

- ISMS 인증제도는 정부가 ISMS 모델을 개발·제공하고 기업이 스스로 ISMS를 구축·운영할 수 있도록 하며 기준에 적합한 경우 인증을 부여하여 기업 차원의 정보보호 환경 조성을 촉진하려는 취지로 2001년 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 개정을 통해 도입되었음.

- ISMS 인증을 받으려는 자는 관리체계 수립 및 운영에 대한 기준(16개)과 보호대책 요구사항(64개)을 충족하여야 함¹⁾.

○ 현행법 제47조제2항은 ISMS 인증을 받아야 하는 대상²⁾으로

1) ISMS 인증제도 관련 구체적인 내용은 9p 제도소개 자료 참조

2) 「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.

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 정보통신망서비스를 제공하는 자(이하 “주요정보통신서비스 제공자”라 한다)
2. 집적정보통신시설 사업자
3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

「전기통신사업법」 제6조(기간통신사업의 등록 등) ① 기간통신사업을 경영하려는 자는 대통령

① 기간통신사업자로서 대통령령³⁾으로 정하는 바에 따라 정보통신망서비스를 제공하는 자(이하 “주요정보통신서비스 제공자”)(제1호),

② 집적정보통신시설 사업자(제2호),

③ 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준⁴⁾에 해당하는 자(제3호)를 규정하고 있음.

○ 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관⁵⁾의 경우

령으로 정하는 바에 따라 다음 각 호의 사항을 갖추어 과학기술정보통신부장관에게 등록(정보통신망에 의한 등록을 포함한다)하여야 한다. 다만, 자신의 상품 또는 용역을 제공하면서 대통령령으로 정하는 바에 따라 부수적으로 기간통신역무를 이용하고 그 요금을 청구하는 자(이용요금 상품 또는 용역의 대가에 포함시키는 경우도 같다)는 기간통신사업을 신고하여야 하며, 신고한 자가 다른 기간통신역무를 제공하고자 하는 경우에는 본문에 따라 등록하여야 한다.

1. 재정 및 기술적 능력
2. 이용자 보호계획
3. 그 밖에 사업계획서 등 대통령령으로 정하는 사항

3) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」

제49조(정보보호 관리체계 인증 대상자의 범위) ① 법 제47조제2항제1호에서 “대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자”란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 「전기통신사업법」 제2조제3호에 따른 전기통신회선설비를 설치·보유하고 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
2. 「전기통신사업법」 제38조제1항에 따라 기간통신사업자로부터 이동통신서비스를 제공받아 재판매하는 전기통신사업자

4) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 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.

5) 「공공기관의 운영에 관한 법률」 제4조(공공기관) ① 재정경제부장관은 국가·지방자치단체가 아닌 법인·단체 또는 기관(이하 “기관”이라 한다)으로서 다음 각 호의 어느 하나에 해당하는

현재 제3호의 사업규모 및 정보통신서비스 규모 기준에 따라 해당 기준을 충족하는 경우 ISMS 인증 의무대상으로 분류되고 있으며, 2026년 8월 기준 정보보호 관리체계 인증을 취득한 공공기관은 의무 대상 기관 21곳(병원 12곳 포함), 의무대상이 아닌 기관 24곳 등 총 45곳임.

<ISMS 인증 취득 공공기관 현황>

[ISMS 인증 의무대상으로서 인증 취득 공공기관 현황]

연번	기관명	연번	기관명	연번	기관명
1	칠곡경북대학교병원	8	양산부산대학교병원	15	한국마사회
2	분당서울대학교병원	9	경상국립대학교병원	16	공영홈쇼핑
3	부산대학교병원	10	서울대학교병원	17	한국조폐공사
4	전남대학교병원	11	화순전남대학교병원	18	한국문화진흥
5	경북대학교병원	12	충남대학교병원	19	강원랜드
6	충북대학교병원	13	서울올림픽기념국민체육진흥공단	20	한국철도공사
7	전북대학교병원	14	에스알	21	인천국제공항공사

기관을 공공기관으로 지정할 수 있다.

1. 다른 법률에 따라 직접 설립되고 정부가 출연한 기관
 2. 정부지원액(법령에 따라 직접 정부의 업무를 위탁받거나 독점적 사업권을 부여받은 기관의 경우에는 그 위탁업무나 독점적 사업으로 인한 수입액을 포함한다. 이하 같다)이 총수입액의 2분의 1을 초과하는 기관
 3. 정부가 100분의 50 이상의 지분을 가지고 있거나 100분의 30 이상의 지분을 가지고 임원 임명권한 행사 등을 통하여 해당기관의 정책 결정에 사실상 지배력을 확보하고 있는 기관
 4. 정부와 제1호부터 제3호까지의 어느 하나에 해당하는 기관이 합하여 100분의 50 이상의 지분을 가지고 있거나 100분의 30 이상의 지분을 가지고 임원 임명권한 행사 등을 통하여 해당 기관의 정책 결정에 사실상 지배력을 확보하고 있는 기관
 5. 제1호부터 제4호까지의 어느 하나에 해당하는 기관이 단독으로 또는 두개 이상의 기관이 합하여 100분의 50 이상의 지분을 가지고 있거나 100분의 30 이상의 지분을 가지고 임원 임명권한 행사 등을 통하여 해당 기관의 정책 결정에 사실상 지배력을 확보하고 있는 기관
 6. 제1호부터 제4호까지의 어느 하나에 해당하는 기관이 설립하고, 정부 또는 설립 기관이 출연한 기관
- ② 제1항에도 불구하고 재정경제부장관은 다음 각 호의 어느 하나에 해당하는 기관을 공공기관으로 지정할 수 없다.
1. 구성원 상호 간의 상호부조·복리증진·권익향상 또는 영업질서 유지 등을 목적으로 설립된 기관
 2. 지방자치단체가 설립하고, 그 운영에 관여하는 기관
 3. 「방송법」에 따른 한국방송공사와 「한국교육방송공사법」에 따른 한국교육방송공사

[ISMS 인증 의무대상이 아님에도 인증 취득 공공기관 현황]

연번	기관명	연번	기관명	연번	기관명
1	서민금융진흥원	9	한국고용정보원	17	한국중부발전
2	한국서부발전	10	중소기업은행	18	한국전력거래소
3	부산항만공사	11	한국약품안전관리원	19	예금보험공사
4	건강보험심사평가원	12	한국교육학술정보원	20	한국산업기술시험원
5	한국농업기술진흥원	13	한국재정정보원	21	농림수산물교육문화정보원
6	한국수력원자력	14	한국자산관리공사	22	한국산업안전보건공단
7	한국공항공사	15	국민건강보험공단	23	국립암센터
8	한국과학기술기획평가원	16	한국도로공사	24	공무원연금공단

자료: 과학기술정보통신부, 2026.8.

- 개정안은 「공공기관의 운영에 관한 법률」 제4조에 따라 지정된 공공기관 전체를 ISMS 인증 의무대상에 추가하려는 것으로, 정보통신망을 이용한 서비스를 제공하는 공공기관 또한 ISMS 인증을 받게 함으로써 정보보호 관리체계 인증의 실효성을 높이는 효과가 있을 것으로 보임.
- 다만, 개정안과 관련하여 다음의 사항을 고려할 필요가 있음.
- 첫째, 모든 공공기관을 기관 규모나 업무 특성과 관계없이 일률적으로 인증 의무대상으로 하는 것이 적정한지 검토할 필요가 있음.
- 현행법상 인증 의무대상도 주요정보통신서비스 제공자, 집적정보통신시설 사업자(데이터센터 사업자) 및 매출액·이용자 규모가 큰 사업자 등 처리하는 정보가 많거나 해당 서비스가 다른 정보통신서비스에 미치는 영향이 큰 사업자로 규정된 점을 감안하면, 공공기관도 기관마다 보유한 정보의 성격과 중요성이 차이가

있으므로 기관이 보유·처리하는 정보의 종류와 중요도, 개인정보 처리 규모, 대국민 정보서비스의 이용 규모 및 침해사고 발생 시 파급효과 등을 고려하여 의무대상과 인증범위를 합리적으로 설정할 필요가 있음.

- 둘째, ISMS 인증 및 심사 업무는 과학기술정보통신부가 직접 수행하지 않고 이를 수행할 정보보호 관리체계 인증기관과 정보보호 관리체계 심사기관을 지정⁶⁾하고 있는데, 현재 심사기관으로 지정된 기관은 모두 민간법인 또는 단체라는 점에서 공공기관의 보안상 민감한 정보나 정보보호 체계에 민간기관이 접근할 수 있게 되는 문제가 발생할 수 있음.
- 따라서, 공공기관의 ISMS 인증은 과학기술정보통신부가 인증업무를 직접 수행하거나 공공기관 대상 ISMS 인증·심사업무를 수행하는 별도의 공공기관을 지정하여 수행할 수 있도록 제한하는 방안 또는 심사기관에 대한 강화된 보안요건을 적용하여 관리·감독을 강화하고 심사기관의 독립성을 확보하기 위한 조치를 마련하는 등 방안을 고려할 필요가 있어 보임.
- 참고로, 공공기관에 대한 ISMS 인증 의무화와 관련한 내용으로 제22대 국회에서 발의된 3건의 유사한 개정안⁷⁾이 전체회의 상정

6) ·정보보호 관리체계 인증기관 : 한국인터넷진흥원(KISA), 금융보안원(FSI)
·정보보호 관리체계 심사기관 : 한국정보통신진흥협회(KAIT), 한국정보통신기술협회(TTA),
개인정보보호협회(OPA), 차세대정보보안인증원(NISC),
한국경영인증원(KMR), 한국생산성본부인증원(KPCQA)

7) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」(김기현 의원, 2212287)
「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」(차지호 의원, 2213021)

(2025.11.17.) 후 소위원회에 회부되어 있는 상황이므로 동 개정안과 함께 논의할 필요가 있음.

다. 정부 및 관련 단체 의견

1) 과학기술정보통신부, 국가정보원

- 공공기관의 정보보호에 관하여는 「국가정보원법」을 근거⁸⁾로 ISMS 인증제도와 유사한 ‘사이버보안 실태평가⁹⁾’를 실시 중이며, 유사 제도가 운영 중인 만큼 규제의 중복 적용 및 공공기관의 부담 가중 우려 등을 고려하여 신중한 검토가 필요함.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」(김상훈 의원, 2213361)

8) 「국가정보원법」

제4조(직무) ① 국정원은 다음 각 호의 직무를 수행한다. (중략)

4. 다음 각 목의 기관 대상 사이버공격 및 위협에 대한 예방 및 대응

가. 중앙행정기관(대통령 소속기관과 국무총리 소속기관을 포함한다) 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처 및 「행정기관 소속 위원회의 설치·운영에 관한 법률」에 따른 위원회

나. 지방자치단체와 그 소속기관

다. 그 밖에 대통령령으로 정하는 공공기관

「사이버안보 업무규정」

제13조(사이버보안 실태 평가) ① 국가정보원장은 중앙행정기관등의 사이버보안 업무 수행을 위한 조직, 인력, 예산, 직무교육 및 사이버보안에 대한 자체 진단·점검 등 사이버보안 실태를 평가할 수 있다. (이하 생략)

제7조(사이버보안 업무 대상 공공기관의 범위) 법 제4조제1항제4호다목에서 “대통령령으로 정하는 공공기관”이란 다음 각 호의 기관을 말한다.

1. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관

- 9) 국가정보원이 중앙행정기관 등에 대한 사이버보안 업무 수행을 위한 조직, 인력, 예산, 직무교육 및 사이버보안에 대한 자체 진단·점검 등 사이버보안 실태를 평가하는 제도로서 관리자 보안·기술적 보안·위기대응 역량 등 3개 분야 100개 지표로 구성됨(국가사이버안보센터 사이버보안 실태평가 제도소개 자료)

< ISMS 인증 - 사이버보안 실태평가 제도 비교 >

구분	ISMS 인증	사이버보안 실태평가
주관	과학기술정보통신부·인증기관	국가정보원
성격	정보보호 관리체계에 대한 인증	국가·공공기관의 사이버보안 업무 수행실태 평가
범위	관리체계, 조직·자산 등 관리적 부문과 물리적·기술적 보호대책 등	조직·인력·예산, 자체 점검, 기술적 보호조치, 위기대응 등
방식	서면·현장심사, 인증위원회 심의	기관평가·현장실사
후속관리	인증 유효기간 중 사후심사	평가결과 통보 및 개선조치
법적효과	인증 취득 여부가 법적 의무 충족과 연결	기관의 보안 수준 평가 및 개선
적용기관	정보통신망법상 의무대상	국가기관·공공기관 등 사이버안보 업무 대상

자료 : 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도 안내서 및
국가사이버안보센터 사이버보안 실태평가 제도소개 자료 바탕 재구성

문 의 처

02)6788-5235

참고

ISMS(ISMS-P) 제도

[출처] 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도 안내서
(과학기술정보통신부, 개인정보보호위원회, 한국인터넷진흥원)

□ 법적 근거

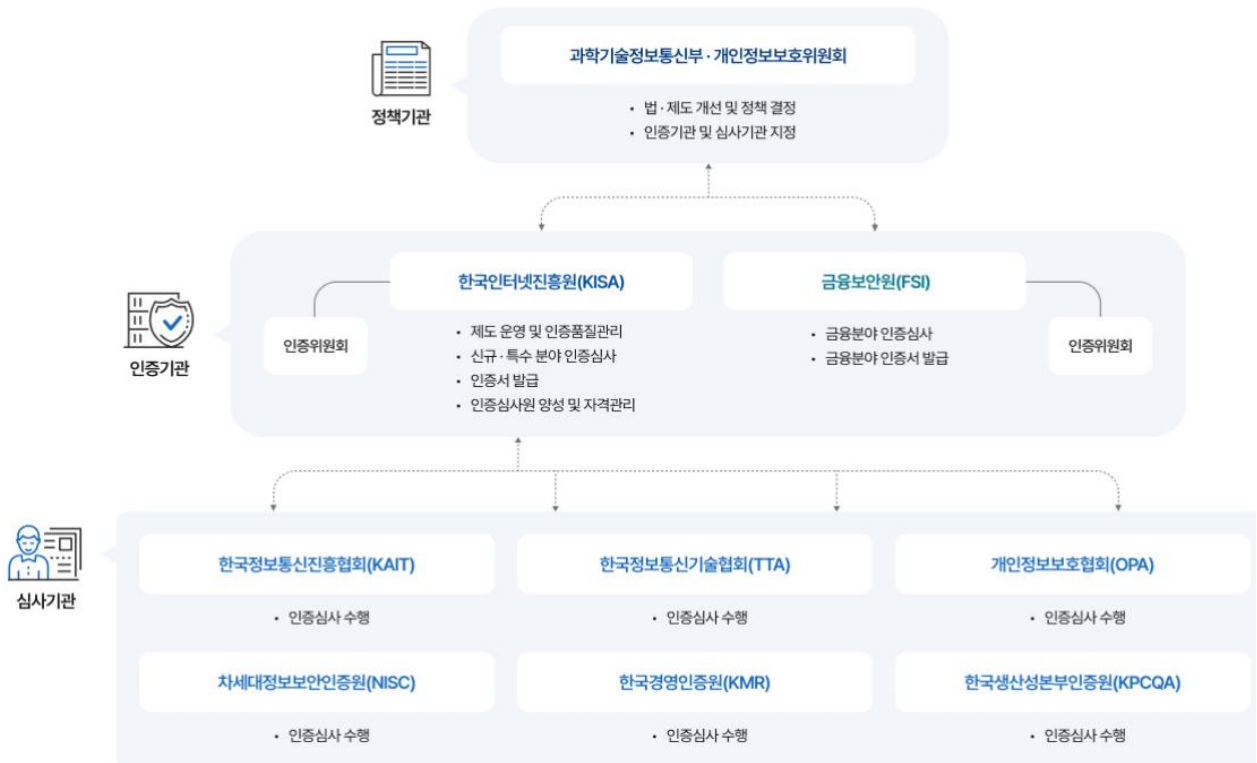
- 정보보호 및 개인정보보호 관리체계 인증제도는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조, 제47조의2 및 제47조의7, 같은 법 시행령 제47조부터 제54조의 규정 및 같은 법 시행규칙 제3조에 따른 정보보호 관리체계 인증과 「개인정보 보호법」 제32조의2, 같은 법 시행령 제34조의2부터 제34조의8의 규정에 따른 개인정보보호 관리체계 인증을 법적근거로 함.
- 과학기술정보통신부와 개인정보보호위원회는 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」를 공동으로 시행중임.

□ 인증 유형

인증의 유형		주요내용
정보보호 관리체계 인증 (ISMS)		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)		개인정보의 흐름과 정보보호 영역을 모두 인증하는 경우 보호하고자 하는 정보서비스가 개인정보의 흐름을 가지고 있어 개인정보 처리 단계별 보안강화가 필요한 조직
정보보호 관리체계 예비인증		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 있음.

□ 인증 추진체계



○ 정책기관(협의회)

- 과학기술정보통신부장관과 개인정보보호위원회는 ISMS-P 인증 운영에 관한 정책 사항을 협의하기 위하여 ISMS-P 인증 협의회를 구성하여 운영함.

○ 인증기관

- 법정 인증기관인 한국인터넷진흥원 또는 과학기술정보통신부장관과 개인정보보호위원회가 지정한 인증기관이 인증에 관한 업무를 수행함.
- 인증기관은 신청기관이 수립·운영하는 관리체계를 인증기준에 따라 심사하고, 인증위원회를 운영하여 인증기준에 적합한 기관에게 인증서를 발급함.

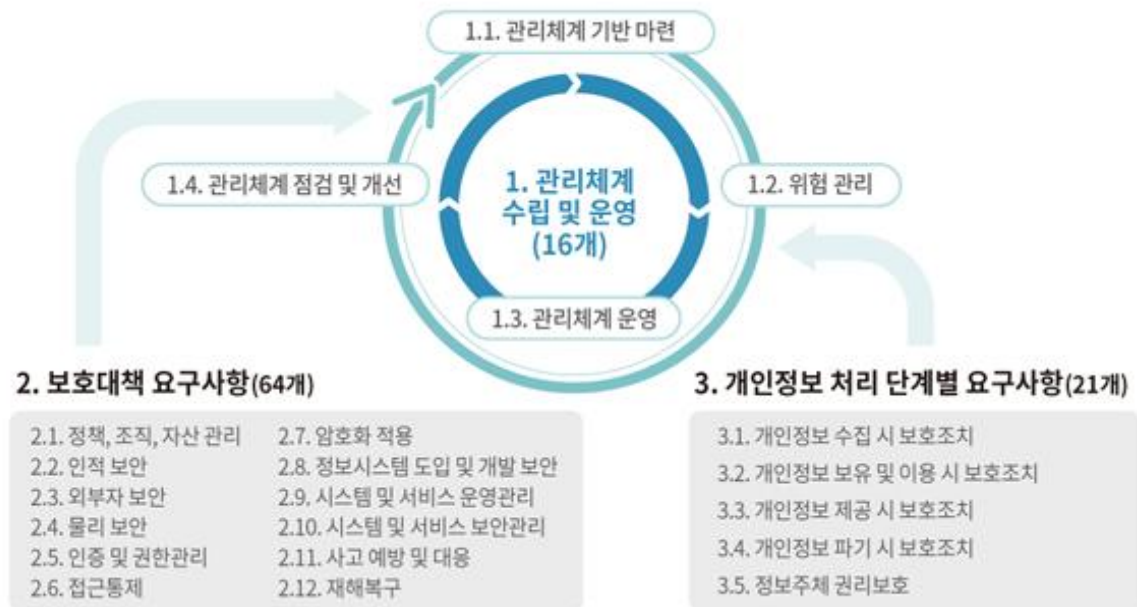
○ 인증위원회

- 인증위원회는 인증심사 결과가 인증기준에 적합한지 여부, 인증 취소에 관한 사항, 이의신청에 관한 사항 등을 심의·의결함.

○ 심사기관

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

□ 인증 기준



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