	★차장	팀장	IT전략실장	경영전략본부장	
협 조		팀장			
		추모시설운영처장			
		기획조정실장			

문서번호	IT전략실-1836
보존기간	30년
결재일자	2023.04.07.
공개여부	부분공개(5,7)

「정보보호 역량 강화를위한」

정보보호관리체계(ISMS) 인증추진 계획

2023.

서울시설공단 IT전략실

「정보보호 역량 강화를위한」

정보보호관리체계(ISMS) 인증추진 계획

정보보호관리체계 인증 추진을 통하여 현재 공단의 정보보안 체계의 법적·기술적·환경적 취약점에 대한 개선 및 보완 조치를 시행하여 정보보호 역량을 강화하고자 함

Ⅰ 추진 근거

▢ 관련근거

○ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조

○ 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(과기정통부)

○ 『2023년도 주요사업계획』 및 『2023년 정보보안업무 추진계획』

Ⅱ 인증추진 개요

▢ 인증목적

○ 정보보호관리체계(ISMS) 인증 추진을 통한 정보보호 수준 제고

< 정보보호관리체계(ISMS[1]) >

- 정의 : 기관의 정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원 또는 인증기관이 증명하는 제도
- 인증의무대상 : 정보통신망서비스제공자(ISP), 직접정보통신시설사업자(IDC), 연간매출액 또는 세입이 1500억원 이상인 상급병원, 재학생수가 1만명 이상인 학교 등

▢ 인증 필요성

○ 조직 전반의 정보보호 및 개인정보보호를 위한 지속적이고 체계적인 위험관리(Risk Management) 중요성 부각

1) ISMS : Information Security Management System

▢ 인증 기대효과

○ **(신뢰성 향상)** 공단의 정보보호 관리 노력에 대한 신뢰성 향상

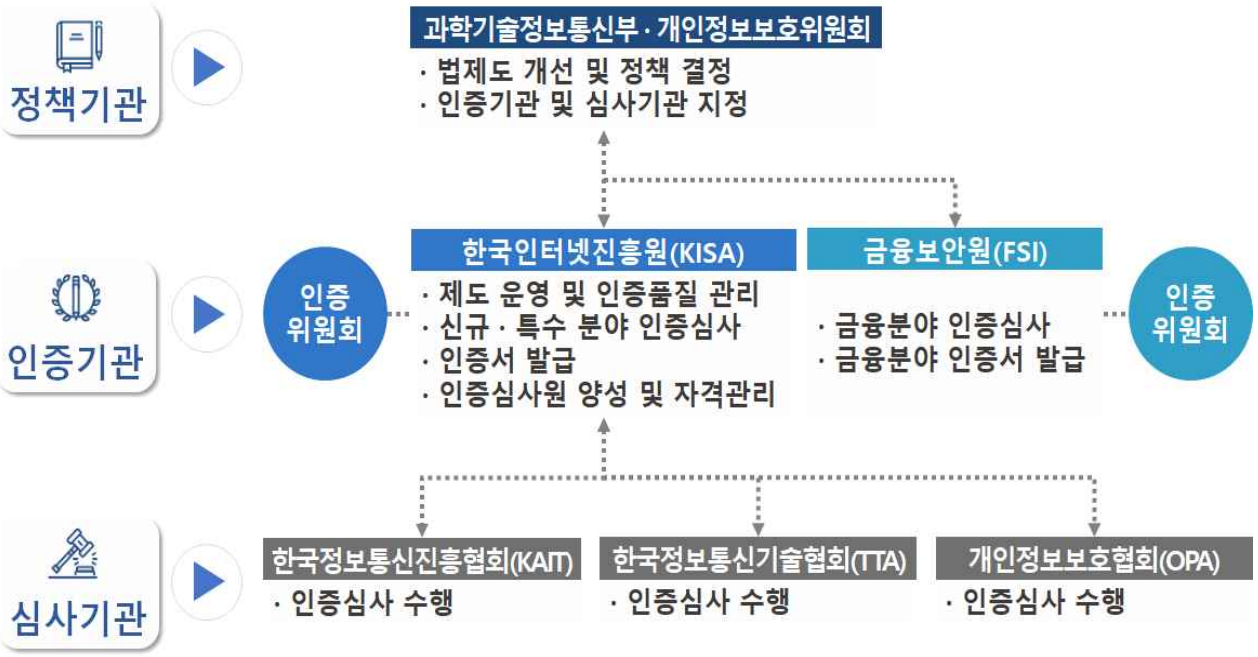
○ **(안정성 제고)** 정보보호 위험관리 및 개인정보보호 역량 강화를 통한 비즈니스 안정성 제고

○ **(법적 준거성 확보)** 윤리 경영을 위한 정보보호와 개인정보보호의 법적 준거성 확보

○ **(사이버 침해사고 위협 대응)** 융합화·고도화되는 사이버 침해 위협에 효과적인 대응 가능

▢ 인증 체계

○ **(추진체계)** 정책기관, 인증기관, 심사기관으로 구성

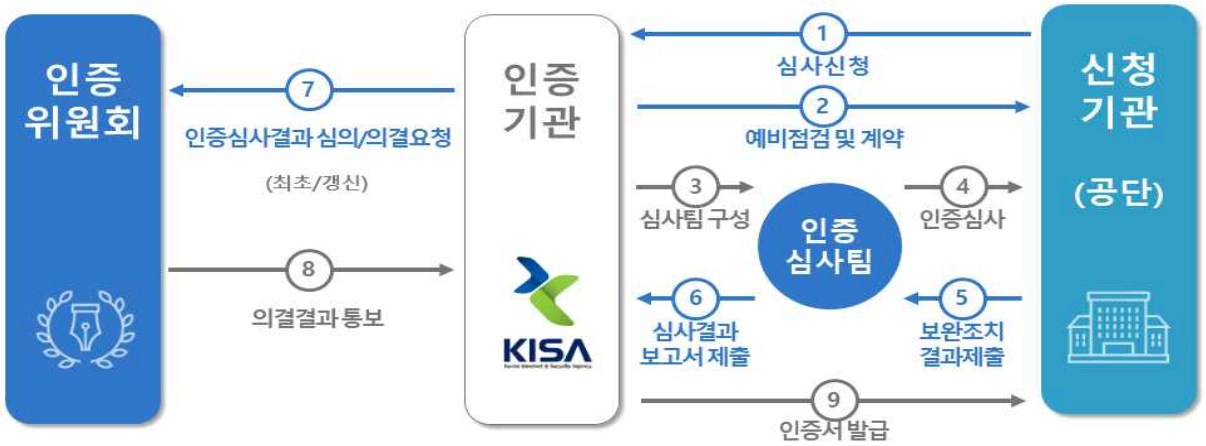


○ **(인증기준)** ① 관리체계 수립 및 운영(16개 항목, 42개 세부점검항목)
② 보호대책 요구사항(64개항목, 192개 세부점검항목)

○ **(인증절차)** 한국인터넷진흥원에 정보보호관리체계(ISMS) 인증신청

인증신청 이후(8주)	인증심사(2주)	보완조치(4~12주)	인증단계(9주)
• 신청서 제출 • 심사일 확정 • 예비점검 • 인증수수료 납부 • 심사단 구성	• 인증심사 (서면/현장심사) • 결함보완 사항 점검 • 심사결과 작성	• 결함보완 사항 보완조치 • 보완조치서 제출 • 결함보완 사항 이행조치 점검	• 인증위원회 개최 • 인증서 발급

※ 인증심사 상황에 따라 인증신청 후 19주(4.75월) ~ 31주(7.75월) 소요



▢ 인증 기준 항목

○ 관리체계 수립 및 운영(4개분야 16개 항목 42개 세부 점검항목)

영 역	분 야	항 목
1. 관리체계 수립 및 운영 (16항목)	1.1 관리체계 기반 마련	1.1.1 경영진의 참여
		1.1.2 최고책임자의 지정
		1.1.3 조직 구성
		1.1.4 범위 설정
		1.1.5 정책 수립
		1.1.6 자원 할당
	1.2 위험관리	1.2.1 정보자산 식별
		1.2.2 현황 및 흐름분석
		1.2.3 위험 평가
		1.2.4 보호대책 선정
	1.3 관리체계 운영	1.3.1 보호대책 구현
		1.3.2 보호대책 공유
		1.3.3 운영현황 관리
	1.4 관리체계 점검 및 개선	1.4.1 법적 요구사항 준수 검토
		1.4.2 관리체계 점검
		1.4.3 관리체계 개선

○ 보호대책 요구사항(12개 분야 64개 항목 192개 세부 점검항목)

영 역	분 야	항 목
2. 보호대책 요구사항 (64항목) (계속)	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 업무환경 보안
	2.5 인증 및 권한관리	2.5.1 사용자 계정 관리
		2.5.2 사용자 식별
		2.5.3 사용자 인증
		2.5.4 비밀번호 관리
		2.5.5 특수 계정 및 권한 관리
		2.5.6 접근권한 검토
	2.6 접근통제	2.6.1 네트워크 접근
		2.6.2 정보시스템 접근
		2.6.3 응용프로그램 접근
		2.6.4 데이터베이스 접근
		2.6.5 무선 네트워크 접근
		2.6.6 원격접근 통제
		2.6.7 인터넷 접속 통제

영 역	분 야	항 목
2. 보호대책 요구사항 (64항목)	2.7 암호화 적용	2.7.1 암호정책 적용
		2.7.2 암호키 관리
	2.8 정보시스템 도입 및 개발 보안	2.8.1 보안 요구사항 정의
		2.8.2 보안 요구사항 검토 및 시험
		2.8.3 시험과 운영 환경 분리
		2.8.4 시험 데이터 보안
		2.8.5 소스 프로그램 관리
		2.8.6 운영환경 이관
	2.9 시스템 및 서비스 운영관리	2.9.1 변경관리
		2.9.2 성능 및 장애관리
		2.9.3 백업 및 복구관리
		2.9.4 로그 및 접속기록 관리
		2.9.5 로그 및 접속기록 점검
		2.9.6 시간 동기화
		2.9.7 정보자산의 재사용 및 폐기
	2.10 시스템 및 서비스 보안관리	2.10.1 보안시스템 운영
		2.10.2 클라우드 보안
		2.10.3 공개서버 보안
		2.10.4 전자거래 및 핀테크 보안
		2.10.5 정보전송 보안
		2.10.6 업무용 단말기기 보안
		2.10.7 보조저장매체 관리
		2.10.8 패치관리
		2.10.9 악성코드 통제
	2.11 사고 예방 및 대응	2.11.1 사고 예방 및 대응체계 구축
		2.11.2 취약점 점검 및 조치
		2.11.3 이상행위 분석 및 모니터링
		2.11.4 사고 대응 훈련 및 개선
		2.11.5 사고 대응 및 복구
	2.12 재해 복구	2.12.1 재해, 재난 대비 안전조치
		2.12.2 재해 복구 시험 및 개선

▢ 인증 유지

구 분	내 용	심사절차
최초 심사	정보보호 관리체계 인증 취득을 위한 심사 (범위 변경 등 중요한 변경사항 발생시 최초심사)	1.준비단계 ~ 4.인증단계 진행 (인증 유효기간 : 3년)
사후 심사	정보보호 관리체계를 지속적으로 유지하고 있는지에 대한 심사 (연 1회 이상)	2.신청단계 ~ 3.심사단계 진행 (인증 유효일로 부터 매1년)
갱신 심사	유효기간(3년) 만료일 이전에 유효기간 연장을 목적으로 하는 심사	2.신청단계 ~ 4.인증단계 진행 (유효기간 만료일 이전에 신청)

Ⅲ 인증대상 및 범위

▢ 정보보호 관리체계 범위 및 대상 서비스

○

****

****

****

****

○ **********

구 분	업무명(URL)	내 용
**********	**********	**********
**********	**********	**********
	**********	**********

☐ 인증대상 조직 범위

○

****

****

○ 인증대상 부서별 담당 업무

부 서	인원	담 당 업 무	위 치
**********	**	• ********** • ********** • **********	*****
**********	*	• **********	*****
********** ********** **********	**	• **********	**********
계	**		

▢ 정보자산 범위

○ 공단의 서비스를 직접적으로 운영하는데 필요한 정보자산, 정보자산을 보호하기 위한 간접적인 정보자산(정보보호시스템 등) 으로 구분

구 분	대 상	수량
서버	Windows, Linux, Unix	**
네트워크	스위치, 백본	**
정보보호시스템	방화벽, 유해사이트 차단, DB암호화 등	**
데이터베이스	통합정보시스템 운영과 관련된 DBMS	**
PC	해당 부서 내 모든 데스크톱 및 노트북	**
Web/WAS	웹서비스를 위한 상용 어플리케이션	**
응용프로그램	통합정보시스템, 홈페이지	**
소프트웨어	업무용 소프트웨어 라이선스 보유현황	**
문서	정보보호 관련 문서	*****
물리적 자산	UPS, 항온항습기, 소화설비 등	**
저장매체	업무용 USB드라이브 등	**
※ **********		**

※ 인증심사 추진시 현행화에 따른 변동 가능

▢ 물리적 범위

○ **********

시 설	주 소	기 능
****	**********	• **********
	**********	• **********
*********	**********	• **********

Ⅳ 인증심사 사전컨설팅 결과

□ 사업내용

○ **********

○ **********

○ **********

○ **********

□ 컨설팅 진행결과(**********)

○ **********

_ **********

_ **********

구 분	주요 문제점
**********	**********
	**********
**********	**********
	**********
**********	**********
	**********
**********	**********
	**********

○ **********

_ **********

_ **********

보안시스템	PC	데이터베이스	WEB	WAS
***	***	***	***	***
네트워크	Unix 서버	Windows 서버	어플리케이션	계
***	***	***	***	***

○ **********

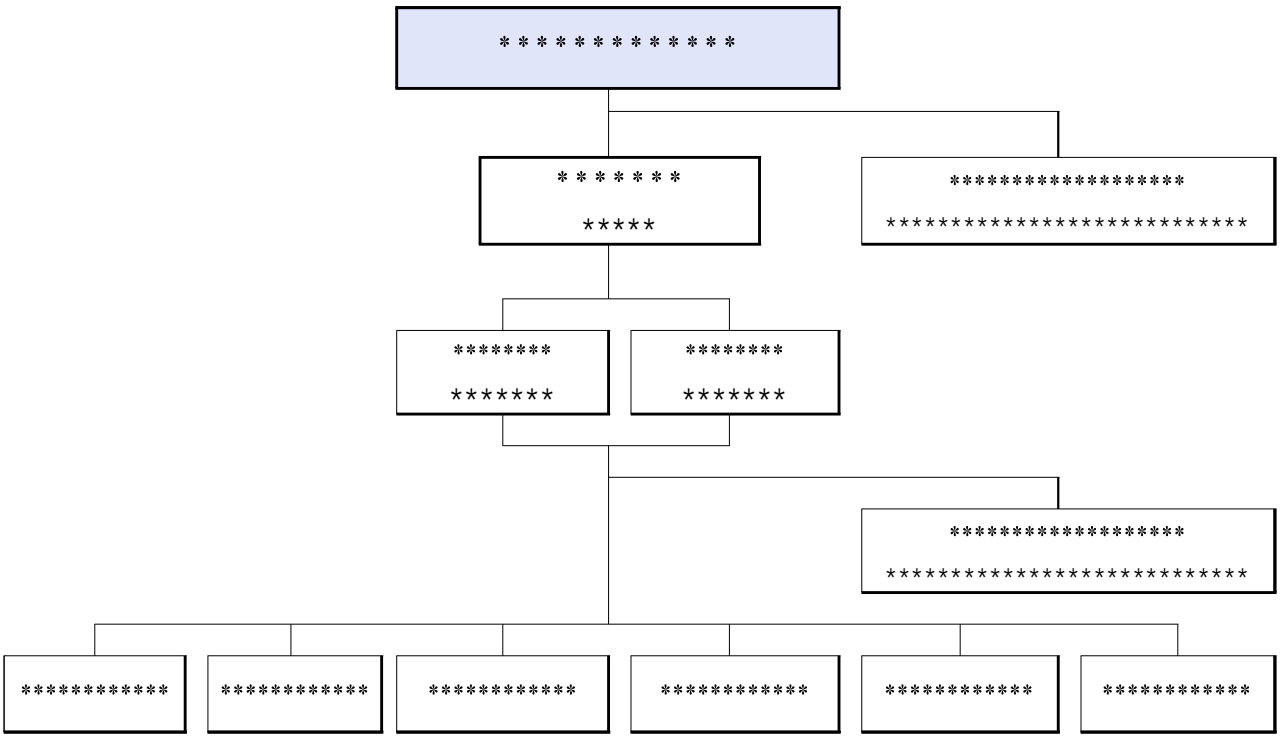
_ **********

_ **********

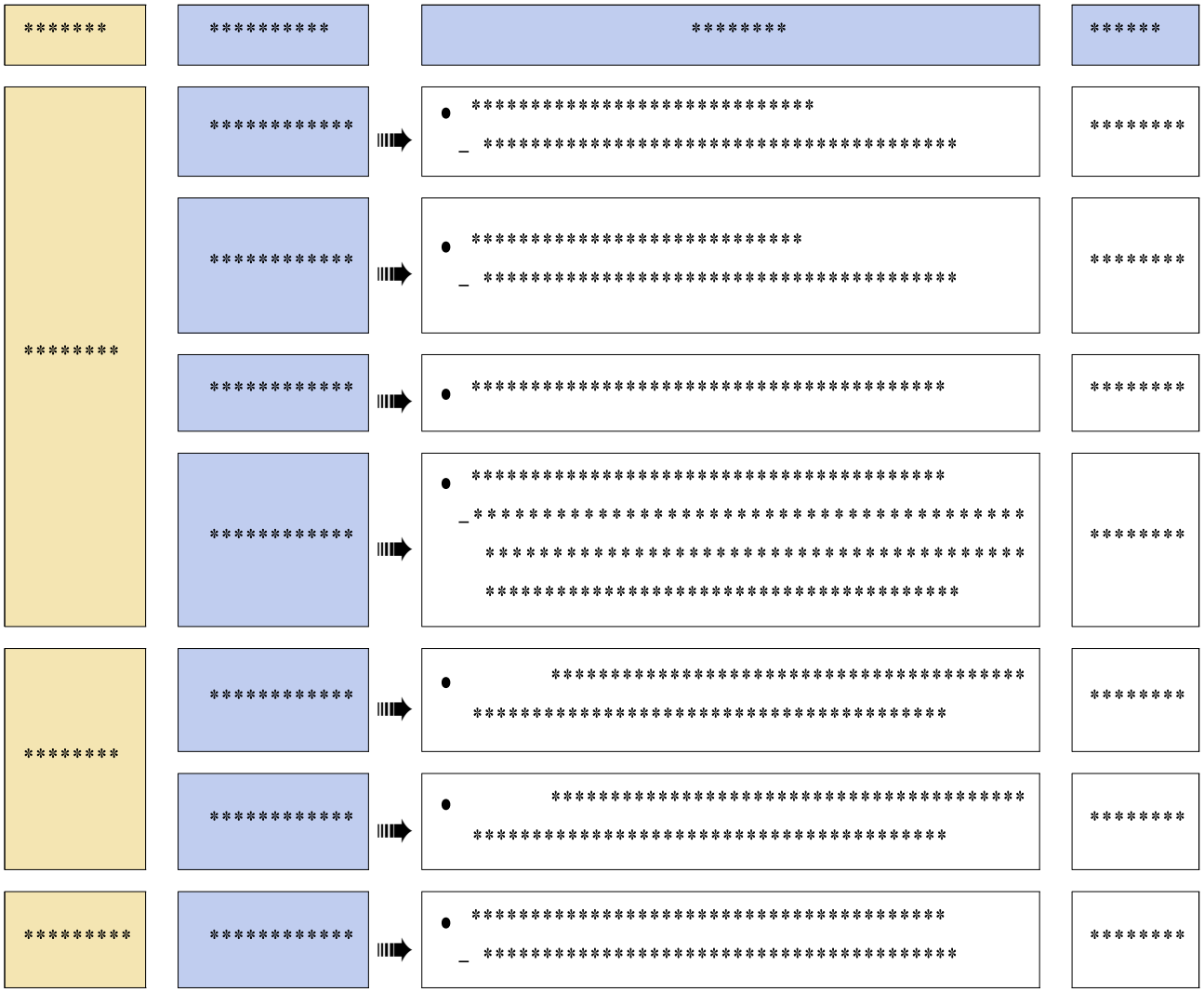
구 분	주요 문제점
**********	**********
**********	**********
**********	**********
**********	**********
**********	**********
**********	**********
**********	**********
**********	**********
**********	**********
**********	**********
**********	**********

V ISMS 인증 추진

□ **********



▢ **********



▢ 편성예산 및 인증수수료

○ **********

_ **********

_ **********

_ **********

※ **********

○ **********

→ **********

※ **********

Ⅵ 향후 일정

○ **********

※ **********

○ **********

붙임 1. **********

2. **********

3. **********

4. **********