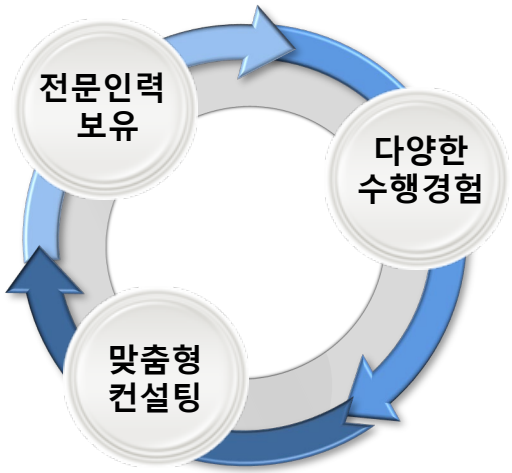
소만사 정보보호/개인정보보호 컨설팅 소개자료

SOMANSA

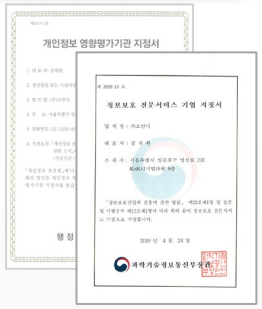
1. 왜 소만사 정보보호 컨설팅인가? (1/2)

So Creative + Man to man + Safety = SOMANSA

- ㈜소만사 정보보호 컨설팅은 정보보호에 특화된 혁신적인 인재를 보유하고 있으며,
- 개인정보보호 수준진단, 종합정보보호관리체계, 취약점 분석평가 등 자사의 솔루션을 활용한 맞춤형 컨설팅을 통해
- 최적의 보호대책을 수립하여 시스템을 안정적으로 운영할 수 있는 방안을 제시합니다.



전문인력 보유



- **정보보호 전문서비스 및 개인정보영향평가 전문기업**
  - ✓ 컨설팅 본부 내 全 전문인력 지식정보보호 전문인력 등재
  - ✓ 개인정보영향평가 전문인력 24명 등재

맞춤형 컨설팅

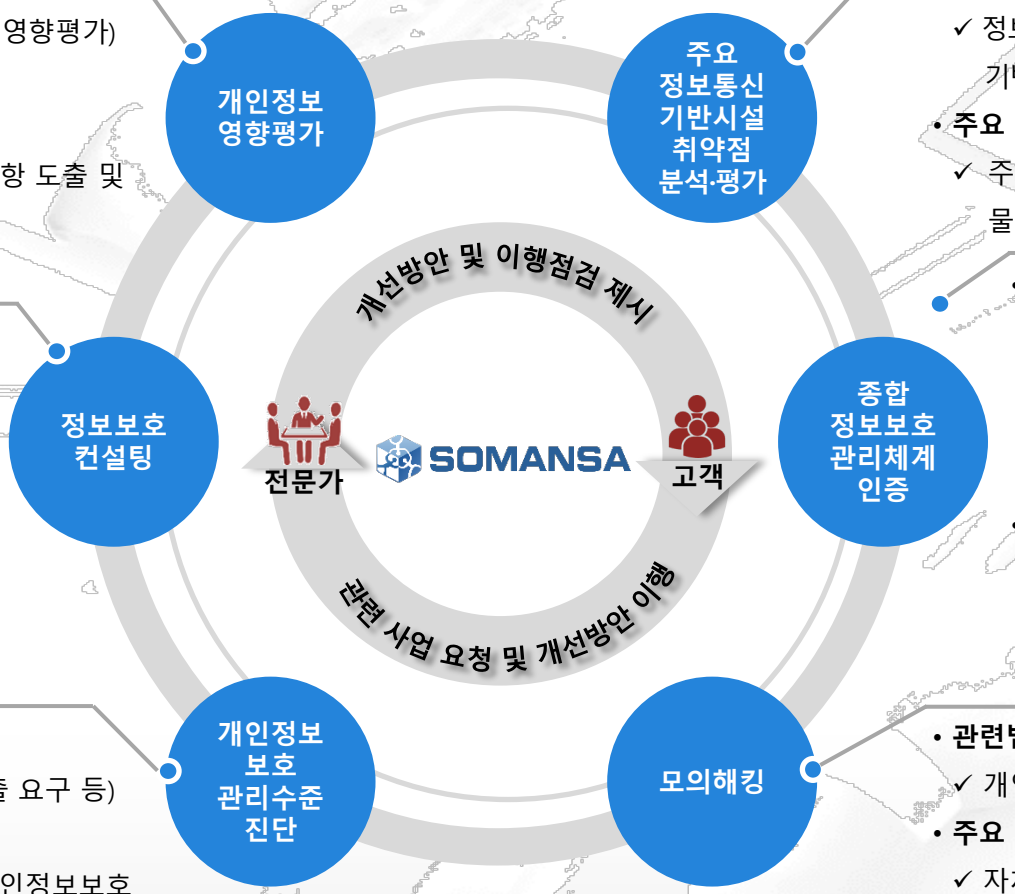
- **기관의 상황에 맞는 맞춤형 컨설팅 수행**
  - ✓ 기관 현황파악을 위해 자사의 정보자산 식별 솔루션 적용 등 정량적 기법 및 정성적 기법 활용
  - ✓ 현황파악 후 기관에 적절한 보호대책 제안

다양한 수행경험

보건복지부
KISA 한국인터넷진흥원
GS엠비즈
한국전력공사
NPS 국민연금

- **800개 기관 개인정보보호 수준진단 수행**
- **ISMS-P / ISMS / PIMS 인증컨설팅**
- **주요정보통신기반시설 취약점 분석평가**

2. 소만사에서 서비스하는 컨설팅 사업은 무엇인가?



- **관련법률**
  - ✓ 개인정보 보호법 제33조(개인정보영향평가) 준수
- **주요 내용**
  - ✓ 개인정보 생명주기에 따른 미흡사항 도출 및 개선방안 제시

- **관련법률**
  - ✓ 정보통신기반 보호법 제5조(주요정보통신기반시설 보호대책의 수립 등)
- **주요 내용**
  - ✓ 주요정보통신기반시설에 대해 관리적·물리적·기술적 취약점 분석평가

- **관련법률**
  - ✓ 보안업무 규정 및 국가정보보안 기본지침(국가정보원)
  - ✓ 전자정부법 제56조 및 전자정부법 시행령 제68조·제69조에 따른 정보보안 관리실태 평가를 대비

- **관련법률**
  - ✓ 정보통신망법 제47조(정보보호 관리체계 인증)
  - ✓ 정보통신망법 제47조의3(개인정보 보호 관리체계 인증)
- **주요 내용**
  - ✓ 정보보호 및 개인정보 관리체계를 102개(80개+22개) 통제 항목에 따라 점검 및 인증하는 제도

- **관련법률**
  - ✓ 개인정보 보호법 제11조 (자료제출 요구 등)
- **주요 내용**
  - ✓ 행정안전부 진단지표 기준으로 개인정보보호 수준 측정

- **관련법률**
  - ✓ 개인정보의 안전성확보조치 제6조(접근통제)
- **주요 내용**
  - ✓ 자체 보유 K.O Script를 통한 자동 점검
  - ✓ 국정원 홈페이지 보안관리 8대 취약점 및 OWASP TOP10 기반 웹·모바일 취약점 점검

3. 개인정보 영향평가

수행근거

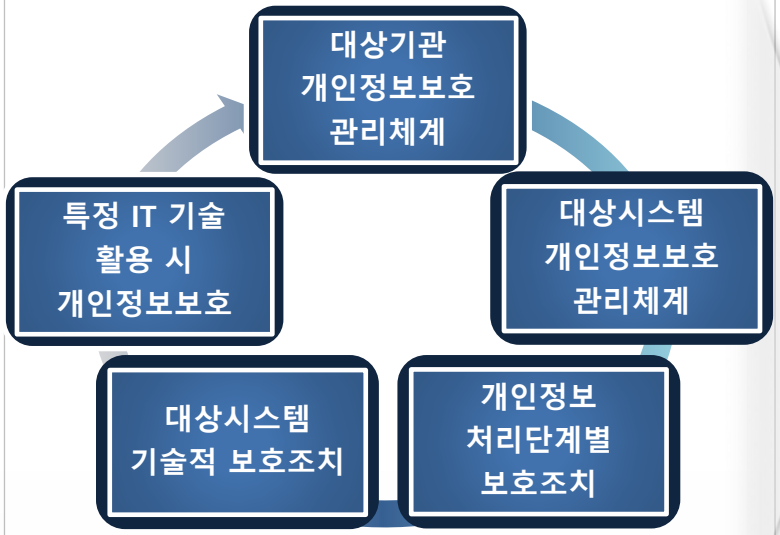
- 「개인정보보호법 제33조」에 의거 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 하고 그 결과를 행정안전부장관에게 제출하여야 한다.

영향평가 필요성 검토

해 당 여 부
주민등록번호 5만건 이상 보유
다른 시스템과 연계된 결과 개인정보 50만건 이상 보유
개인정보 100만건 이상 보유

✓ 하나라도 해당될 경우 개인정보 영향평가 대상

영향평가 수행



✓ 총 5개의 영역 25개 평가분야에 대해 78개의 지표로 개인정보에 미치는 영향을 사전에 분석

영향평가서 작성 및 제출

행정안전부

영향평가서 작성 → 행정안전부 제출

✓ 영향평가서 작성

✓ 영향평가 완료 후 2개월 내 행정안전부 제출

✓ 개선방안에 대한 이행

✓ 영향평가서 제출한 날로부터 1년 이내 이행점검 확인서 제출

4. 종합 정보보호 관리체계 인증 컨설팅(1/2)

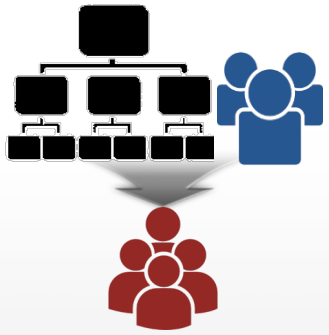
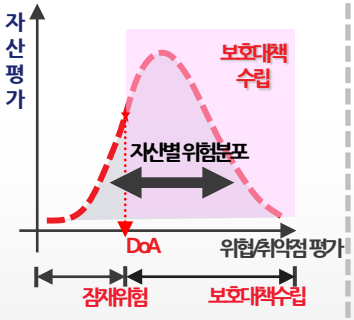
목적

- ✓종합 정보보호 관리체계 인증 획득
- ✓정보보호 수준의 향상
- ✓개인정보보호 수준의 향상
- ✓위험요소에 대한 보호대책 수립

기대 효과

- ✓종합 정보보호 관리체계 인증 획득을 통한 기업 신뢰도 및 안정성 향상
- ✓보안사고 예방 및 (개인)정보보호 관리에 대한 인식 제고

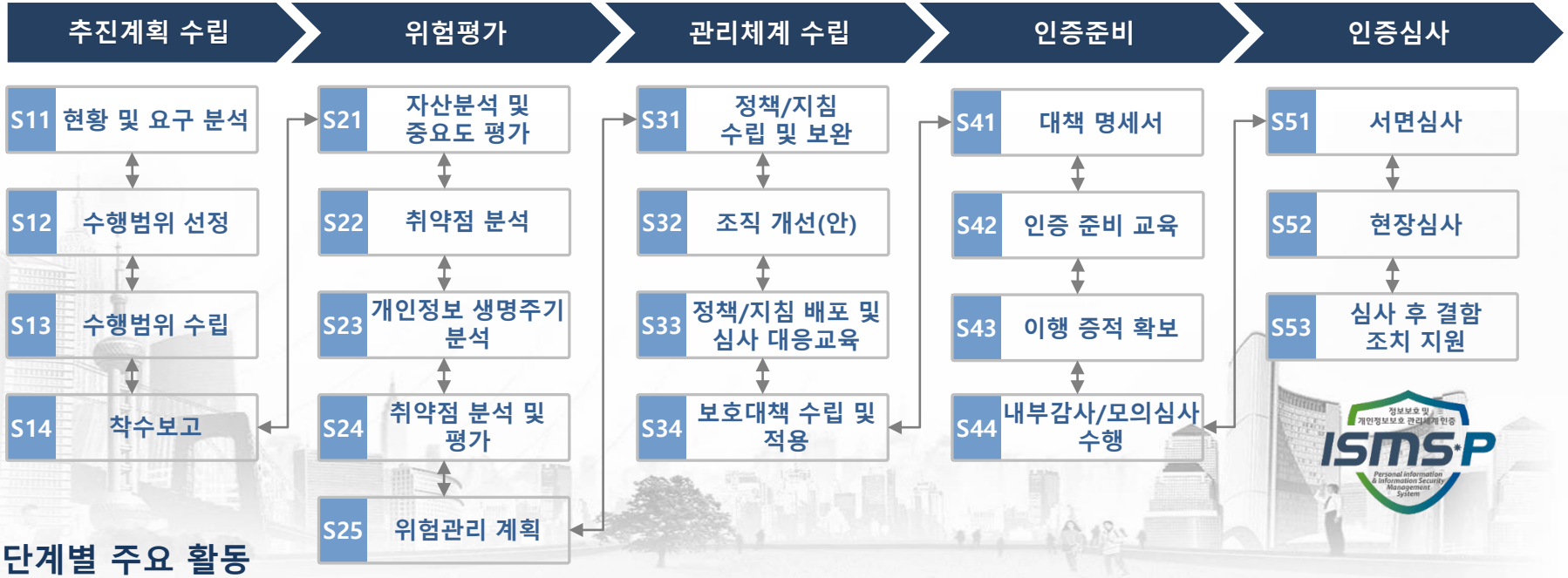
수행 내용

수립 및 범위 설정	(개인)정보보호책임 및 조직구성	위험관리	(개인)정보보호 대책구현	사후관리
				

SOMANSA

4. 종합 정보보호 관리체계 인증 컨설팅(2/2)

종합 정보보호 관리체계 수행 절차



단계별 주요 활동

- 프로젝트요구사항분석
- 수행(인증) 범위를 선정
- 세부 수행과제 정의 및 TFT구성
- 관련 담당자 지정 및 수행방안 공유

- 자산 식별 및 중요도 평가
- 관리적/물리적/ 기술적 취약점 진단
- 개인정보 생명주기 분석
- 위험분석 및 위험관리 계획서 작성

- 관리체계 수립
- 개인정보보호 조직 개선 및 보호대책 수립

- 인증심사 기준에 따라 이행 증적 확보
- 인증범위 내 조직 및 시스템 등에 적용 후 내부감사/모의심사 수행

- 서면심사 자료 대응 지원
- 현장심사 시 대응 지원
- 심사 후 결함보고서 작성 지원

SOMANSA

5. 개인정보 관리수준 진단

수준진단

- 목적 : 개인정보보호법 제11조에 의거 개인정보 보호 정책 추진, 성과평가 등을 위하여 수행
- 수행대상 : 중앙부처 및 산하기관, 광역·기초자치단체 등 총 800개 기관
- 수행내용 : 3개 분야 13개 지표 25개 항목에 대한 진단 및 평가

개인정보보호 관리수준 진단영역

관리적 영역

- 개인정보보호 정책, 지침, 절차 적정성 검토
- 개인정보보호 위·수탁 및 교육이행 진단
- 개인정보보호 수집절차 적정성 검토

분석, 평가

기술적 영역

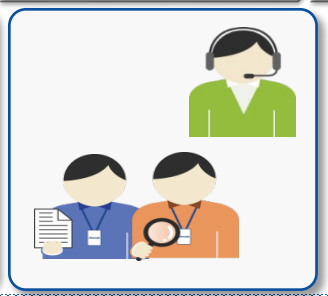
- 접근통제
- PC/서버 內 주민등록번호 점검

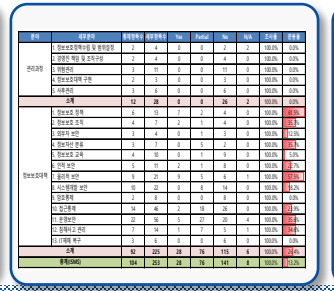
물리적 영역

- 출입통제 /사무환경 보안
- 자산 반·출입 통제

수행절차

자료수집 및 분석 → 현장점검 → 수준진단 결과배포 → 진단지표 개선





- 진단영역에 대한 자료 수집
- 행정안전부 진단대상에 대한 자료 분석

- 자료분석 시 미흡기관 현장점검
- 인터뷰 및 자사 솔루션을 통한 정량적 분석실시

- 진단영역에 대한 평가결과에 대한 기관 배포
- 기관 이의신청 시 내용 수정

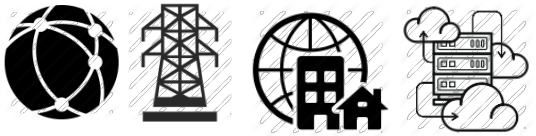
- 개인정보보호법 검토
- 진단지표 개선방안 제시

SOMANSA

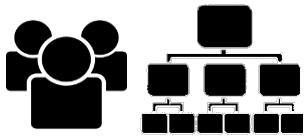
6. 주요정보통신기반시설 취약점 분석·평가 컨설팅

주요 대상

- 「정보통신기반보호법 제8조」에 의거하여 지정된 주요정보통신기반시설
- 철도, 항공, 방송, 에너지, 통신 등 국가적 영향 범위가 큰 시설



자산 식별



- 공통자산 식별
- 정보자산 식별
- 식별된 자산들에 대한 자산가치 평가

취약점 분석

- 취약점 분석 Tool을 이용한 자동화 분석
- 취약점에 따른 위험평가

보호 대책 수립

- 취약점에 따른 개선방안 및 보호대책 수립
- 위험도 산정 후 개선사항 우선순위 선별

보호조치 및 이행점검

- 컨설팅 후 즉시개선 사항 조치
- 조치결과에 대한 이행점검 실시

7. 모의해킹 컨설팅

목적

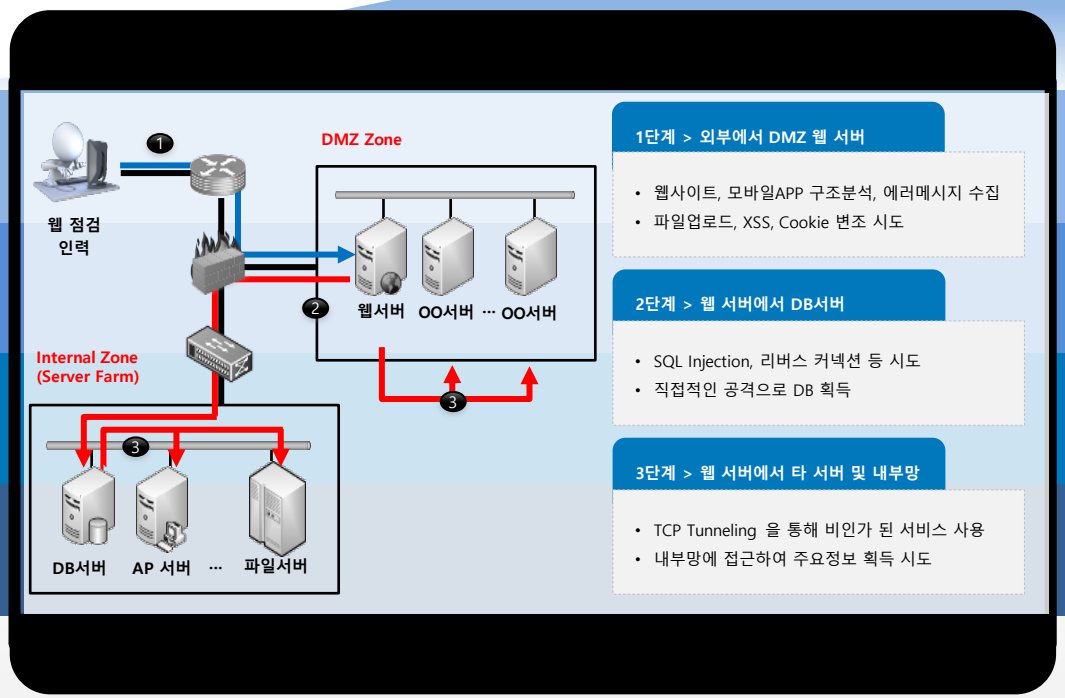
- ✓ 내 · 외부의 악의적인 공격으로부터 서비스 및 정보를 보호하여 안전하고 편리한 웹 서비스를 제공
- ✓ 모바일 환경에서 다양한 형태로 나타날 수 있는 위협으로부터 보호

수행내용

기대효과

- ✓ 웹어플리케이션 · 모바일 서비스 환경에서 다양한 보안 위협을 도출하여 대응방안

100%



1단계 > 외부에서 DMZ 웹 서버

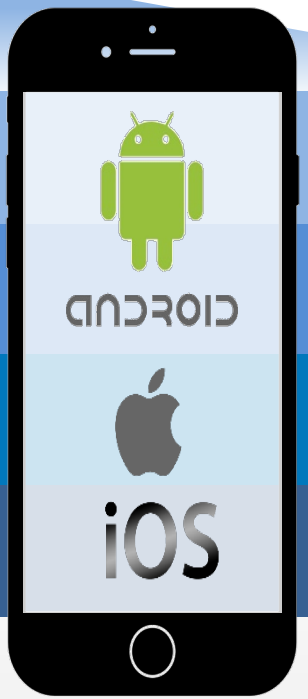
- 웹사이트, 모바일APP 구조분석, 에러메시지 수집
- 파일업로드, XSS, Cookie 변조 시도

2단계 > 웹 서버에서 DB서버

- SQL Injection, 리버스 커넥션 등 시도
- 직접적인 공격으로 DB 획득

3단계 > 웹 서버에서 타 서버 및 내부망

- TCP Tunneling 을 통해 비인가 된 서비스 사용
- 내부망에 접근하여 주요정보 획득 시도



01	진단 대상 선정
02	구조 및 기능 분석
03	자동 · 수동진단
04	진단결과 분석 및 보호대책 수립

SOMANSA