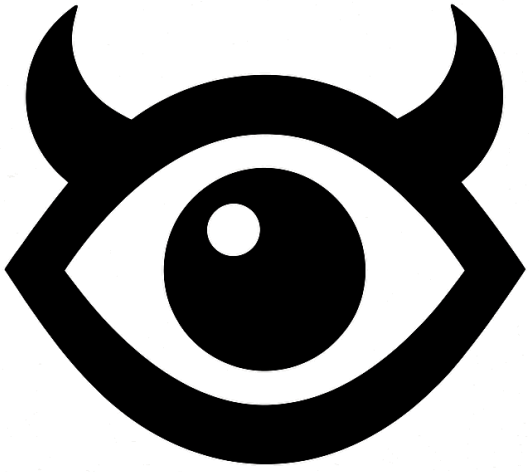
ISMS-P 심사팀장 출신,
업계 최상위 보안전문가

와 함께하는
최고의 보안컨설팅을 합리적인 비용으로 만나 보세요.



monsters

1 ISMS-P 인증 컨설팅

ISMS인증 의무대상자(정보통신망법 제47조 2항)

인증 의무대상자는 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 표에서 기술한 의무대상자 기준에 하나라도 해당되는 경우 반드시 인증을 획득하여야 합니다.

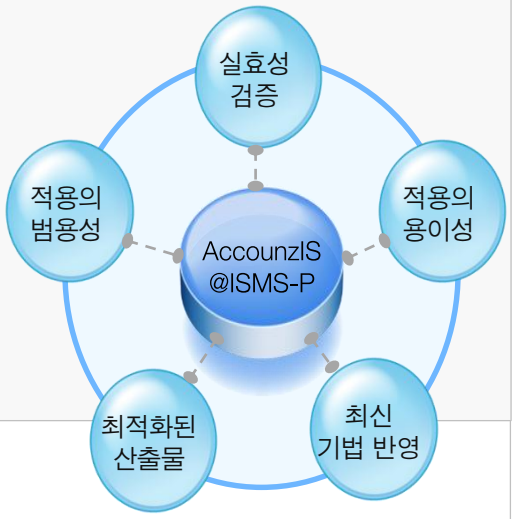
구분	의무대상자 기준
ISP	「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
IDC	정보통신망법 제46조에 따른 집적정보통신시설 사업자
다음의 조건 중 하나라도 해당하는 자	연간 매출액 또는 세입이 1,500억원 이상인 자 중에서 다음에 해당되는 경우 • 「의료법」 제3조의4에 따른 상급종합병원 • 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
	정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
	전년도 직전 3개월간 정보통신서비스 일일평균 이용자 수가 100만명 이상인 자

※ ISMS-P 인증의무대상자가 인증 미획득 시 3000만원 이하의 과태료 부과 및 정보보호 사고 시 과징금 등 가중처벌

AccounzIS@ISMS-P 컨설팅 방법론

Monsters@ISMS-P 방법론은 당사가 수행한 다수의 프로젝트에서 그 실효성을 검증 받았으며, 현황분석 및 취약점 분석, 위험평가, 정보보호 이행계획 수립의 일관성 있는 접근 뿐만 아니라 지속적 정보화 추진체계 구현을 통한 IT거버넌스 대응 및 참여인력의 역량이 극대화할 수 있도록 지원합니다.

단계	현황분석	취약점 점검	위험관리	대책 구현	인증지원
절차	C1000	C2000	C3000	C4000	C5000
	내·외부 환경분석	관리적 취약점 점검	위협 분석	정보보호 대책수립	증적 관리
	범위 선정	물리적 취약점 점검	취약성 분석	정보보호 계획수립	IT 보안감사
	자산식별	기술적 취약점 점검	위험 평가	정책 및 지침 개선	모의심사
	자산중요도 평가			교육	인증심사 지원



2 전자금융기반시설 취약성 분석·평가

전자금융기반시설 취약성 분석·평가 (전자금융거래법 제21조의3)

전자금융업자는 전자금융거래의 안전성과 신뢰성 확보를 위한 전자금융기반시설, 주요정보통신기반시설 등에 대한 종합적 취약점 분석 · 평가를 실시 하여야 합니다.

전자금융 기반시설 취약점 분석·평가 (종합점검)

연간 1회

관련근거

전자금융거래의 안전성과 신뢰성 확보를 위한 전자금융기반시설, 주요정보통신기반시설 등에 대한 종합적 취약점 분석·평가
[전자금융거래법 제21조의3, 정보통신기반보호법 제9조]

공개용 홈페이지 취약점 분석·평가

연간 2회

관련근거

공개용 홈페이지 등에 대한 취약점 분석·평가
[전자금융거래법 제21조의3]

전자금

고객사와의 미팅을 통해, 다음의 점검분야의 점검대상의 자산을 식별하여 취약점 점검의 범위를 도출해 드립니다. 또한 취약점 점검은 다음과 같은 절차에 따라, 취약점 점검부터 대책수립, 이행점검까지 전 과정을 지원합니다.

분야		점검항목	중점점검사항
인프라 영역(필수)	정보보호 관리체계	FISM 288개 항목	전자금융감독규정에서 정한 내용을 기반으로 금융회사에서 정한 정보보호체계 및 관리의 적절성 등을 평가
	서버	SRV 118개 항목	불필요한 서비스 운영 등 운영체제 보안설정 등에 관한 적절성을 평가
	데이터베이스(DBMS)	DBM 27개 항목	DBA 계정권한, DBMS 비밀번호 등에 관한 보안 설정의 적절성 등을 평가
	네트워크 인프라	INF 19개 항목	망분리, 접근통제 등 네트워크 구성 및 가용성 확보 여부 등을 평가
	네트워크 장비	NET 43개 항목	네트워크 장비 보안설정 등에 관한 적절성을 평가
	정보보호시스템 장비	ISS 42개 항목	보안정책 및 정보보호시스템의 보안설정 등에 관한 적절성을 평가
서비스 영역(필수)	웹 애플리케이션	WEB 48개 항목	인터넷뱅킹 등 웹 기반 전자금융거래 서비스에 대한 침해가능 여부 등을 평가
	모바일 애플리케이션	MOB 56개 항목	모바일뱅킹 등 모바일 기반 전자금융거래 서비스에 대한 침해가능 여부 등을 평가
	HTS 애플리케이션	HTS 16개 항목	증권회사에서 제공하는 HTS 애플리케이션에 대한 침해가능 여부 등을 판단
모의해킹 (선택)			시나리오 기반 침입경로 및 해킹 가능성 확인

3 인프라 취약점 점검

인프라 취약점 점검 서비스 개요

IT인프라 유형에 따라 다음과 같은 취약점 점검항목과 점검방법을 정하여 고객의 IT환경 및 법적 준거성을 고려한 취약점 점검을 수행합니다. 특히 기술적인 점검항목 중 법적 의무조치가 요구되는 개인정보처리시스템의 식별과 법적 취약점 항목을 식별하여 법률 상 의무조치가 시급한 정보자산과 취약점 요소를 식별합니다.

현황분석		취약점 점검		점검결과 분석		보고서 작성	
정보자산 식별/분석	추가 점검 대상 파악	자동 점검	수동 점검	취약점 분류	원인 분석	보고서 작성	개선방안 도출

- 정보 자산 식별/분석
  - 점검 대상 시스템 자산분석
  - 정보자산 운용현황 및 현재의 보안 수준에 대한 인터뷰
- 추가 점검 대상 파악
  - 기존의 취약점 점검 내역을 확인하여 추가 점검이 필요한 대상 파악

- 자동 점검
  - 자동화된 점검 체크 리스트를 활용하여 취약점 점검을 수행함
- 수동 점검
  - 주요 서비스를 제공하는 장비의 경우, 권한을 가진 담당자가 체크리스트에 따라 수행하고, 수행결과를 분석·평가하여 점검

- 취약점 분류
  - 도출된 취약점을 위험도와 영향도를 고려하여 우선 순위를 선정
- 취약점 원인 분석
  - 점검 결과 도출된 취약점을 분석하여 해당 취약점의 발생 원인을 파악

- 보고서 작성
  - 취약점 점검 수행 절차와 도출된 취약점 및 분석 결과에 대한 모든 내용을 작성
- 개선방안 도출
  - 도출된 취약점에 대해 긴급/ 단기/ 중장기 보호대책을 구분하여 명령어 레벨의 상세한 보호대책을 제시

■ **인프라 취약점 점검 항목 (예시 – 정보통신서비스제공자, 전자금융업자, 공공기관 등 점검항목과 방법 상이)**

구분	서버					네트워크	보안 장비	어플리케이션	PC
	OS (UNIX)	OS (Windows)	WEB	WAS	DBMS				
점검항목	82	76	10	10	26	13	13	32	19
점검방법	수동 (스크립트)	수동 (스크립트)	수동 (스크립트)	수동 (스크립트)	수동 (스크립트)	수동	수동	수동	수동 (스크립트)

기대효과

인프라 취약점 진단을 통해 고객이 운용하고 있는 주요 정보시스템(서버, 네트워크, DBMS, 정보보호시스템 등)에 대한 기술적 취약점 진단을 수행하고 도출된 위협에 대한 보호대책을 제시함으로써, 그로 인한 침해사고 발생위험을 낮추고 보안수준을 제고 합니다.

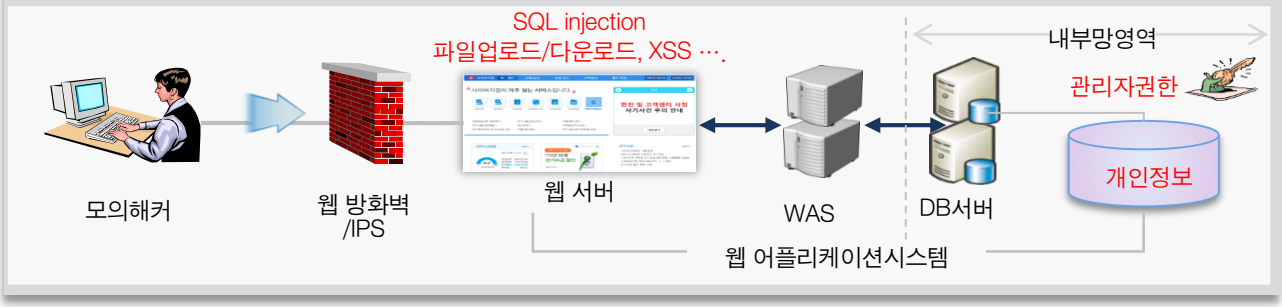
1. 정보보호, 개인정보보호, 산업보안, 정보통신기반보호 등의 법적 준거성 확보
2. IT인프라, 웹 어플리케이션 특성에 따른 취약점 점검 및 문제점 조기 발견
3. 도출된 취약점에 따른 보안가이드 및 개선대책을 통해 위험관리 기반 마련
4. 실 업무 적용이 가능한 정보보호 교육 및 기술이전을 통한 정보보호 기술기반 확보

4 모의해킹

모의해킹 서비스 개요

해커입장(외부자)에서의 모의해킹과 내부자 입장에서의 취약점 분석으로 외부에서 내부 네트워크를 점검하는 서비스로 이용자 포털 모의해킹을 통한 개인정보 유출의 가능성 사전 탐지 및 예방합니다.

사전협의	정보수집 분석	취약성 분석	침투	보고서 작성
• 침투 대상 파악 • 침투 정도 협의 • 침투 시간 결정 • 보고서 일정 협의	• 네트워크 구성 • 서버 자산 파악 • 보안 장비 파악 • 운영 Application	• 취약점 점검 • 네트워크 취약성 • 서버취약성 • Application 취약성	• 취약점공격 • 공격전이/확산 • 공격결과확보 • 공격결과복구	• 취약점원인 • 공격과정 • 공격결과 • 대응책수립



■ 웹 어플리케이션 취약점 점검 항목

주요정보통신기반시설 기준

- 1. 버퍼 오버플로우
- 2. 포맷스트링
- 3. LDAP 인젝션
- 4. 운영체제 명령 실행
- 5. SQL 인젝션
- 6. SSI 인젝션
- 7. XPath 인젝션
- 8. 디렉터리 인덱싱
- 9. 정보 누출
- 10. 악성 콘텐츠
- 11. 크로스사이트 스크립팅
- 12. 약한 문자열 강도
- 13. 불충분한 인증
- 14. 취약한 패스워드 복구
- 15. 크로스사이트 리퀘스트 변조(CSRF)
- 16. 세션 예측
- 17. 불충분한 인가
- 18. 불충분한 세션 만료
- 19. 세션 고정
- 20. 자동화 공격
- 21. 프로세스 검증 누락
- 22. 파일 업로드
- 23. 파일 다운로드
- 24. 관리자 페이지 노출
- 25. 경로 추적
- 26. 위치 공개
- 27. 데이터 평문 전송
- 28. 쿠키 변조

기대효과

모의해킹을 통해 발생 가능한 취약점 사전 파악하여 발생 가능한 실질적인 위험을 감소시키고 서비스의 안전성 및 신뢰성을 제고 합니다.

1. 홈페이지 모의해킹을 통한 개인정보 유출 가능성 사전 탐지 및 예방
2. OWASP10을 포함하는 어플리케이션 보안 취약점 해소를 통한 시스템 안전성 확보
3. 개인정보 유출 등의 해킹 사고 발생시 법적 책임 완화
4. 고객에게 안정적 서비스를 제공하여 기업 이미지 향상

5 ISO/IEC 27001, ISO/IEC 27701 컨설팅

ISO/IEC 27001, ISO/IEC 27701

ISO/IEC 27001과 ISO/IEC 27701은 기업의 정보자산과 개인정보를 국제 기준에 따라 체계적으로 보호하기 위한 가장 신뢰받는 글로벌 표준입니다.

구분	ISO 27001	ISO 27701
목적	정보보안	개인정보 보호
대상	모든 정보자산	개인정보(PII)
관계	기본 표준	27001 확장
법 연계	정보보호 전반	GDPR, 개인정보법
단독 인증	가능	✕ 불가

ISO/IEC27001,27701인증 필요성

- 개인정보보호법, 전자금융거래법, GDPR 등 국내외 법적 요구사항과 연계
- 금융, 의료, 공공기관, IT 서비스 등에서는 필수적 또는 강력히 요구되는 인증
- 고객 및 파트너에게 정보보호 관리체계가 국제 기준에 맞게 운영되고 있음을 보증
- 글로벌 비즈니스, 특히 해외 거래 시 공신력 있는 보안 인증으로 활용
- 입찰, 제안요청서(RFP), 협력사 선정에서 필수 요건으로 제시되는 경우 많음

ISO/IEC27001,27701 인증 기대효과

- 정보보호 위험관리를 통한 비즈니스 안정성 제고
- 윤리 및 투명경영을 위한 정보보호 법적 준거성 확보
- 침해사고, 집단소송 등에 따른 사회·경제적 피해 최소화
- 인증 취득 시 정보보호 대외 이미지 및 신뢰도 향상
- IT관련 정부과제 입찰 시 인센티브 부여

6 개인정보보호 수준평가

개인정보 관리/보호 수준진단 서비스

(법적근거) 「개인정보 보호법」 제11조의2(개인정보 보호수준 평가)
①보호위원회는 공공기관 중 중앙행정기관 및 그 소속기관, 지방자치단체, 그 밖에 대통령령으로 정하는 기관을 대상으로 매년 개인정보 보호 정책·업무의 수행 및 이 법에 따른 의무의 준수 여부 등을 평가(이하 "개인정보 보호수준 평가"라 한다)하여야 한다.

[보안뉴스 박은주 기자] 개인정보보호위원회(위원장 고학수, 이하 개인정보위)는 개인정보 보호법 개정(제11조의2)에 따라 종전 '공공기관 관리수준 진단(이하 관리수준 진단)'을 대폭 개선했다. 개인정보 보호수준 평가대상을 확대하고, 평가체계를 강화한' 공공기관 개인정보 보호수준 평가제(이하 '보호수준 평가제')'를 2024년 3월 15일부터 시행한다고 밝혔다. [출처 2024-01-18 보안 뉴스]

「관리수준 진단제」와 「보호수준 평가제」 비교

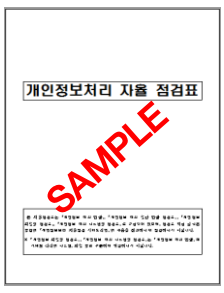
구분	종 전	변 경
명칭	공공기관 관리수준 진단	공공기관 보호수준 평가
법적 근거	· 개인정보 보호법 제11조(자료제출 요구 등) 준용	· **개인정보 보호법 제11조의2**(개인정보 보호수준 평가)
대상	· **800여 개** 공공기관 - 중앙행정기관, 광역 및 기초자치단체, 공공기관(공기업, 지방공사·공단 등)	· **1,600여 개** 공공기관 - 중앙행정기관 및 **소속기관**, 광역 및 기초자치단체, **시·도교육청 및 교육지원청**, 공공기관(공기업, 지방공사·공단 등)
결과 환류	· 미흡기관 현장컨설팅 및 기획점검 시행 (※법적 근거 없음)	**법령에 따라** · **평가 결과 우수기관 및 우수직원 포상** · **개선 권고 및 조치결과 요구** 등 · 미흡기관 현장컨설팅 및 실태점검 시행
제재 조치	· 없음	· 자료 미제출·부실 제출에 대한 **과태료 부과**

개인정보 관리/보호수준 진단 방법론

공공기관의 법적 의무사항 이행 수준 진단 및 컨설팅 서비스 제공

중앙행정기관 및 그 소속기관, 산하 공공기관, 지방자치단체, 지방공기업, 시도교육청 및 교육지원청 등 (특화된 지표 적용)

- 개인정보 보호수준 평가단 구성·운영
- 자체평가(정량지표, 60점), 심층평가(정성지표, 40점) 및 현장검증 실시
- 개인정보 보호수준 평가 설명회, 컨설팅 및 온라인 교육 컨텐츠 제공



monsters

Leader. 강나루
010.4183.2129
nr.kang@cklabs.co.kr