ISMS/ISMS-P

20240717 SSL 세미나 강혜인

목차

보안 컨설팅

조직/고객의 사업목적 당성을 위해 정보보호 전문 컨설턴트로 구성된 전문가 집단이 조직의 ICT 자산/조직/프로세스/체계에서 발생할 수 있는 보안 위협과 위험을 사전에 분석해 대응 계획과 대책을 수립하고 최적의 정보보호 체계/시스템을 구축할 수 있도록 지원하는 서비스

보안 컨설팅

정보보호 컨설팅의 법률적 근거

제9조(취약점의 분석 · 평가) ①관리기관의 장은 대통령령으로 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석 · 평가하여야 한다. <개정 2020. 6. 9.>

- " 정보통신기반 보호법 제 9조 " 에 따라 주요 정보통신기반시설 관리 기관은 매년 취약점 분석 평가를 실시
- KISA의 “주요 정보통신 기반시설 기술적 취약점 분석/평가 기준“
- ISMS-P
- ISO27001
- 클라우드 보안 인증(CSAP)

주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드

분류	점검항목	항목 중요도	항목코드
3. 서비스 관리	finger 서비스 비활성화	상	U-19
	Anonymous FTP 비활성화	상	U-20
	r 계열 서비스 비활성화	상	U-21
	cron 파일 소유자 및 권한설정	상	U-22
	Dos 공격에 취약한 서비스 비활성화	상	U-23
	NFS 서비스 비활성화	상	U-24
	NFS 접근 통제	상	U-25
	automountd 제거	상	U-26
	RPC 서비스 확인	상	U-27
	NIS, NIS+ 점검	상	U-28
	tftp, talk 서비스 비활성화	상	U-29
	Sendmail 버전 점검	상	U-30
	스팸 메일 릴레이 제한	상	U-31
	일반사용자의 Sendmail 실행 방지	상	U-32
	DNS 보안 버전 패치	상	U-33
	DNS Zone Transfer 설정	상	U-34
	웹서비스 디렉토리 리스팅 제거	상	U-35
	웹서비스 웹 프로세스 권한 제한	상	U-36
	웹서비스 상위 디렉토리 접근 금지	상	U-37
	웹서비스 불필요한 파일 제거	상	U-38
	웹서비스 링크 사용 금지	상	U-39
	웹서비스 파일 업로드 및 다운로드 제한	상	U-40
	웹서비스 영역의 분리	상	U-41
	ssh 원격접속 허용	중	U-60
	ftp 서비스 확인	하	U-61
	ftp 계정 shell 제한	중	U-62
	Ftpusers 파일 소유자 및 권한 설정	하	U-63
	Ftpusers 파일 설정	중	U-64
	at 파일 소유자 및 권한 설정	중	U-65
	SNMP 서비스 구동 점검	중	U-66
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	U-67
	로그온 시 경고 메시지 제공	하	U-68
	NFS 설정파일 접근 제한	중	U-69
	expn, vrfy 명령어 제한	중	U-70
	Apache 웹 서비스 정보 숨김	중	U-71
4. 패치 관리	최신 보안패치 및 벤더 권고사항 적용	상	U-42
5. 로그 관리	로그의 정기적 검토 및 보고	상	U-43
	정책에 따른 시스템 로깅 설정	하	U-72

보안 컨설팅

하는 일

보안 취약점 점검

- 시스템 보안 취약점 점검
- 웹 보안 취약점 점검
- 모바일 앱 보안 취약점 점검
- 시큐어코딩 소스코드 취약점 점검
- 모의침투 테스트

위험 평가 분석

- ICT 자산 분석
- 위협 분석
- 취약성 분석
- 위험 평가

정보보호체계 구현

- 정보보호체계 구현
- 취약점 보호 대책 수립
- 단계별 이행 계획 수립
- 중장기 보안 계획 수립

ISMS

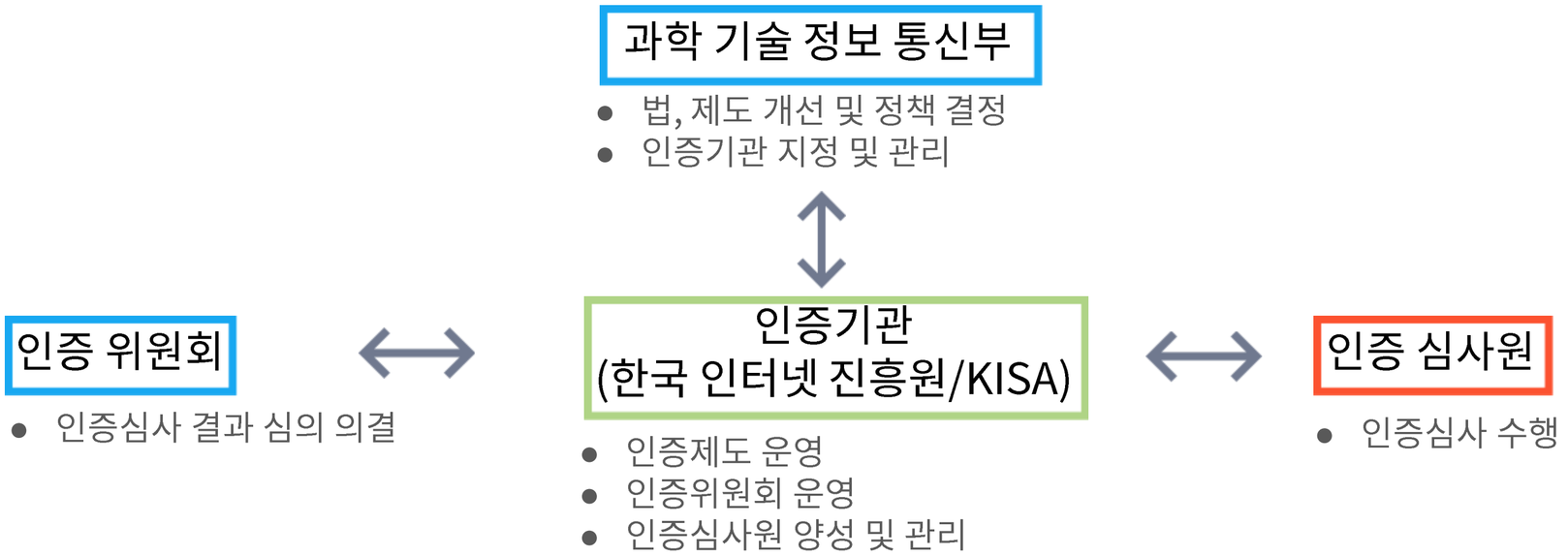
정보보호관리체계(Information Security Management System)

법이 정한 일정 규모 이상의 기업/기관이 충분한 보안요건을 충족하는지 심사하는 제도

ISMS

정보보호관리체계(Information Security Management System)

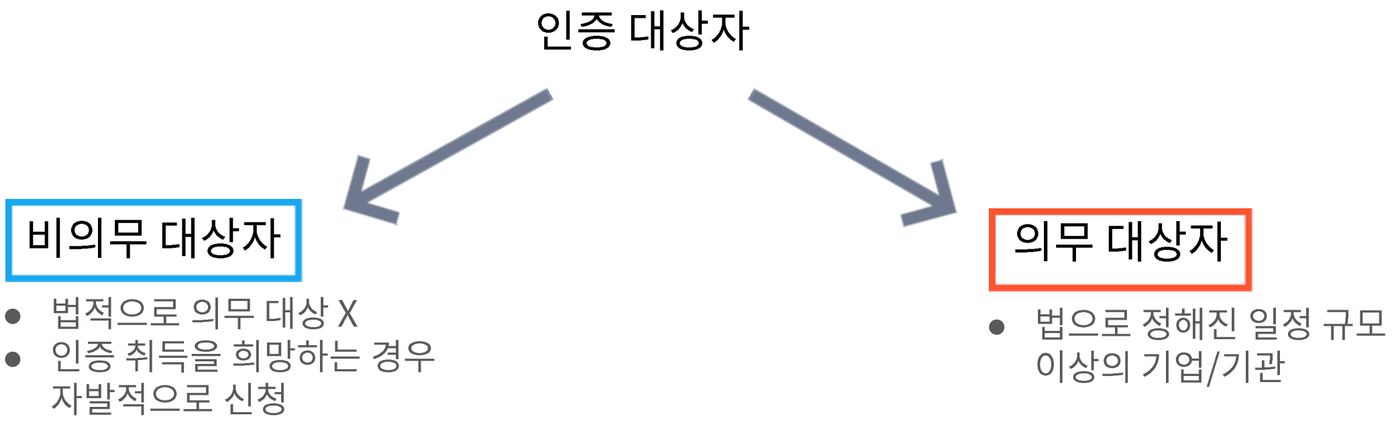
인증 체계



ISMS

정보보호관리체계(Information Security Management System)

인증 대상자



ISMS

정보보호관리체계(Information Security Management System)

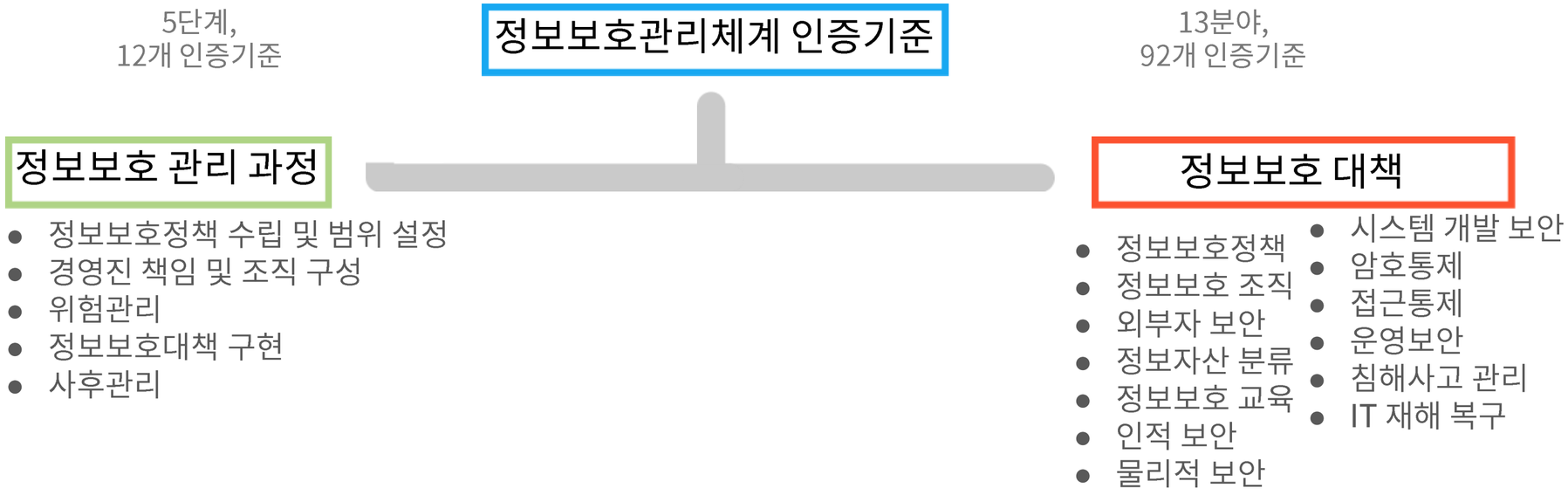
의무 대상자 기준

대상자 기준	세부분류(정보통신서비스제공자)	비고
(**ISP**)전기통신사업법의 전기통신 사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자	인터넷접속서비스, 인터넷전화서비스 등	서울 및 모든 광역시에서 정보통신망 서비스제공(**SKT,SK브로드 밴드,KT,LGU+**등)
(**IDC**)타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자	서버호스팅, 코로케이션 서비스 등	정보통신서비스부문 전년도 매출액 100억 이하인 영세 VIDC 제외
(매출액및이용자기준)연간 매출액 또는 세입 등이 **1,500억원 이상**이거나 정보통신서비스매출액 **100억** 또는 이용자수 **100만명 이상**인 사업자	인터넷쇼핑몰, 포털, 게임, 예약, Cable-SO 등	정보통신 서비스부문 전년도 매출액 **100억이상** 또는 전년도말 기준 직전 3개월간 일일평균 이용자수 **100만명 이상**
	상급종합병원 대학교	직전연도12월31일기준으로 재학생 수가 **1만명 이상**인「고등교 육법」제2조에 따른 학교

ISMS

정보보호관리체계(Information Security Management System)

인증 기준



ISMS

정보보호관리체계(Information Security Management System)

과태료

ISMS 의무 대상자인데도 불구하고, 미인증시 3,000만원 이하의 과태료가 부과

- 정보통신망법 제76조에 근거

제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다.
6의3. 제47조제2항을 위반하여 정보보호 관리체계 인증을 받지 아니한 자

머니투데이
https://news.mt.co.kr › mtview

대형병원 해킹 늘어도…일부는 "그냥 과태료 내" 정보보호 외면

2023. 6. 28. — 이에 일부 **사례**이지만 인증대신 3000만원의 **과태료** 처분을 받는 곳들도 있는 것으로 전해졌다. ... 이를 통해 국내·외 **ISMS-P** 유사 인증제도 및 등급화 **사례** ...

"ISMS 안 받겠다" 보안은 뒷전, 과태료 선택한 곳만 30여개

[디지털데일리 최민지기자] 일부 정보보호관리체계(ISMS) 인증 의무화 대상 기업 및 기관들의 보안윤리 의식 부재에 대한 우려가 제기되고 있다.

ISMS 의무화 대상 42개 대학교 현황 분석... 인증 취득 14곳에 불과

국내 대학들의 잇따른 개인정보 유·노출 사고로 비판이 고조되고 있는 가운데 정보보호관리체계(ISMS) 인증 의무화 대학들의 인증 취득 비율도 아직...

ISMS-P

ISMS + PIMS = 정보보호 관리 체계 + 개인 정보보호 관리 체계

PIMS?
Personal Information Management System

기관 및 기업이 개인정보보호 관리체계를 갖추고 체계적/지속적으로 보호 업무를 수행하는지 객관적으로 심사해 기준 만족 시 인증을 부여하는 제도

개인정보보호 관리체계 구축을 통해 기업이 보유하고 있는 개인정보를 안전하게 관리하고 인증 기업의 대외 신뢰도 향상에 기여

PIMS

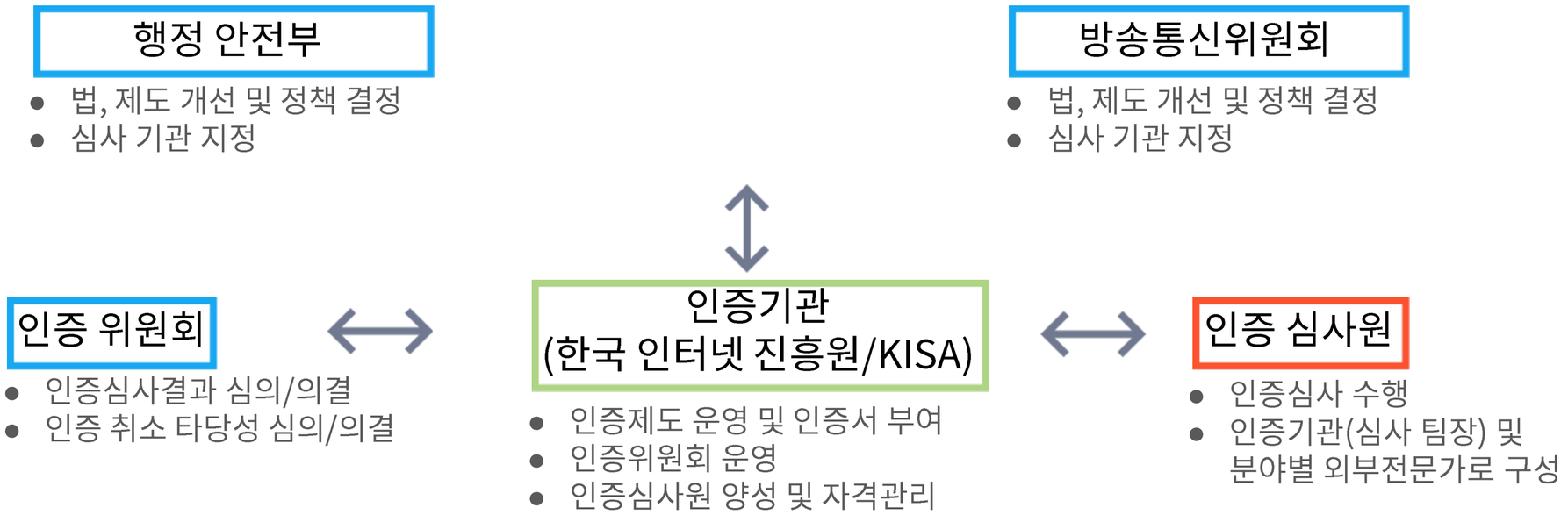
개인 정보보호 관리 체계 Personal Information Management System

PIMS 법적 근거

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조의 3
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제54조의 2
- 개인정보 보호법 제32조의 2
- 개인정보 보호법 시행령 제 34조의 2~제 34조의 8
- 개인정보보호 관리체계 인증 등에 관한 고시

PIMS

개인 정보보호 관리 체계 Personal Information Management System



PIMS

개인 정보보호 관리 체계 Personal Information Management System

인증 대상

개인정보보호 활동을 체계적이고 지속적으로 수행하기 위해 필요한
관리적/기술적/물리적 보호조치를 포함한 종합적 관리체계를 수립 및 운영하고
있는 개인정보 수집/취급 사업자

인증심사 기준

- 국내외의 표준 + '개인정보 보호법' + '정보통신망 이용촉진 및 정보보호 등에 관한 법률' + 국내 환경
- 개인정보 유관 컴플라이언스 대응을 위한 최소 구현 사항, 법적 준거성, 체계적 운영 측면을 보완
- 개인정보보호 관련 조직 및 담당자가 해야 할 실제 활용 부분을 강조

PIMS

개인 정보보호 관리 체계 Personal Information Management System

구성요소

관리과정 요구사항

- 관리체계 수립(정책, 범위, 조직 등)
- 실행 및 운영(개인정보 식별, 위험관리, 구현 등)
- 검토 및 모니터링(사후관리)
- 교정 및 개선(개선활동, 교육)

생명주기 및 권리보장 요구사항

- 생명주기 관리(수집, 이용 및 제공, 보유, 파기)
- 정보주체 권리보장

보호대책 요구사항

- 관리적(인적, 침해사고)
- 기술적(접근권한, 접근통제, 운영보안, 암호화, 개발보안)
- 물리적(영상정보처리기기, 물리적 보안, 매체)

PIMS

개인 정보보호 관리 체계 Personal Information Management System

인증취득 시 혜택

기업에서 개인정보 사고가 발생할 경우, 과징금, 과태료 경감 제공

- 과징금 : 위반 전기통신사업자가 개인정보보호를 위한 것이었다는걸 방송통신위원회가 인정할 경우(절반 경감)
- 과태료 : 위반행위의 동기/내용/결과/유형 및 개인정보보호를 위한 사업자의 노력 등을 고려해 과태료 금액의 절반 범위 내에서 가중 혹은 경감

ISMS-P

ISMS + PIMS = 정보보호 관리 체계 + 개인 정보보호 관리 체계

정보통신망의 안정성 확보 및 개인정보보호를 위해 조직이 수립한 일련의 조치와 활동이 인증기준에 적합함을 인증기관이 평가하여 인증을 부여하는 제도

융합화, 고도화되고 있는 침해 위협을 효과적으로 대응할 수 있도록 기업의 정보보호 및 개인정보보호 수준 제고를 위해 운영

ISMS-P

ISMS + PIMS = 정보보호 관리 체계 + 개인 정보보호 관리 체계

ISMS와 PIMS가 통합되었다고 PIMS에 해당하지 않던 기업이 PIMS 심사를 받지 않아도 됨

ISMS-P

ISMS + PIMS = 정보보호 관리 체계 + 개인 정보보호 관리 체계
인증심사의 종류 및 절차

최초심사 : ISMS-P 인증을 처음으로 취득하고자 할 때 수행하는 심사(통과하면 3년의 유효기간이 부여)
사후심사 : 인증을 취득한 이후 ISMS-P가 지속적으로 유지되고 있는지 확인하는 것이 목적 / 인증 유효기간 동안 매년 1회 이상 실시
인증을 취득한 범위와 관련해 침해사고 혹은 개인정보 유출사고가 발생한 경우 한국인터넷진흥원은 필요에 따라 인증관련 항목의 보안향상을 위해 필요한 지원 등이 가능
갱신심사 : ISMS-P 인증의 유효기간 갱신을 위해 실시하는 인증심사

ISMS-P

ISMS + PIMS = 정보보호 관리 체계 + 개인 정보보호 관리 체계
인증심사의 종류 및 절차

인증 절차 및 소요시간

	① 준비		② 심사					③ 인증		
인증 절차	관리체계 구축 후 운영	인증 신청	심사 준비	인증 심사	보완 조치	조치결과 확인	심사 결과보고서 작성	인증 위원회 심의 준비	인증 위원회 심의	인증서 교부
소요 기간	2개월 이상	심사 8주전	심사 6주전	1~2주	100일 이내		30일 이내	2주~4주	1일	인증위원회 심의·의결 후 2주 이내

ISMS-P

ISMS + PIMS = 정보보호 관리 체계 + 개인 정보보호 관리 체계
인증기준

관리체계 수립 및 운영(16개)

- 관리체계의 메인프레임
- 전반적인 관리체계 운영 라이프사이클 구성

보호대책 요구사항(64개)

- 정책, 조직, 자산 교육등 관리적 부문과 개발, 접근통제, 운영관리, 보안관리 등 물리적/기술적 부문의 보호대책에 관한 사항으로 구성

개인정보 처리 단계별 요구사항(22개)

- 개인정보 생명주기에 따른 보호조치 사항으로 구성

ISMS-P

ISMS + PIMS = 정보보호 관리 체계 + 개인 정보보호 관리 체계

인증범위

정보통신서비스를 기준으로 관련된 정보시스템, 장소, 조직 및 인력을 포함해 해당 서비스에서 처리되는 개인정보의 흐름에 따라 해당 개인정보를 처리하는 정보 시스템, 조직 및 인력, 물리적 장소 등

ISMS 의무 대상자가 ISMS 의무인증 범위를 포함해 ISMS-P 인증을 신청하는 경우, ISMS-P 단일심사로 진행 가능
ISMS 의무인증 범위에 대해서는 ISMS 인증을 신청하고 일부 서비스에 대해서는 개인정보 영역을 포함한 ISMS-P 인증을 신청해 2개의 인증심사를 동시에 진행하는 것도 가능

ISMS와ISMS-P의 차이?

ISMS : 총 80개의 인증기준(보호대책 요구사항 64개 + 관리체계 수립 및 운영(16개)
ISMS-P: : 총 102개의 인증기준(ISMS 인증기준 + 개인정보 처리 단계별 요구사항 22개)

<table>
<tr><th colspan="2">인증</th><th>구분</th><th colspan="2">인증기준 분야별 개수</th></tr>
<tr><td rowspan="11">ISMS-P
(102)</td><td rowspan="9">ISMS(80)</td><td rowspan="3">1. 관리체계 수립 및 운영
(16)</td><td>1.1 관리체계 기반마련 (6)</td><td>1.2 위험관리 (4)</td></tr>
<tr><td>1.3 관리체계 운영 (3)</td><td>1.4 관리체계 점검 및 개선 (3)</td></tr>
<tr><td rowspan="6">2. 보호대책 요구사항
(64)</td><td>2.1 정책, 조직, 자산관리 (3)</td><td>2.2 인적보안 (6)</td></tr>
<tr><td>2.3 외부자 보안 (4)</td><td>2.4 물리보안 (7)</td></tr>
<tr><td>2.5 인증 및 권한 관리 (6)</td><td>2.6 접근 통제 (7)</td></tr>
<tr><td>2.7 암호화 적용 (2)</td><td>2.8 정보시스템 도입 및 개발 보안 (6)</td></tr>
<tr><td>2.9 시스템 및 서비스 운영관리 (7)</td><td>2.10 시스템 및 서비스 보안관리 (9)</td></tr>
<tr><td>2.11 사고 예방 및 대응 (5)</td><td>2.12 재해복구 (2)</td></tr>
<tr><td rowspan="3">-</td><td rowspan="3">3. 개인정보 처리단계별
요구사항
(22)</td><td>3.1 개인정보 수집 시 보호조치 (7)</td><td>3.2 개인정보 보유 및 이용 시 보호조치 (5)</td></tr>
<tr><td>3.3 개인정보제공 시 보호조치 (3)</td><td>3.4 개인정보 파기 시 보호조치(4)</td></tr>
<tr><td colspan="2">3.5 정보주체 권리보호 (3)</td></tr>
</table>

크게 다른점은 없고, 개인정보보호 관리체계가 포함이 되는가 안되는가의 차이

Home > ISMS-P > 인증서 발급현황

인증서 발급현황

종합 정보보호 관리체계를 만들어갑니다

ISMS-P 연도별 인증서 발급현황

업체명 | 검색어(인증번호)를 입력하세요 | 검색

감사합니다.