ISMS-P 인증의 이해

SK_cloud_26th 김윤호

1. 정보보호 및 관리체계의 법적 근거와 고시명,주무부처 기재

정보보호 및 개인정보보호 관리체계 인증(ISMS-P)
개인정보보호 관리체계 인증(PIMS)'과 '정보보호 관리체계 인증(ISMS)'으로 개별 운영되던 인증체계를 하나로 통합한 '통합인증제도'로 2018년 11월 7일부터 시행되었다.[1)]

- 법적 근거

「개인정보 보호법」 제32조(개인정보 보호 인증)
「개인정보 보호법 시행령」 제32조

- 고시명

「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」

- 제1조(목적)

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다) 제47조제3항·제4항, 같은 법 시행령 제47조부터 제53조의2까지의 규정 및 같은 법 시행규칙 제3조에 따른 정보보호 관리체계 인증과, 「개인정보 보호법」 제32조의2, 같은 법 시행령 제34조의2부터 제34조의8까지의 규정에 따른 개인정보보호 인증의 통합 운영에 필요한 사항을 정하는 것을 목적으로 한다.

- 주무부처

개인정보보호위원회 + 과학기술정보통신부 공동 주관, KISA 운영

---

1) 개인정보보호위원회, https://www.pipc.go.kr/np/default/page.do?mCode=I030020000

2. 정보보호 및 개인정보보호 관리체계의 인증기준 구분 기재

정보보호 및 개인정보보호 관리체계 인증기준은 크게 '1. 관리체계 수립 및 운영', '2. 보호대책 요구사항', '3. 개인정보 처리 단계별 요구사항' 3개 영역에서 총 102개의 인증기준으로 구성되어 있다. 정보보호 관리체계(ISMS) 인증을 받고자 하는 신청기관은 '1. 관리체계 수립 및 운영', '2. 보호대책 요구사항' 2개 영역에서 80개의 인증기준을 적용받게 되며, 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증을 받고자 하는 신청기관은 '3. 개인정보 처리 단계별 요구사항'을 포함하여 102개의 인증기준을 적용받게 된다.

< ISMS, ISMS-P 기준>

ISMS : 정보보호 관리체계(ISMS)의 인증기준은 관리체계 수립 및 운영, 보호대책 요구사항으로 나누어 5개 영역, 16개 분야, 총 80개 항목으로 구성된다. 이는 조직의 정보보호 정책 수립부터 물리적·기술적 보안 대책, 침해사고 대응에 이르기까지 전반적인 정보보호 관리 수준을 검증하는 기준이다

ISMS-P : ISMS의 80개 항목에 더해 개인정보 수집, 이용, 제공, 보유 및 파기 등 개인정보 처리 단계별 보호조치 22개 항목을 추가하여 총 102개 인증기준으로 구성된다. ISMS-P는 기업이나 기관이 정보보호뿐만 아니라 개인정보보호까지 아우르는 종합적인 관리체계를 갖추고 있음을 보여준다.