**정보**

- 정보란 ‘어떠한 출처로부터 유래된 지식’. 유의미하고 가치를 가진 것

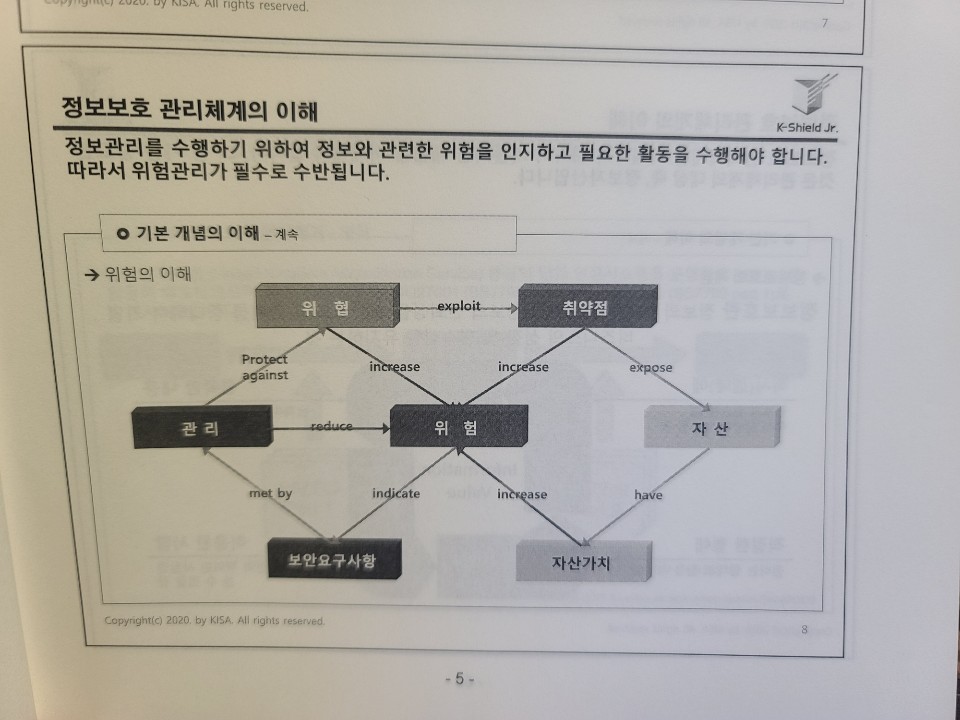
- 정보는 다른 중요 비즈니스 자산과 마찬가지로 조직에 있어 가치가 있고, 지속적으로 적절히 보호되어야 할 필요가 있는 자산이다.

- 정보의 특성 :

가용성(Availability) : 인가된 사용자가 필요 시 정보 및 관련 자산에 접근할 수 있도록 보장하는 것(파괴/지체로부터의 보호) (예) 통신사, 핸드폰)

무결성(Integrity) : 정보 및 처리방법의 정확성과 완전성을 보장하는 것(변조로부터의 보호)예)통장

기밀성(Confidentiality) : 접근이 인가된 자만이 해당 정보에 접근할 수 있다는 것을 보장하는 것(공개로부터의 보호)



**위험에 영향을 줄 수 있는 변수들**

- 자산 : 조직에 가치가 있는 유/무형의 경제적/비경제적 자원보호의 대상

- 위협 : 자산에 원치 않는 결과나 해악을 미칠 수 있는 사건이나 행위

- 취약점 : 위협이 발생하기 위한 사전 조건이나 상황

**정보보호의 개념**

- 정보보호란 정보의 “4R”을 확보하여 정보의 신뢰성을 보장하고 그 가치를 증대하여 기업 비즈니스의 성장 및 연속성을 유지하는 것.

- 적시에(정보가 필요할 때 즉시 활용이 가능할 것. **R**ight Time)

- 적절한 형태(원하는 형태로 활용 가능할 것. **R**ight Form)

- 정확한 내용(정확하고 신뢰할 수 있을 것. **R**ight Information)

- 허용된 사람(권한이 부여된 사람만 볼 수 있을 것. **R**ight People)

**정보보호 관리체계**

- 정의 : 조직에서 비즈니스의 연속성 확보를 위하여 각종 위협으로부터 정보자산을 보호하기 위한 위험관리 기반의 체계적이고 지속적인 프로세스 개선활동이다.

**KISA-ISMS 인증제도**

- 주요 정보자산 유출 및 피해를 사전 예방하고 대처할 목적으로 기업이 수립 및 운영 중인 ISMS가 인증심사 기준에 적합한 지를 인증하는 제도

- 법적 근거 : 정보통신망법 제 47조

- 인증유효기간 : 3년 (매년 1회 사후심사)

- 인증체계 : 과학기술정보통신부, 인증기관(KISA), 인증위원회, 인증심사원

- PDCA 모델을 기반으로 한 SPDCA 프로세스를 제시하고 있다. (Plan(계획) – Do(실행) – Check(평가) – Act(개선))

**정보보호관리체계 Life Cycle**

- 정보보호 정책수립 및 범위 설정 -> 경영진 책임 및 조직 구성 -> 위험관리 -> 정보보호 대책구현 -> 사후관리 // 반복

**정보보호 관리전략 TOP 10**

1. 최고 경영자의 후원과 확약을 받아라

- 필요성 : 정보보호 프로그램은 임원진에 의해 공식적으로 추진되거나 지지를 받는 경우 더욱 성공적이다.

- 전략 : 위험 식별, 문제점의 수치화 (비용, 과태료 등 금전적 문제로 예측 가능하도록). 임원진을 위한 보고주기 확립. 사례 중심으로 이해할 수 있도록

2. 전사적인 지원과 참여를 이끌어라

- 필요성 : 정보보호 프로그램은 사업의 목표를 지원할 수 있어야 한다. 사업 단위의 적극적 참여 시 더욱 성공적이다.

- 전략 : 규칙적, 지속적인 장기활동 계획 개발. 조직 단위로 스스로 정보보호 활동에 참여할 수 있는 필요성을 인식하도록 계도. 이해관계자와의 관계 발전

3. 산업 표준들을 사용, 적용, 연계하라

- 필요성 : KISA ISMS와 같은 정보보호 관리표준을 채택. COBIT, ITIL과 같은 IT 표준 채택. 표준의 채택은 기업 간의 협력을 더욱 효과적이며 효율적으로 이끈다.

- 전략 : 산업 표준을 사용 (TTA, ITU-T, NIST 등 공식 표준 권장). IT 프레임워크 구축

4. 사람들이 쉽게 정당한 일을 하도록 만들어라

- 필요성 : 사람들이 정보보호 프로그램에 참여하고, 기업의 폭 넓은 지지를 얻는 간단하고 효과적인 기술. 정보보호는 업무를 방해하지 않아야 한다.

- 전략 : 정책과 표준은 명확하게 작성. 정보보호 업무 통합. 업무 프로세스가 적용된 정보보호 활동

5. 프로세스를 세련되게 다듬어서 문서화 후 공표하라

- 필요성 : 프로세스가 명백하게 문서화되어 있지 않을 경우, 불확실한 가정을 통한 결정을 내림. 프로세스는 역할과 책임, 활동, 적절한 서비스 수준 협약(SLA)을 정의

- 전략 : 프로세스의 시각적 문서화. 프로세스의 효과 측정

6. 훈련과 교육이 핵심임을 인지하라

- 필요성 : 훈련과 교육은 가장 효과적이고 강력한 기술. 기업은 전사적 정보보호 훈련과 인식제고 프로그램을 개발 / 유지. 운전면허가 없으면 LAMBORGHINI도 무쓸모

- 전략 : 조직의 전 계층을 훈련. 개개의 조직, 업무, 직군 등을 고려한 업무와 연계된 차별화된 훈련 시행

7. 보안이 아니라 위험을 관리하라

- 필요성 : 최대한의 보안의 강요가 아닌 위험관리, 법률과 규제에 대한 순응, 내부감사, 통제 등을 연계한 전사적인 위험관리가 필요함.

- 전략 : 기업의 사업전략의 이해. 위험평가를 수행하고 그 결과를 사업 결정 시 반영하도록 프로세스 수립

8. 사실과 수치들을 관리하라

- 필요성 : 측정지표에 따른 수집, 분석을 통해 기업은 객관화된 근거에 의하여 현명한 경영의사를 결정, 지시할 수 있다. 측정지표는 현 상황을 통해 용이한 의사결정, 상과 향상을 도와주는 도구

- 전략 : 측정지표 프레임워크에 대한 이해. 기업에 의미 있는 측정지표 개발. 측정지표 프로그램을 통해 얻고자 하는 바를 명확히 선정하고 파악

9. 내부 규정 준수를 지원하라

- 필요성 : 타율적인 규제 강조는 반발력만 키움. 기업 정보보호 프로그램을 개발하고 장지적으로 유지해야 함.

- 전략 : 규제 준수의 자율성 강조. 애매한 요구사항은 명확하게 수정하고 법적 요구사항을 중재. 규정 준수에 따른 징계보다는 이득이 있도록 설정

10. 새로운 기업 비즈니스의 창의적 시도를 지원하라

- 필요성 : 정보보호는 기업의 반드시 필요한 부분임을 인식해야 함. 위협을 줄이고, 기존의 비즈니스 내에 정보보호 프로그램이 투명하게 통합

- 전략 : 정보보호 관련 회의에 경영진 참석 유도. 비즈니스 위험의 관점에서 정보보호를 설명.

**정보보호 관리체계 수립 절차**

- 정보보호 정책수립 및 범위설정(정보보호 정책의 수립. 범위 설정)

-> 경영진 책임 및 조직구성(경영진 참여. 정보보호 조직 구성 및 자원 할당)

-> 위험관리(위험관리 방법 및 계획 수립. 위험 식별 및 평가. 정보보호대책 선정 및 이행계획 수립)

-> 정보보호 대책구현(정보보호대책의 효과적 구현. 내부 공유 및 교육)

-> 사후관리(법적 요구사항 준수검토. 정보보호 관리체계 운영현황 관리. 내부 감사)

**사전 단계**

- 수행조직을 구성한다. 통상적으로 TFT 형식으로 구성.

**운영 절차 수립 방법**

- Step#1. 정책 분석 및 요구사항 확인

-> 정보보호 정책 및 지침 등에서 적용될 가능성이 있는 조항 확인

-> 해당 조항에서의 요구조건 및 관련 보안 요구사항 확인

- Step#2. 절차 정리 및 시뮬레이션

-> 결재처리, 공문 등 반드시 수행해야 할 절차 확인

-> 각 절차의 프로세스화 작성

-> 해당 프로세스의 이행 시 발생 가능한 제약사항, 문제점 등 도출

- Step#3. 필요 양식 개발

-> 요구사항 등에서 확인된 반드시 기록해야 할 사항 등의 존재여부 확인

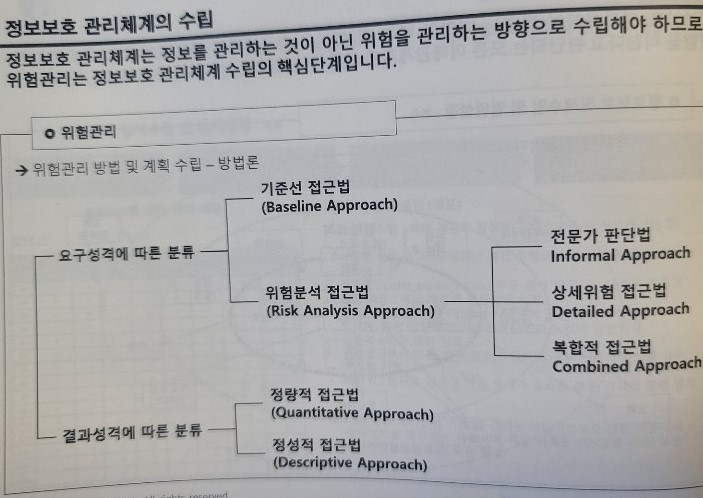
-> 해당 기록사항을 효율적으로 작성 및 관리할 수 있는 양식 개발(필요 시)

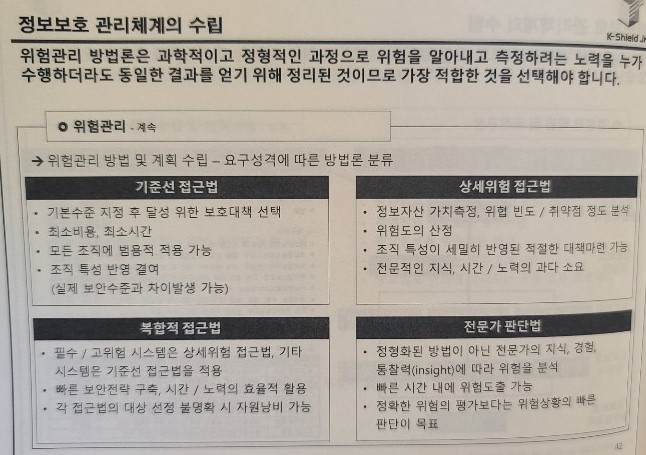
- Step#4. 절차 운영 및 피드백

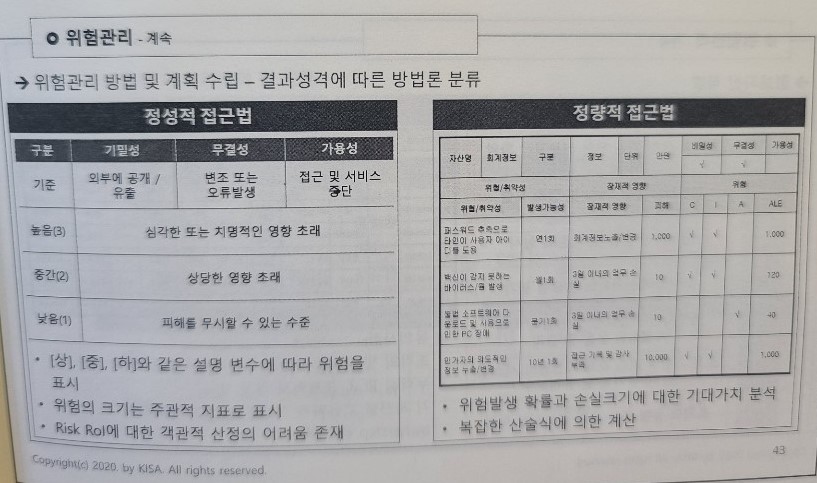
-> 해당 절차 및 양식을 관련 부서에게 전달하고 충분히 설명

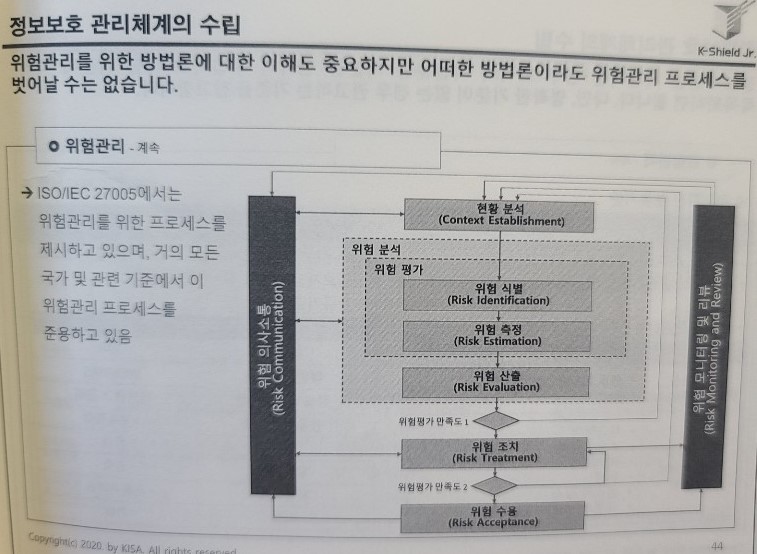
-> 계도기간 등을 적용하여 숙지할 수 있도록 지원

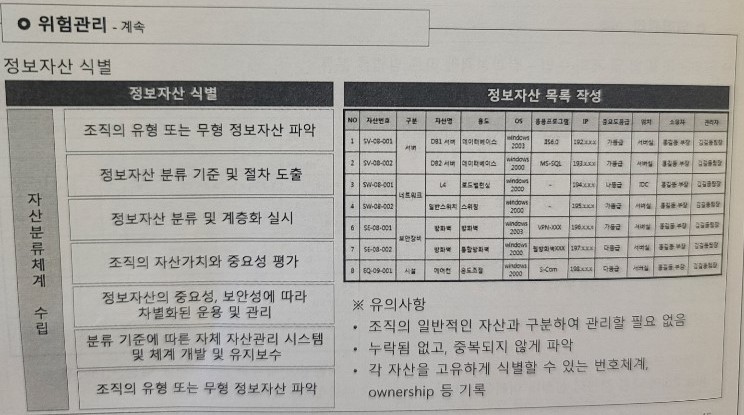
**위험관리**

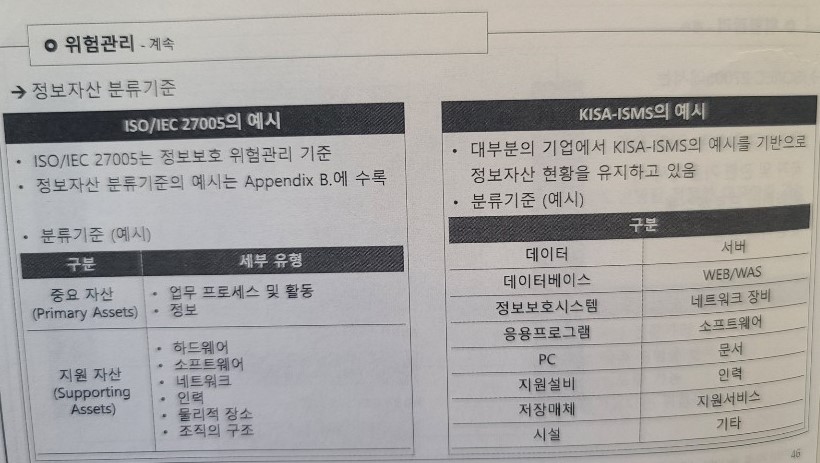


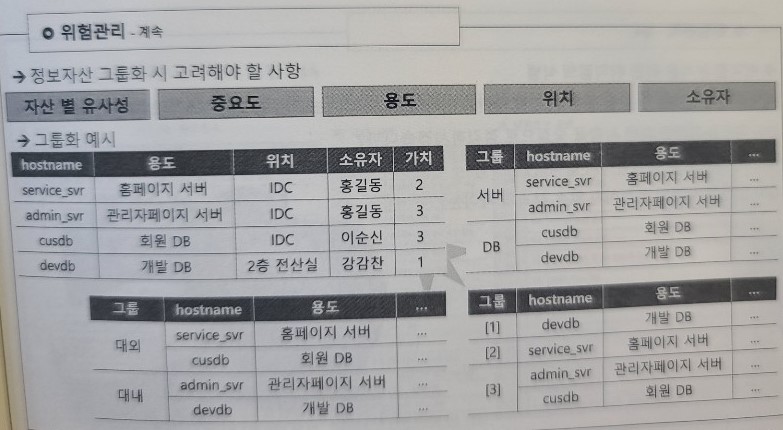


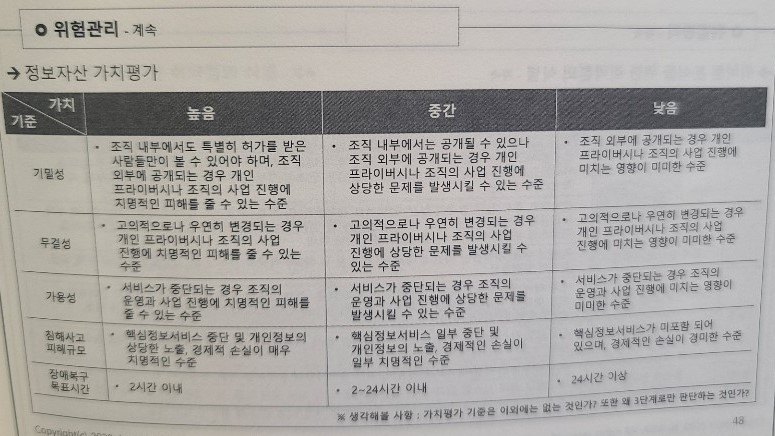












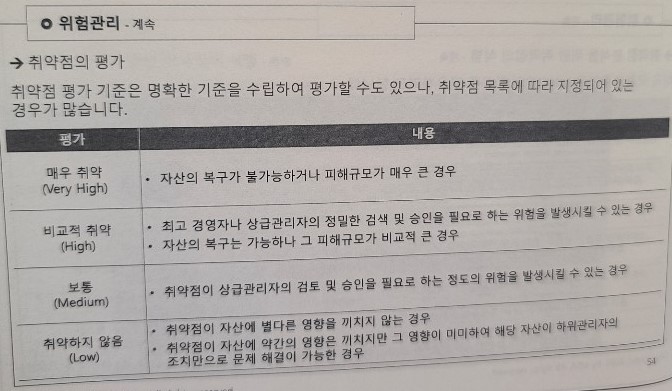
**취약점 분석을 위한 취약점의 식별**

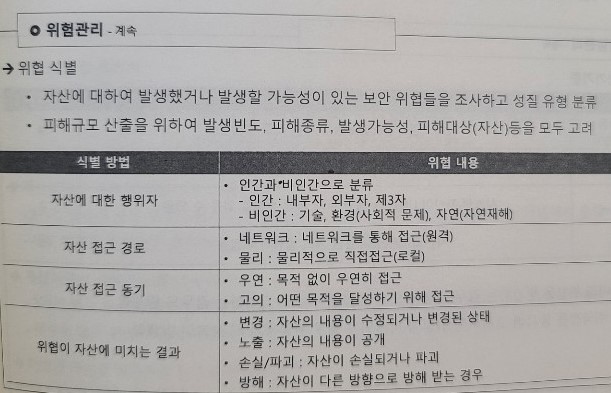
- KISA-KSMS, ISO27001 등의 정보보호 관리체계 인증기준을 근거하여 식별하는 경우가 많음

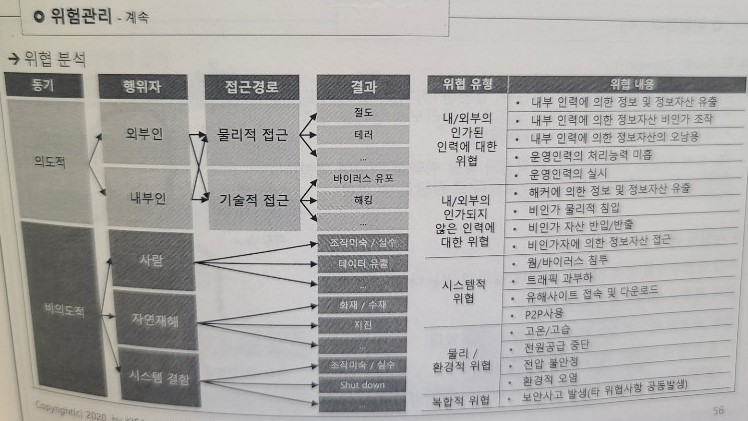
- [주요 정보통신기반시설 취약점 분석, 평가 기준], [전자금융기반시설 취약점 분석 평가 항목]

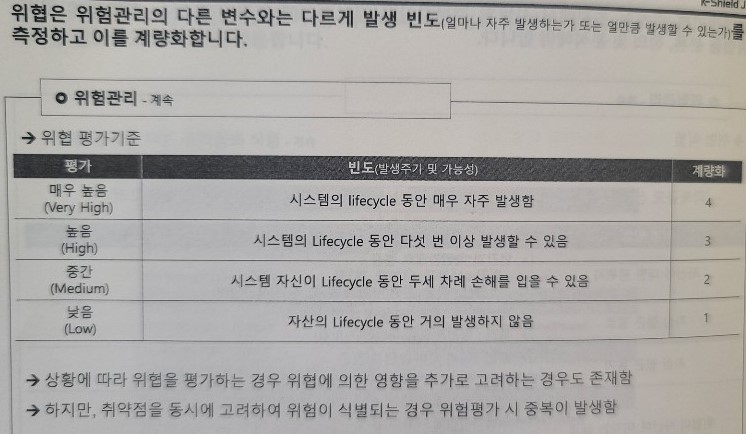
- 미국 국립표준연구소(NIST)의 자료를 활용하기도 한다.

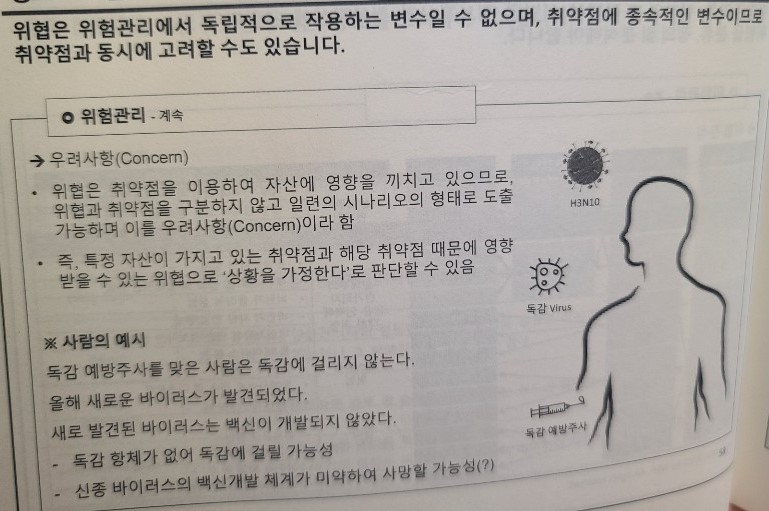
- 웹 취약점인 경우OWASP에서 발표하는 취약점을 활용한다.



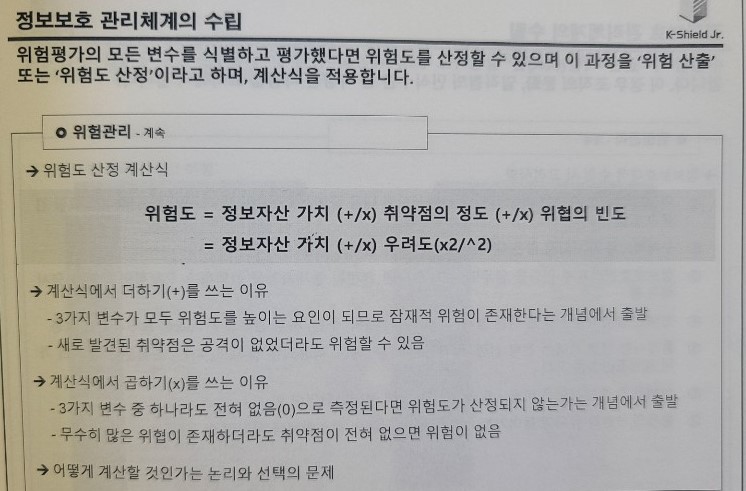


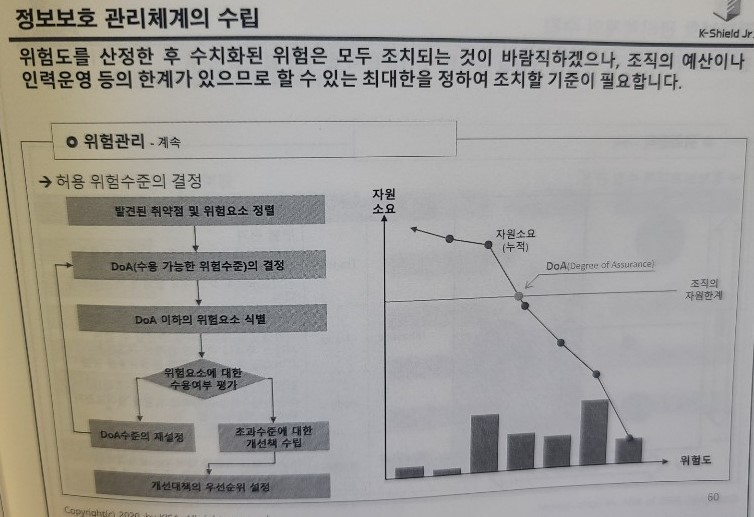


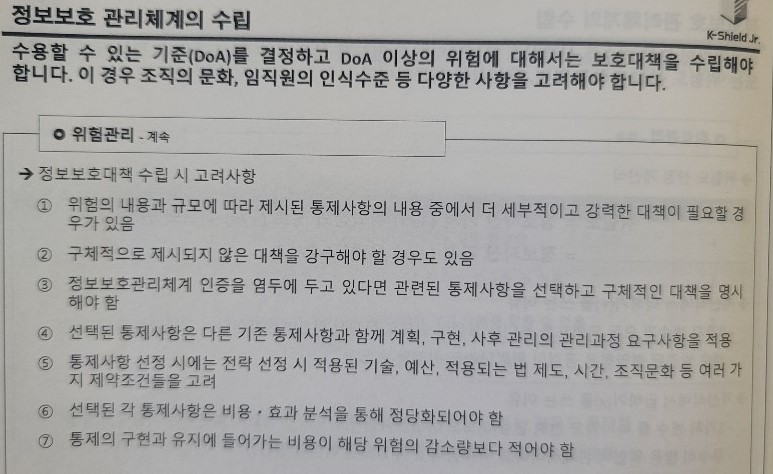


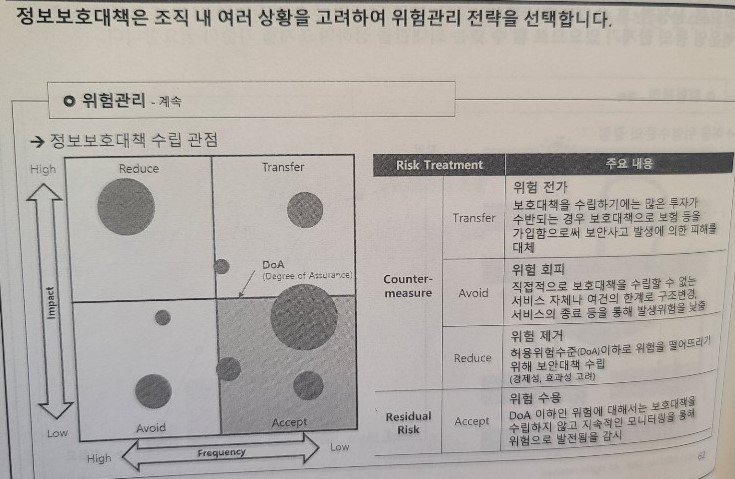


- Concern은 시나리오 형태로 도출.









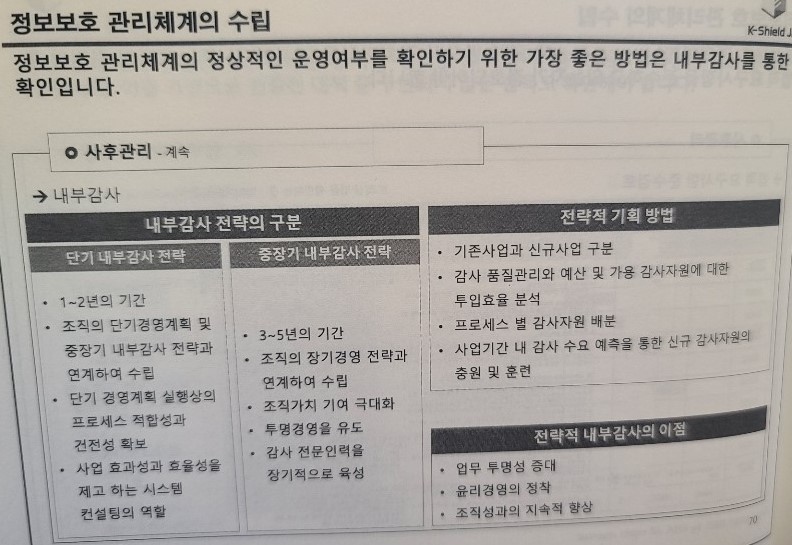
**위험조치 과제 수립 / 이행**

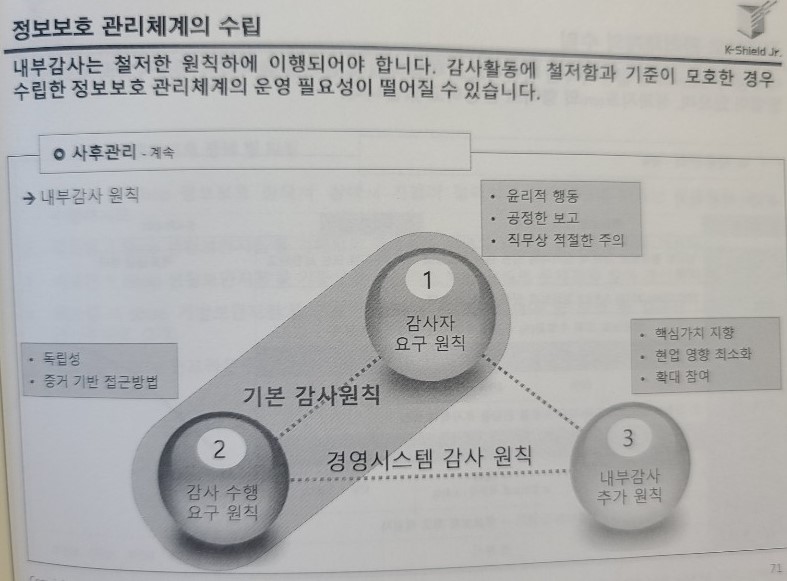
- 위험처리 방법이 결정된 이슈 및 문제점을 해결하기 위한 구체적인 계획을 수립 후 이행 가능하도록 영역을 구분하여 과제화 한다.

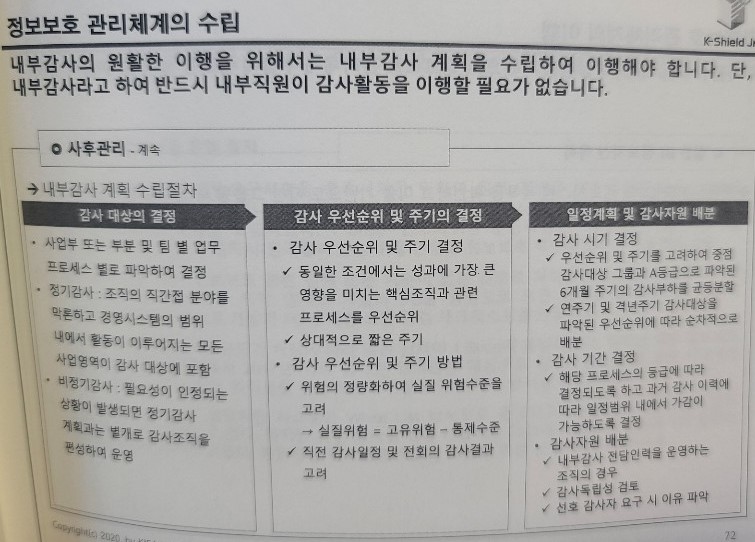
- 수립된 이행조치 과제는 조직 내 사업단위 활동으로 구성하여 구체적인 추진 조직과 목표, 이행 세부계획, 예산, 일정 등을 수립한다.

- 위험 평가 결과 -> 대책 선정 -> 프로젝트 선정 -> 우선순위 결정 -> 이행계획 정리

**사후관리**







**물리 보안 운영**

**물리적 보안요구사항**

- 눈으로 보이는 사전에 허가된 사람, 차량, 장비만 사업장에 드나들 수 있도록 통제하는 것이다.

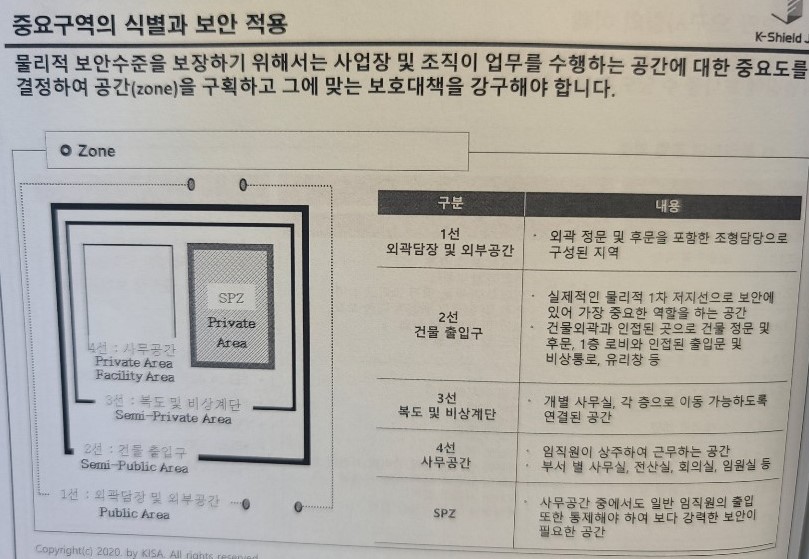
**물리적 보안체계의 구성**

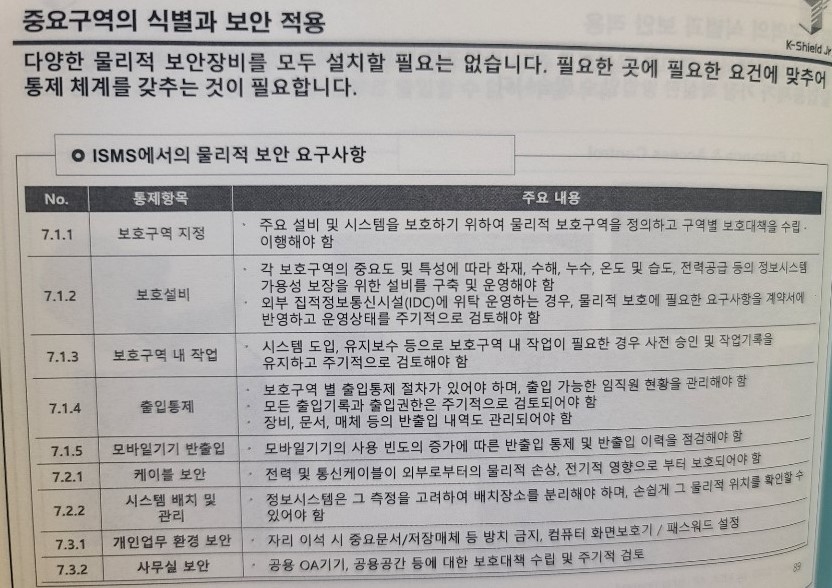
- Zone( + Special Protection Zone)

-> Entrance

-> Access Control (+ Vehicle)

-> Perimeter Detection (주변 감시)(cctv 등)





**개인정보보호 운영**

- 가명정보 vs 익명정보

가명정보란 가명처리를 함으로써 원래 상태로 복원하기 위해서 추가정보를 사용하거나 결합하는 그런게 없으면 개인을 알아볼 수 없는 정보

익명정보란 누군지 알아볼수 없도록 마스킹처리한 정보

