

ISMS + PIMS

인증제도 통합에 따른 고시 개정사항 안내

2018.11.13.



CHAPTER

I

ISMS, PIMS 인증제도
통합에 따른 고시 개정사항 안내

통합인증제도 알아보기

개요

인증제도 통합 추진배경

ISMS

Information Security Management System

정보보호 관리체계 인증

2001 ISMS 인증제도 도입

2002 인증기준 고시 제정

2013 인증 의무화

※ 정보보호 안전진단 제도 폐지

2014 인증기관 심사기관 추가 지정

2015 인증 의무대상 확대

PIMS

Personal Information Management System

개인정보보호 관리체계 인증

2010 방통위 의결 기반 PIMS 시행

2012 정보통신망법에 법률적 근거 마련

※ 대상: 정보통신서비스 제공 사업자

2013 개인정보보호법 기반 PIPL 제도 시행

※ 대상: 공공기관/대기업, 중소기업, 소상공인

2016 PIMS, PIPL 인증제도 통합

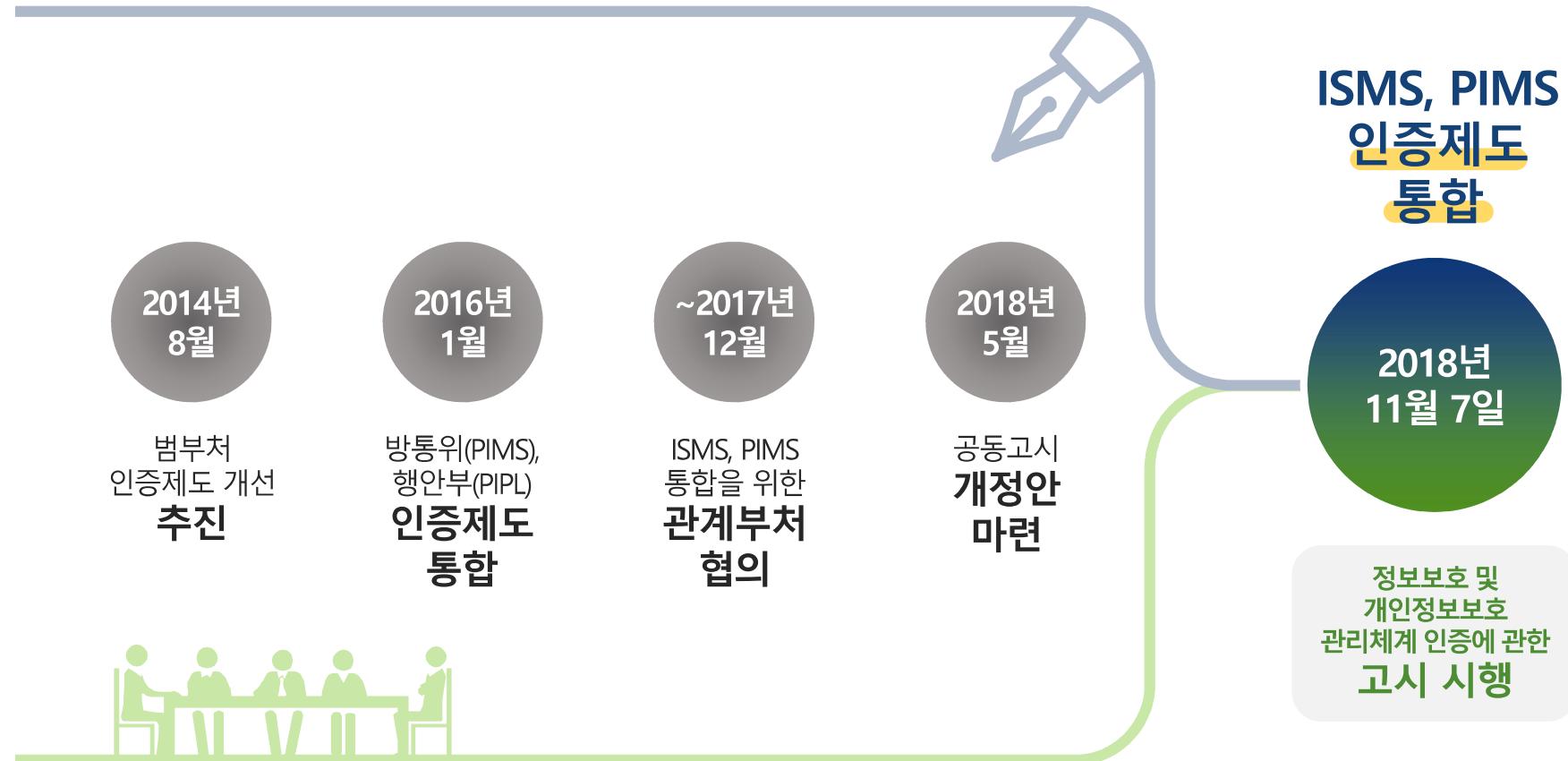
융합화, 고도화되고 있는 침해위협에 효과적인 대응을 위해

정보보호와 개인정보보호의 연계 필요

심사항목이 유사하고 개별 운영에 따른 **기업의 혼란 및 재정·인력상 부담 발생**

ISMS, PIMS 통합 추진

추진경과



기대효과

ISMS·PIMS
인증제도 통합을 통해
복수의 인증제도
운영에 따른
기업 혼란 해소

'통합이 필요하다'
59.9%

2016년 기업대상
ISMS 인증제도
인식조사 설문

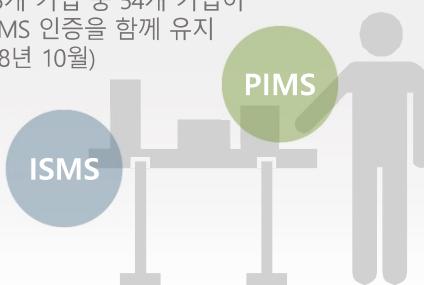


융합화·고도화되는
침해위협에
효과적으로 대응
가능

정보시스템(ISMS)의 안정성과
개인정보 흐름(PIMS) 상에서의
위험성을 함께 고려

PIMS, ISMS 인증 모두 유지
72%

PIMS 인증을 유지하는
75개 기업 중 54개 기업이
ISMS 인증을 함께 유지
(18년 10월)



신청기관이
인증에 소요되는
비용·행정·인력
부담 절감

ISMS, PIMS 제도 개별 운영
중인 행정절차 및
인증심사 절차를 통합

'타 규제제도와의
중복에 따른
비용·행정·인력적
부담이 가장 크다'

2016년 기업대상
ISMS 인증제도
인식조사 설문



법령과의 관계

법령



과학기술정보통신부

정보통신망법
제47조
시행령 제47조~제54조
시행규칙 제3조



방송통신위원회

정보통신망법
제47조의 3
시행령 제54조의2



행정안전부

개인정보보호법
제32조의2
시행령 제34조의2~제43조의7

고시

정보보호
관리체계 인증 등에
관한 고시(ISMS)

개인정보보호
관리체계 인증 등에 관한 고시(PIMS)

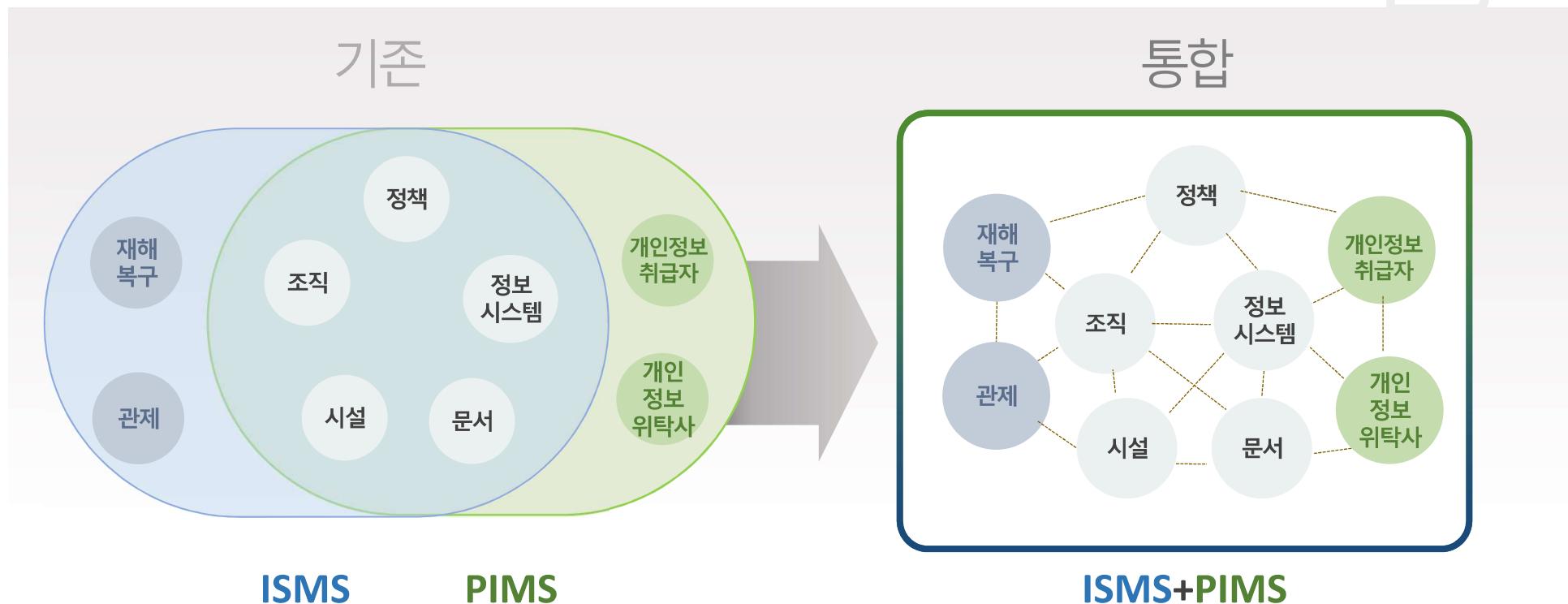
통합

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(ISMS-P)
과학기술정보통신부 | 방송통신위원회 | 행정안전부 공동고시

통합 인증 개요

I | 2

정보와 개인정보를 단일제도에서
체계적으로 보호할 수 있도록 인증제도 통합



통합 인증 개요

1 | 2

개요



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

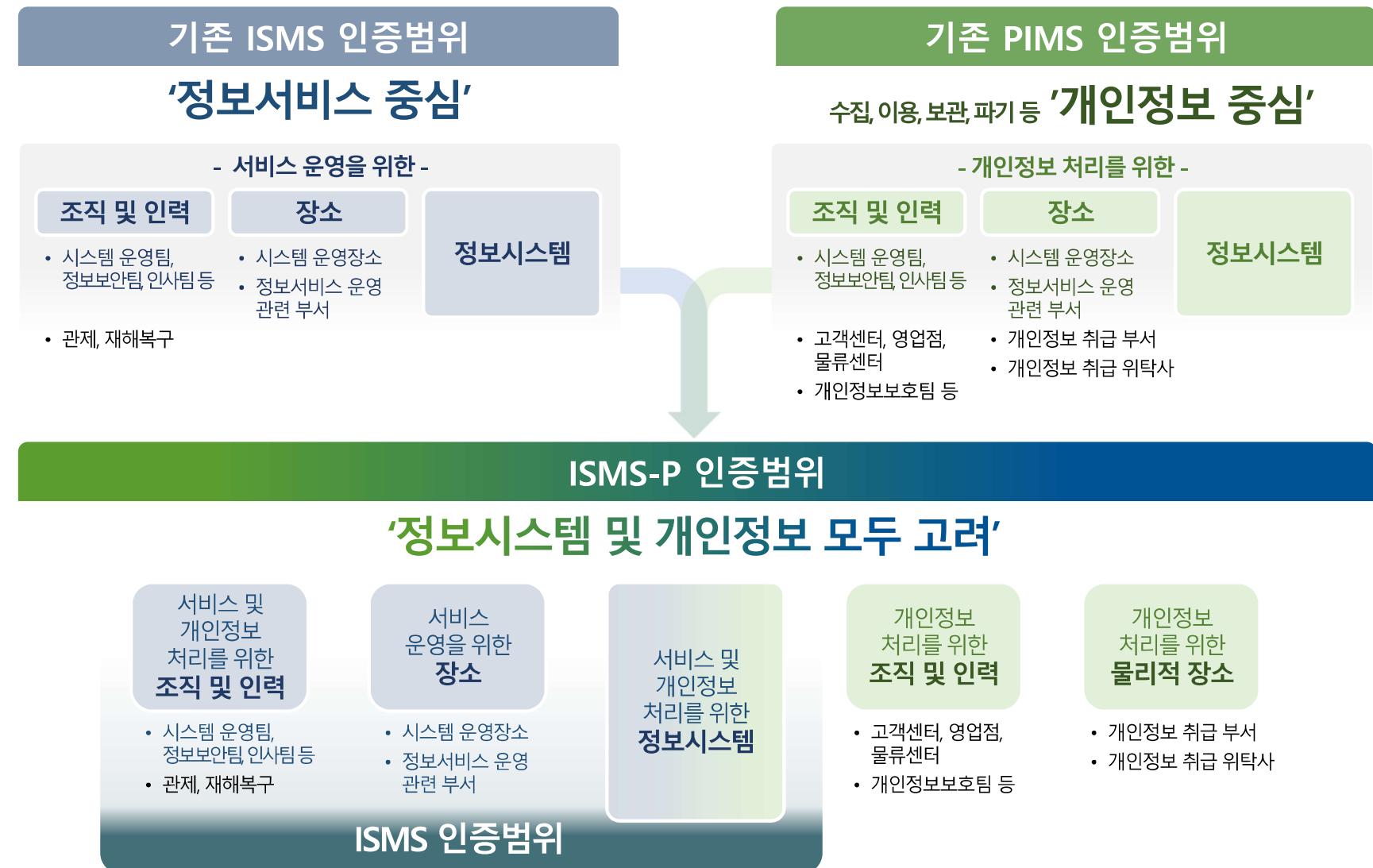


정보보호 관리체계 인증(ISMS)

정보보호 중심으로 인증하는 경우

기존의 ISMS 의무대상 기업·기관,
개인정보를 보유하지 않거나 개인정보 흐름의 보호가 불필요한 조직 등

통합 인증 범위



CHAPTER

II

ISMS, PIMS 인증제도
통합에 따른 고시 개정사항 안내

통합인증제도 알아보기
인증체계

어떤 기관에서
인증업무를
하게 되나요?



담당 기관 및 체계



인증기관·심사기관 지정

신규지정 절차

고시 제6조, 제7조, 별표2



재지정 절차

고시 제9조, 별표2

기존 인증기관 또는 심사기관
유효기간 종료 6개월 전부터 종료일까지 재지정 신청
(재지정 공고 없음)

공정성 및 독립성 확보

고시 제10조

인증심사의 공정성 및 독립성 확보를 위해
관련 컨설팅 수행, 인증절차 생략, 심사에 영향력 행사 등 금지 노력

참고

고시 시행 이전 인증기관, 심사기관 경과규정

고시 부칙 제3조

- 지정서의 유효기간까지 기존 ISMS 인증기준으로 심사 가능
- KAIT('20년 4월 6일 까지), TTA('21년 2월 8일까지), 금융보안원('21년 7월 9일까지)
- 단, 신규로 지정 받은 경우 새로운 지정서 유효기간까지 기존 ISMS 인증기준으로 사후심사 가능



CHAPTER

III

ISMS, PIMS 인증제도
통합에 따른 고시 개정사항 안내

통합인증제도 알아보기
인증기준

인증 기준이
어떻게
바뀌었나요?



인증 기준 변경사항

1 | 2

인증
기준



참고

- PIMS의 규모별 인증기준 폐지
- ISMS 인증을 받더라도 범위 내 개인정보의 보호대책 및 준거성은 충족하여야 함
- 세부 점검 항목은 홈페이지 (<https://isms.kisa.or.kr>) 배포



인증 기준 변경사항

1 | 2

유사·중복항목 통합 및 재배치



유사·중복항목 통합 예시

(통합) 2.1.1 정책의 유지관리

정책의 공표 + 정책의 검토
+ 정책문서 관리

(통합) 2.5.4 비밀번호 관리

사용자 패스워드 관리
+ 이용자 패스워드 관리

(통합) 3.1.3 주민등록번호 처리 제한

주민등록번호 수집이용제한
+ 주민등록번호 대체 수단

(통합) 3.5.2 정보주체 권리 보장

권리행사의 방법 및 절차
+ 개인정보 열람 + 개인정보 정정, 삭제
+ 개인정보 처리정지

최신 기술 및 이슈 반영

클라우드 서비스, 핀테크, 외부자 관리,
침해사고 탐지 강화 등을 반영한
신규기준 개발 및 기존항목 개선

신규 및 개선 예시

- 신규 -

1.2.2 현황 및 흐름분석

2.10.2 클라우드 보안

2.3.1 외부자 현황 관리

⋮

- 기존항목 개선 -

2.11.3 이상행위 분석 및 모니터링

2.10.4 전자거래 및 핀테크 보안

⋮

법개정에 따른 요구사항 반영

개인정보보호법, 정보통신망법의
개정에 따라
추가, 강화된 보호조치 반영 필요

법개정에 따라 추가된 인증기준

3.1.7 홍보 및 마케팅 목적 활용 시 조치

3.2.4. 이용자 단말기 접근 보호

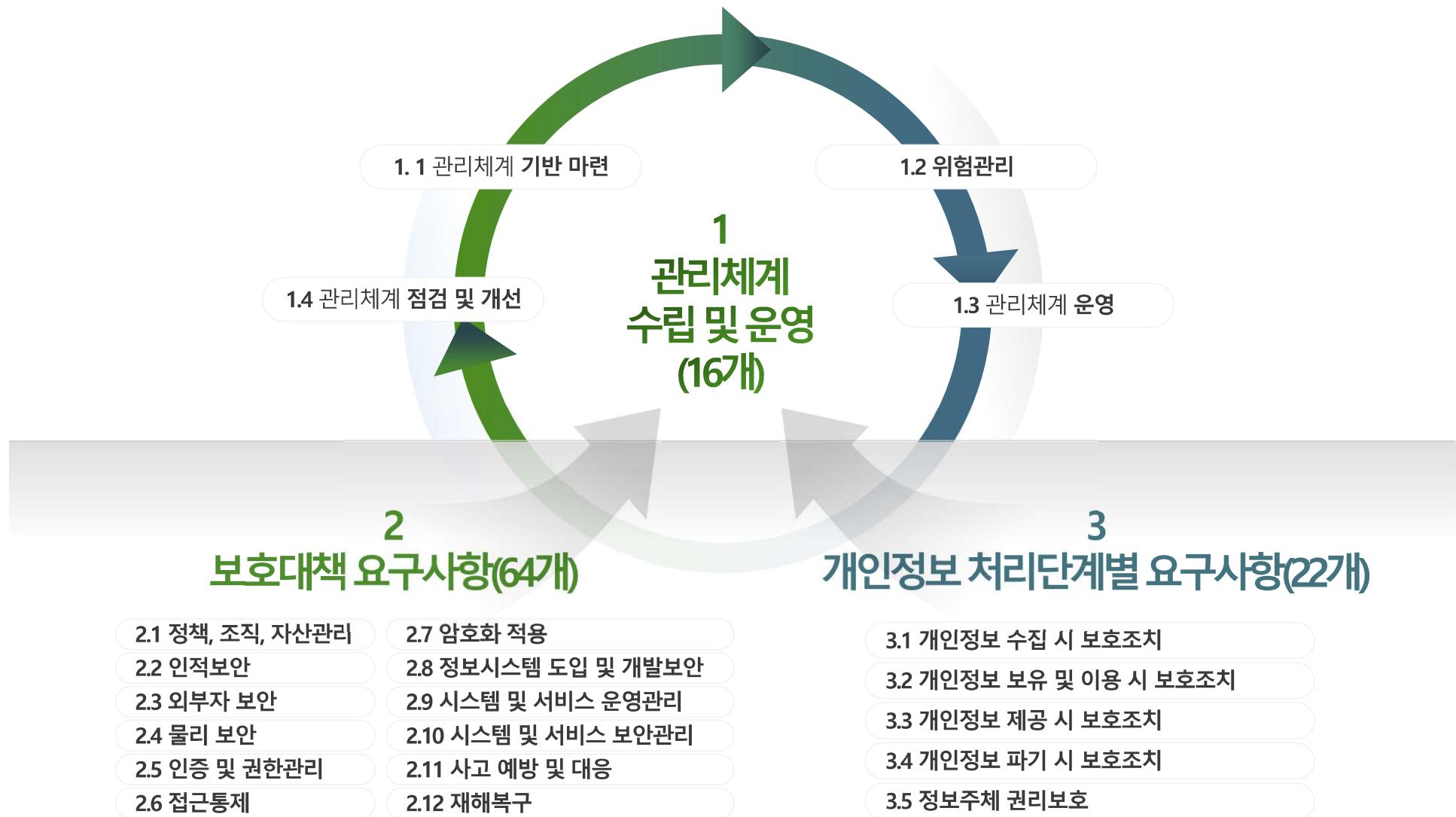
3.3.4 개인정보의 국외이전,

3.4.2. 처리목적 달성 후 보유 시 조치

3.4.3 휴면 이용자 관리

통합 인증기준 개념

인증기준 통합 (고시 별표 7)



인증심사 생략 대상 및 요건

ISMS 일부 심사 생략을 받을 수 있는 대상 (고시 제20조 제1항)

아래의 인증 또는 정보보호 조치를 한 자

ISO/IEC 27001 인증을 받은 자

「정보통신기반 보호법」 제9조에 따른
취약점의 분석·평가를 받은 자

- **ISMS 단일 인증만 가능**하며 ISMS-P 인증, 혼합인증은 일부 생략을 할 수 없음
- 생략은 최초·갱신 심사 시점에 신청이 원칙이며 사후심사 때 생략 신청 시 인증서 변경 등의 절차 필요

생략 요건 (고시 제20조 제2항)

- 국제표준 정보보호 인증 또는 정보보호 조치의 범위가 **정보보호 관리체계 인증의 범위와 일치할** 것
- 정보보호 관리체계 인증 **심사 시에** 국제표준 정보보호 인증 또는 정보보호 조치가 **유효할** 것

생략 신청 (고시 제20조 제3항)

인증심사 일부 생략
신청서를 작성하여 인증신청 시 제출



생략 사항 인증서 표기 (고시 제20조 제4항)

인증심사의 일부를 생략하여 심사한 경우에는
그 사실을 인증서에 표기

인증심사 생략 항목

고시 별표5

분야		항목	
2.1	정책, 조직, 자산 관리	2.1.1	정책의 유지관리
		2.1.2	조직의 유지관리
		2.1.3	정보자산 관리
2.2	인적 보안	2.2.1	주요 직무자 지정 및 관리
		2.2.2	직무 분리
		2.2.3	보안 서약
		2.2.4	인식제고 및 교육훈련
		2.2.5	퇴직 및 직무변경 관리
		2.2.6	보안 위반 시 조치
2.3	외부자 보안	2.3.1	외부자 현황 관리
		2.3.2	외부자 계약 시 보안
		2.3.3	외부자 보안 이행 관리
		2.3.4	외부자 계약 변경 및 만료 시 보안
2.4	물리 보안	2.4.1	보호구역 지정
		2.4.2	출입통제
		2.4.3	정보시스템 보호
		2.4.4	보호설비 운영
		2.4.5	보호구역 내 작업
		2.4.6	반출입 기기 통제
		2.4.7	업무 환경 보안
2.12	재해복구	2.12.1	재해, 재난 대비 안전조치
		2.12.2	재해 복구 시험 및 개선

CHAPTER

IV

ISMS, PIMS 인증제도
통합에 따른 고시 개정사항 안내

통합인증제도 알아보기
인증 절차

통합인증을
어떻게 받을 수
있나요?



인증신청 개요

개정 전 인증기준으로 고시 시행 후 6개월 까지 최초, 간신심사 가능
인증범위 내 개인정보를 보유하더라도 기업의 자율판단으로 ISMS, ISMS-P 선택

심사 신청

고시 시행 이전 기준으로
심사 수행 (고시 부칙 제4조)
※ 인증심사일 기준

최초심사, 간신심사

고시 시행 후 6개월(2019년 5월 7일)까지 기존 기준으로
인증심사 가능

사후심사

인증서의 유효기간까지 기존 취득한 인증기준으로
사후심사 가능

신규 기준으로
심사 신청

고시 시행일부터 신규 기준으로 **최초심사를** 준비하여 신청
기준 인증취득 기업·기관은 인증범위 조정 및 인증서 변경
시 상담 필요

인증에 따른 심사 구분

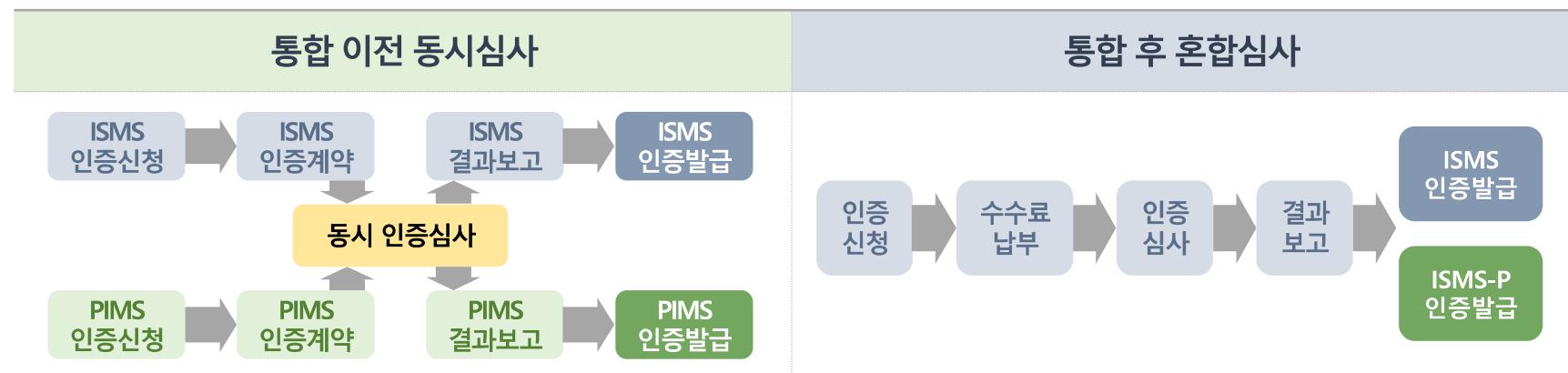
단일심사

- 하나의 인증만 신청하는 경우(예: ISMS 인증만 신청, ISMS-P 인증만 신청)



혼합심사

- 같은 관리체계 내에서 일부 서비스만 개인정보보호를 포함하여 인증을 받고자 하는 혼합심사의 경우 수수료와 심사과정을 통합하였으며 유효기간 및 심사주기가 동일하고 범위만 다른 2장의 인증서 발급
 - 예시) ISMS 인증 범위(금고서비스 운영), ISMS-P 인증 범위(인터넷뱅킹 서비스 운영)
 - 다른 기간에 개별로 받는 인증은 해당되지 않음 (예: 상반기 ISMS, 하반기 ISMS-P 인증)



인증 의무 대상자

■ 의무 대상자는 인증 선택 가능 (고시 제19조제3항)

정보보호 관리체계 인증

정보보호 및 개인정보보호 관리체계 인증

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

- 인증 의무 취득기간을 '매년 1월~12월'에서 '**차년도 8.31까지**'로 개정하고 '19년도 의무 대상자'부터 적용
- 다만, 이 고시 시행 이전에 의무대상자가 된 자로서 최초의 인증신청을 신규인증기준으로 하는 경우에는 개정 규정을 적용

참고

- 제19조 제4항은 인증을 취득하지 않은 신규 의무 대상자의 인증취득에 해당하는 조항이며, 이미 인증을 취득한 사후, 간접심사 대상자는 해당되지 않음
- 인증을 취득한 자가 인증의무기간 유예를 위해 고의로 인증을 취소하고 다시 신청하는 것은 제19조제4항에 해당하지 않으며 과태료 대상이 됨
- 18년 의무대상자인 인증취득기업이 기존 인증을 취소하고 신규 인증으로 받는다면
· 18년 12월 31일까지 인증을 취득해야 함



인증수수료

인증수수료 (별표6)

직접 인건비 + 제경비 + 기술료 + 직접경비

직접인건비
인증심사에
투입되는
인증심사원에
대한 인건비로 산정

제경비
최대
(직접인건비×120%)

기술료
최대
{(직접인건비+제경비)
×40% }

직접경비
교통비, 숙박비 및
식대 등
인증심사업무에
소요되는 직접적인
경비



수수료 지원 (고시 제21조 제3항)

- 「중소기업기본법」 제2조에 따른
소기업에 해당되는 경우
- 인증심사 일부 생략을 신청을 하는 경우(ISMS)
- 정보보호 공시를 한 경우(ISMS)

※ 중복할인 불가, 직접경비 할인 제외, 할인율 별도 공지

수수료 납부 기간 (고시 제22조)

기존

신청기관은 인증심사 계약을 체결한 날로부터 1개월 이내에
인증 수수료를 인터넷진흥원·인증기관 또는 심사기관에 납부

개선

수수료를 청구 받은 날부터 인증심사 시작일 이전까지
심사수행기관에 납부하여야 하며 그렇지 않은 경우
심사수행기관은 인증심사를 실시하지 아니할 수 있다.

인증수수료

수수료 산정 시 입력 값

ISMS 기본수수료	ISMS-P 또는 ISMS+ISMS-P
정보시스템수, 인력 수	정보시스템수, 인력 수, 심사복잡도*

* 심사복잡도 : ISMS-P는 개인정보위탁사, 서비스 수에 따라 추가금액 적용

→ ISMS는 현행 수준 유지, PIMS의 경우 35% 수수료 인하, 2개 인증을 함께 유지한 경우 59% 수수료 인하 효과 가능



보완조치 및 사후관리

보완조치 기간 확대

고시 제25조 제4항

- **보완조치 기간 기존 30일에서 40일로 확대**
(보완조치 기간 이내 심사팀장의 확인이 완료되어야 함)
- **보완조치 사항 미흡 시 재조치 요구기간은 60일 유지**

보완조치 종료 시점 기준

- 심사팀장이 이행점검을 완료하고 완료확인서에 서명하는 일자가 최종 일자가 됨
- 조치 완료일이 휴일이면 휴일이 종료되는 날짜 다음날까지 제출하도록 산정

- **신규기준부터 적용**

사후관리

고시 제27조 제3항



- 사후심사는 1년 주기로 심사를 받아야 함
- 인증 취득한 범위와 관련하여 침해사고 또는 개인정보 유출사고가 발생한 경우 **인터넷진흥원은 필요에 따라 인증관련 항목의 보안향상을 위한 필요한 지원**

갱신심사 신청

고시 제28조

- **사후심사, 갱신심사 연장신청 불가**
- **갱신심사는 유효기간 만료 3개월 전에 신청하여야 하며 신청하지 않고 유효기간이 경과한 때에는 인증의 효력은 상실된다.**

인증위원회

인증위원 풀 구성 및 상시운영 기반 마련

(고시 제29조)

- **인증위원회** 심의·의결 사항
 1. 최초심사 또는 간접심사 결과가 인증기준에 적합한지 여부
 2. 제35조제1항에 따른 인증의 취소에 관한 사항
 3. 제36조에 따른 이의신청에 관한 사항
 4. 그 밖에 정보보호 및 개인정보보호 관리체계 인증과 관련하여 위원장이 필요하다고 인정하는 사항
- **인증위원회는 다양한 분야의 전문가가 포함되는 35인 이내 위원으로 구성(인증위원 pool 구성)**
- 회의마다 전문분야를 고려하여 **6인 이상의 인증위원으로 구성 및 인증위원회 운영**
⇒ 개최빈도를 높여 신청기관의 편의제고 강화

인증번호 체계 및 현황공개

인증현황 공개

(고시 제34조제3항)

인터넷진흥원은 인증정보를 제공하는 홈페이지를 통해 인증현황을 공개



인증번호 체계

(고시 제32조제2항, 별표 8)

ISMS - P - OOOO - 20XX - 0000

P표기	인증기관	인증연도	일련번호
개인정보 포함 시	약자로 표기	최초발행 연도	연도 내 부여순서

인증 마크

(고시 제34조제1항, 별표 8)



인증서

(별지 11호, 12호 서식)

정보보호 및 개인정보보호 관리체계 인증서

1.인증번호 : ISMS-P-KISA-2018-0001

2.업 체 명 : OOOOOO

3.대 표 자 : OOO

4.주 소 : 서울특별시 OOO구 OOO로 OOO

5.인증의 범위 : OOO 서비스 운영

6.유효기간 : 2018년 12월 10일 ~ 2022년 12월 9일

7.심사수행기관 : 한국인터넷진흥원

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항, 제47조의3 제1항, 같은 법 시행령 제47조, 「개인정보 보호법」 제32조의2에 따라 위와 같이 정보보호 및 개인정보보호 관리체계를 인증합니다.

년 월 일

인증기관의 장 직인



정보보호 관리체계 인증서

1.인증번호 : ISMS-KISA-2018-0001

2.업 체 명 : OOOOOO

3.대 표 자 : OOO

4.주 소 : 서울특별시 OOO구 OOO로 OOO

5.인증의 범위 : OOO 서비스 운영

※ 심사 생략 범위 : ISO/IEC 27001 'OOOO 서비스 운영'관련 일부 심사 생략

6.유효기간 : 2018년 12월 10일 ~ 2022년 12월 9일

7.심사수행기관 : 한국인터넷진흥원

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계를 인증합니다.

년 월 일

인증기관의 장 직인



CHAPTER

V

ISMS, PIMS 인증제도
통합에 따른 고시 개정사항 안내

인증 심사원 안내

정보보호
경력이 있는데 ...
인증심사원이
될 수 있을까요?



신규 심사원 자격요건

신규심사원 자격 신청 요건

고시 제13조 별표4



참고

- ✓ 두 가지 이상 중복 업무경력인 경우에 경력기간을 중복하여 합산하지 않음
- ✓ 모든 해당 경력은 신청일 기준 최근 **10년 이내의 경력에 한해 인정**
- ✓ 정보보호 또는 개인정보보호 필수 경력을 옆 표와 같이 대체할 수 있으며 **중복 인정불가**
- ✓ 신청일 기준 취득 완료한 자격만 인정

4년제 대학졸업 이상 또는 이와 동등학력을 취득

정보보호, 개인정보보호 또는 정보기술 경력을 합하여 6년 이상을 보유

정보보호 및 개인정보보호 경력을 각 1년 이상 필수로 보유

구분	경력 인정 요건(중복인정 불가)	인정기간
정보보호 경력	• 정보보호 관련 박사학위 취득자	2년
	• 정보보호 관련 석사 학위 취득자 • 정보보안기사, CISA, CISSP	1년
개인정보보호 경력	• 개인정보보호 관련 박사학위 취득자	2년
	• 개인정보보호 관련 석사 학위 취득자 • 개인정보 영향평가 전문인력, CPPG	1년
정보기술 경력	• 정보기술 관련 박사학위 취득자 • 정보관리기술사, 컴퓨터시스템응용기술사 • 정보시스템감리사	2년
	• 정보기술 관련 석사학위 취득자 • 정보시스템감리원 • 정보처리기사, 전자계산기조작응용기사	1년

인증심사원 자격전환 및 등급 조정

고시 시행 이전 ISMS, PIMS 인증 심사원 경과규정

고시 부칙 제3조 제1항

**고시 시행 후 6개월 또는
심사원 자격 유효기간 중 더 긴 기간까지**
이 고시 시행이전 인증기준의 심사에 참여 가능

자격전환

고시 부칙 제3조제2항



고시 시행 후 6개월 또는 심사원 자격 유효기간 중
더 긴 기간 이내에
**인터넷진흥원이 실시하는 심사원 자격전환
과정을 신청하고 자격전환 과정을 수료**

구분	전환 방안
ISMS, PIMS 자격 모두 보유	1일 신규 제도에 관한 교육
1개 자격만 보유	2일 교육 및 평가시험

※ 자격전환 과정은 개별 심사원에게 별도 안내

기존 심사원 등급 재조정

고시 제12조, 별표3

- ✓ 기존 등급을 초기화 하고 ISMS, PIMS 심사경력을 합산한 신규등급으로 조정 (고시 부칙 제3조제3항)
- ✓ 심사팀장만 가능했던 기존 선임심사원 등급을 초기화하고 ISMS-P 심사참여 일수로 요건 완화

등급

요건

심사원보

인증심사원 자격 신청 요건을 만족하는 자로서
인터넷진흥원이 수행하는 인증심사원 양성과정을
통과하여 자격을 취득한 자

심사원

심사원보 자격 취득자로서 인증심사에 4회 이상
참여하고 심사일수의 합이 20일 이상인 자

선임 심사원

심사원 자격 취득자로서 **정보보호 및 개인정보보호
관리체계 인증심사(ISMS-P)를 3회 이상 참여하고 심
사일수의 합이 15일 이상인 자**

책임심사원

책임심사원 (고시 별표3, KISA 지침)

- 심사능력이 우수하고 참여율이 높은 심사원에 대해 책임심사원 등급부여(기간 1년)

등급	요건
책임심사원	<p>선임심사원이 매년 1월 1일 기준으로 1년 동안 다음의 요건을 모두 만족하는 경우 다음해 1년 동안 책임심사원으로 활동</p> <ol style="list-style-type: none"> 1. ISMS-P 2회를 포함하여 인증심사 4회 이상 참여하고 심사일수의 합이 20일 이상 2. 최초 또는 간접심사 1회 이상 참여 3. 인증심사 수행 결과에 대한 심사원 평가* 총족 <p>※ 인터넷진흥원은 매년 1월 책임심사원을 선정하고 해당 심사원에 그 결과를 안내 ※ 책임심사원 요건은 추후 변경될 수 있으며 변경 시 공지 예정</p>

*심사원 평가 기준 (KISA 지침)

평가항목	평가방법
인증기준 이해력	분야 전문성, 자료요구 및 인터뷰 내용과 인증기준과의 연관성 등
심사보고서 작성능력	양식작성, 문맥오류, 보고서의 논리력 및 전달력, 기한 내 작성 등
피심사자와의 의사소통 능력	인터뷰 언행, 자료요구 및 현장심사 태도 등
결함 판단 능력	정보수집력, 결함에 따른 조치방안의 적절성 등
협업 및 심사태도	심사팀 내 의견제시, 심사참여 적극성, 심사준비, 시간준수, 복장, 보안의식 등
인증심사관련 이의제기	타당성이 인정된 민원 접수 건

인증심사원 자문료

심사원 자문료 (별표6, KISA 지침)

- 소프트웨어산업진흥법 제22조제4항에 따른 **소프트웨어기술자의 일일 노임단가를 참고하고 인증 수수료 인상률을 고려하여 적용**

인증심사원 등급	1일 자문료
----------	--------

심사원보 200,000원

심사원 300,000원

선임심사원 350,000원

책임심사원 450,000원



심사원 자격 유지요건 및 보수교육

■ 심사원 자격 유지 요건

고시 제15조

자격 유효기간 만료 전까지
KISA가 인정하는 보수교육 수료
고시 제15조제2항

※의무시간에 해당하는 보수교육을 수료하여야함

심사원이 인증심사를 참여한 경우
보수교육 시간 중 일부 인정
고시 제15조제3항

KISA는 보수교육 운영에 관한
세부내용을
홈페이지에 사전 공지
고시 제15조제5항

■ 심사원 보수교육

KISA 지침

- ✓ 인터넷진흥원이 인정하는 보수교육을 유효기간(3년) 이내 42시간 이상 수료
- ✓ 보수교육 구분(KISA 운영)

- **필수교육**: 1일 (7시간, 무료과정)
- **선택교육**(심사대체과정) : 5일 (35시간, 유료과정)

※1일 단위 개별 운영

- ✓ 인증심사 5일 참여시마다 선택교육 1일(7시간)을 이수한 것으로 인정



심사원 자격 취소 요건

■ 심사원 자격 취소 요건 (고시 제16조)

- 거짓이나 부정한 방법으로 인증심사원 자격을 부여 받은 경우
- 인증심사원으로서 객관적이고 공정한 인증심사를 수행하지 않은 경우
- 인증심사 업무와 관련하여 고의 또는 중대한 과실로 인터넷진흥원, 인증기관, 심사기관, 인증신청인 등에게 손해를 끼친 경우
- 인증심사 과정에서 취득한 정보 또는 서류를 관련 법령의 근거나 인증신청인의 동의 없이 누설 또는 유출하거나 업무목적 외에 이를 사용한 경우
- 인증신청인으로부터 금전, 금품, 향응, 이익 등을 부당하게 수수하거나 요구한 경우



CHAPTER

VI

ISMS, PIMS 인증제도
통합에 따른 고시 개정사항 안내

통합고시 주요 개정사항



고시 주요 개정사항(종합)

구분	ISMS	PIMS	ISMS-P
제도명칭	정보보호 관리체계의 인증	개인정보보호 관리체계의 인증	정보보호 및 개인정보보호 관리체계 인증
정책기관	과기정통부	방통위, 행안부	<ul style="list-style-type: none"> 과기정통부, 방통위, 행안부 <p>※ 관계부처 협의회 구성</p>
인증기관 심사기관 지정	<ul style="list-style-type: none"> 지정 : 과기정통부 지정대상 : 인증기관, 심사기관 	<ul style="list-style-type: none"> 공동지정 : 방통위, 행안부 지정대상 : 심사기관 	<ul style="list-style-type: none"> 공동지정 : 과기정통부, 방통위, 행안부 지정대상 : 인증기관, 심사기관
인증기준	<ul style="list-style-type: none"> 104개 인증기준 <ul style="list-style-type: none"> - 관리과정(12) - 정보보호 대책(92) 	<ul style="list-style-type: none"> 86개 인증기준 <ul style="list-style-type: none"> - 관리과정(16) - 보호대책(50) - 생명주기(20) <p>※ 유형 별 차등적용</p>	<ul style="list-style-type: none"> 102개 인증기준 <ul style="list-style-type: none"> - 관리체계 수립 및 운영(16) - 보호대책 요구사항(64) - 개인정보 처리단계별 요구사항(22)
심사원 요건	<ul style="list-style-type: none"> 4년제 대학졸업 이상 학력 정보통신 또는 정보 보호 유관 경력 합산 : 6년 	<ul style="list-style-type: none"> 4년제 대학졸업 이상 학력 정보통신 또는 정보 보호 유관 경력 합산 : 6년 <ul style="list-style-type: none"> - 필수 개인정보보호 경력 : 2년 	<ul style="list-style-type: none"> 4년제 대학졸업 이상 학력 정보보호, 개인정보보호, 정보기술경력 합산 : 6년 <ul style="list-style-type: none"> - 필수 정보보호 경력: 1년 - 필수 개인정보보호 경력 : 1년

고시 주요 개정사항(종합)

구분	ISMS	PIMS	ISMS-P
심사원 등급체계	<ul style="list-style-type: none"> 선임심사원 : 심사원 자격으로 3회, 15일 이상 인증심사업무 총괄 심사원 : 심사원보 자격으로 인증심사 4회, 20일 이상 심사원보 : 최초자격 취득 	<ul style="list-style-type: none"> 선임심사원 : 심사원 자격으로 3회, 15일 이상 인증심사업무 총괄 심사원 : 심사원보 자격으로 인증심사 4회, 20일 이상 심사원보 : 최초자격 취득 	<ul style="list-style-type: none"> 선임심사원 : 심사원 자격으로 3회, 15일 이상 <u>ISMS-P 심사 참여</u> 심사원 : 심사원보 자격으로 인증심사 4회, 20일 이상 심사원보 : 최초자격 취득 <p>※ 심사능력에 따른 책임심사원 지정</p>
의무대상자 취득시기	매년 1월1일부터 12월31일까지 인증	해당없음	다음 해 8월31일까지 인증을 받을 수 있도록 기간 변경
인증심사 보완조치	<u>최대 90일</u> (재조치 요구 60일 포함)	<u>최대 90일</u> (재조치 요구 60일 포함)	<u>최대 100일</u> (재조치 요구 60일 포함)
인증마크			 



이상으로 인증제도 통합에 따른 고시 개정사항 안내를 마칩니다

감사합니다

