2023학년도 1학기

정보보안관리및법규 storyboard

주차 및 주차명	7주차. 1~6주 수업정리 및 문제풀이		
작성일자			
담당교수	김근혜		

서울사이버대학교

학습개요 이번 주차의 학습목표와 학습내용을 확인하세요.

학습목표

- 1~6주 동안 학습한 수업 내용을 숙지할 수 있다.
- 관련 학습문제를 함께 풀어보며 적용할 수 있다.

학습내용

1. 수업정리
2. 퀴즈 풀어보기

수업정리

1~2주 수업정리

1주: 정보보호 기본 개념

정보화 시대의
특징과 역기능

팬데믹 기간
사이버보안
환경의 변화

정보보안과
사이버보안
특징 및 역사

1~2주 수업정리

1주: 정보보호 기본 개념

정보화 시대의 특징

1. 산업 경제에서 지식 기반 경제로 전환됨
2. 통신 및 정보 교환을 위한 정보통신 기술(ICT)에 대한 의존도가 높음
3. 대량의 데이터를 처리 · 저장 · 전송하기 위한 ICT기술을 사용함
4. 통신 및 정보 교환을 위해 인터넷을 광범위하게 사용함
5. 비즈니스, 교육, 의료 등 경제의 다양한 분야에서 효율성과 생산성을 향상시키기 위한 ICT기술을 활용함
6. 뉴스, 음악, 비디오와 같은 디지털 콘텐츠를 제작 및 보급함

1~2주 수업정리

1주: 정보보호 기본 개념

정보화 시대의 특징

7 의사결정을 위한 데이터 수집 · 분석 · 사용이 증가함

8 많은 사람들이 온라인 플랫폼을 사용하여 프리랜서 또는 계약 기반으로 일하는 긱(Geek) 경제가 부상함

9 가상 커뮤니티 및 온라인 마켓 플레이스와 같은 새로운 형태의 사회 및 경제 조직이 출현함

10 재택근무와 원격근무의 증가와 함께 업무와 고용의 성격이 변화함

11 사람들이 언제든지 온라인으로 연결하고 소통할 수 있기 때문에 일과 여가의 경계가 모호해짐

1~2주 수업정리

1주: 정보보호 기본 개념

정보화 시대의 역기능

디지털 격차	특정 개인 또는 커뮤니티가 기술 또는 인터넷 액세스에 대한 액세스 권한이 없거나 이를 감당할 수 없는 디지털 격차로 인해 사회적 및 경제적 불평등이 발생함
기술 의존도	비판적 사고 능력, 주의 지속 시간 및 문제해결 능력 감소로 이어질 수 있는 기술에 대한 의존도가 증가함
사이버보안 위험	해킹, 신원 도용, 잘못된 정보 또는 선전의 확산과 같은 사이버보안 위험이 증가함
개인정보보호 문제	회사, 정부 및 기타 조직에서 개인 데이터를 수집하고 공유하므로 개인정보보호 문제가 발생함

1~2주 수업정리

1주: 정보보호 기본 개념

정보화 시대의 역기능

산업 붕괴	자동화와 디지털화가 증가함에 따라 전통적인 직업과 산업이 붕괴됨
신체활동 감소	디지털 엔터테인먼트와 인터넷의 등장으로 좌식 생활 방식이 증가하고 신체활동이 감소함
사회적 고립	사람들이 온라인에서 더 많은 시간을 보내면서 대면 상호 작용 및 인간 접촉에서 단절됨
에코 챔버 (Eco Chamber)	소셜 미디어와 인터넷이 거짓 정보 또는 오해의 소지가 있는 정보를 영속화할 수 있는 잘못된 정보 및 뉴스 에코 챔버가 확산됨

1~2주 수업정리

1주: 정보보호 기본 개념

정보화 시대의 역기능

건강 및 웰빙 이슈	스트레스, 불안, 우울증, 중독 및 중독 사례가 더 많아 정신 건강 및 웰빙에 미치는 영향이 커짐
디지털 과부하	디지털 중독 및 디지털 과부하의 위험이 증가함

1~2주 수업정리

1주: 정보보호 기본 개념

팬데믹 기간 사이버보안 환경의 변화

재택근무

- 팬데믹 기간 동안 많은 사람들이 집에서 일하면서 조직은 직원들이 집에서 회사 네트워크에 액세스할 수 있도록 원격 액세스 솔루션을 신속하게 구현해야 했음
  - ✓ VPN(가상 사설망) 및 클라우드 기반 협업 도구의 사용이 증가하여 새로운 보안 위험이 발생할 수 있음

피싱 및 사회 공학

- 사이버범죄자들은 전염병을 이용하여 COVID-19 관련 주제를 사용하여 사람들을 속여 개인정보를 제공하거나 맬웨어를 설치하도록 하는 피싱 캠페인을 장려함
- 사기꾼들은 사람들이 가짜 자선 단체에 기부하도록 속이기 위해 팬데믹을 이용함

1~2주 수업정리

1주: 정보보호 기본 개념

팬데믹 기간 사이버보안 환경의 변화

공격 표면 증가

- 원격으로 작업하는 사람의 수가 증가함에 따라 조직은 민감한 시스템 및 데이터에 대한 액세스를 더 많은 사람에게 개방해야 했음
  - ✓ 공격자가 표적으로 삼을 수 있는 공격 표면이 증가하여 무단 액세스가 더 쉬워짐

사이버보안 전문가 부족

- 팬데믹으로 인해 디지털화 및 원격 작업의 급격한 증가로 인해 사이버보안 전문가의 수요가 높아 전 세계적으로 사이버보안 전문가가 부족함

1~2주 수업정리

1주: 정보보호 기본 개념

팬데믹 기간 사이버보안 환경의 변화

예산 부족	☑ 많은 조직이 팬데믹으로 인한 경제 침체의 영향을 받아 사이버보안 솔루션 및 교육에 투자하기 어려워짐
사이버보안 서비스 증가	☑ 팬데믹으로 인해 점점 더 많은 비즈니스가 원격으로 운영되어야 하므로 사이버보안 서비스에 대한 필요성이 급격히 증가함 ☑ 많은 조직이 디지털 자산을 보호하기 위해 MSSP(관리형 보안 서비스 공급자)로 전환하고 있음

1~2주 수업정리

1주: 정보보호 기본 개념

정보보안과 사이버보안의 차이점

정보보안		사이버보안
☑ 기밀성, 무결성 및 가용성을 유지하기 위해 무단 액세스, 수정 또는 삭제로부터 데이터를 보호하는 프로세스	정의	☑ 외부 소스로부터 인터넷상의 데이터를 보호하는 프로세스
☑ 모든 유형의 위협으로부터 데이터를 보호하는 데 중점	보호 대상	☑ 무단 디지털 액세스로부터 데이터를 보호하는 데 중점 ☑ 사이버공간을 사용할 때 사이버공격을 방어할 수 있는지에 관한 것

1~2주 수업정리

1주: 정보보호 기본 개념

정보보안과 사이버보안의 차이점

정보보안		사이버보안
☑ 물리적 및 디지털 정보에 적용 ☑ 소스에 관계없이 모든 유형의 데이터에 적용	정보	☑ 디지털 정보에 적용 ☑ 인터넷에 연결된 모든 것을 보호하는 데 사용
☑ 무단 액세스, 공개, 사용, 수정, 중단 또는 파괴로부터 정보를 보호	기능	☑ 무단 액세스, 사이버범죄, 사이버사기 및 법 집행 기관으로부터 정보를 보호
☑ 기술적용	기술 영역	☑ 기술 및 이론적용
☑ 컴퓨터 과학 (Computer Science)	학문 영역	☑ 컴퓨터 과학, 컴퓨터 공학 (Computer Science and Computer Engineering)

1~2주 수업정리

1주: 정보보호 기본 개념

정보보안과 사이버보안의 차이점

정보보안		사이버보안
☑ 모든 종류의 무단 액세스를 방지해야 함	전문가 과제	☑ 무단 디지털 액세스를 방지해야 함
☑ 위험을 처리하기 전에 리소스의 우선 순위를 지정해야 함		☑ 지능적이고 지속적인 위협을 처리해야 함
☑ 정보 자산, 기밀성, 무결성 및 가용성과 관련이 있음		☑ 소셜 미디어 계정, 개인정보 보호 등과 같이 존재하거나 존재하지 않을 수 있는 사이버위험을 처리해야 함

1~2주 수업정리

2주: 정보보호 관리의 개념

1~2주 수업정리

2주: 정보보호 관리의 개념

정보보호 주요정의

기밀성	오직 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 한다는 원칙
무결성	정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질
가용성	정당한 사용자가 정보시스템의 데이터 또는 자원을 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있는 성질

1~2주 수업정리

2주: 정보보호 관리의 개념

정보보호 주요정의

인증	임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는데 사용되는 성질
책임추적성	보안 목적에는 개체의 행동을 유일하게 추적해서 찾아낼 수 있어야 한다는 사항

1~2주 수업정리

2주: 정보보호 관리의 개념

정보보호 관리

기술적 보호대책	정보 시스템, 통신망, 정보(데이터)를 보호하기 위한 가장 기본적인 대책
물리적 보호대책	화재, 수해, 지진, 태풍 등과 같은 자연재해로부터 정보시스템이 위치한 정보처리시설을 보호하기 위한 자연재해 대책
관리적 보호대책	법, 제도, 규정, 교육 등을 확립하고, 보안계획을 수립하여 이를 운영(보안등급, 액세스 권한 등)하며, 위험분석 및 보안감사를 시행하여 정보시스템의 안전성과 신뢰성을 확보하기 위한 대책

1~2주 수업정리

2주: 정보보호 관리의 개념

기본 보안 용어 정의

공격자	시스템을 공격하거나 위협하는 존재
공격	시스템의 보안서비스를 회피하여 보안 정책을 위반하려는 의도된 시도
대응	피해의 최소화 및 적절한 대응을 위해 탐지 · 보고하여 위험, 노출, 공격을 제거하거나 방지하는 행위, 장비, 기법
위험	특정 위협이 가져올 피해가 확률적으로 표현되는 예상 손실
보안정책	시스템이나 기관이 민감하고 중요한 시스템 지원에 보안서비스를 제공하기 위해 명시한 규정과 업무

1~2주 수업정리

2주: 정보보호 관리의 개념

기본 보안 용어 정의

자산	정보 시스템 내의 데이터, 시스템의 서비스, 처리 기능, 통신 대역폭, 시스템 장비(하드웨어, 펌웨어, 소프트웨어, 문서) 시스템 장비 설비
위협	보안을 침해하고 손해를 가져올 수 있는 상황, 행위, 이벤트가 존재할 때의 잠재적 보안 위반
취약점	시스템 보안 정책을 위반할 수 있는 시스템 설계, 구현, 혹은 운영, 관리상의 오류 및 약점

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

IT 거버넌스의 개념

IT 투자가 기업의 사업의 목표를 뒷받침할 수 있도록 하는
프레임워크(Framework)임

1990~2000년대 대형 기업 사기 사건이 발생함

▼

'그람-리치-블라일리 법'(Gramm-Leach-Bliley Act,
일명 Financial Modernization Act)와
'사베인 옥슬리 법'(Sarbanes Oxley Act) 등이 제정됨

▼

기업이 활용해야 할 핵심 프레임워크로 자리잡기 시작함

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

IT 거버넌스의 개념

역할 및 개념

- 기업의 전략을 지원하는 IT의 전략에서부터 그 전략을 통하여 기업에 가치를 제공함
  - ✓ 전략 달성에 부정적 영향을 미치는 위험을 관리함
  - ✓ 기 투자된 IT 자원을 효율적으로 관리하여 그 결과인 성과측정으로 전략에 피드백 되는 일련의 체계를 말함
- IT와 IT프로세스의 위험과 수익 사이에 균형을 맞추어 가치를 창출하면서 기업의 목적을 달성하기 위한 기업통제의 관계구조 및 프로세스임

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

IT 거버넌스의 필요성

1. IT Management만 실행했을 경우의 문제점이 존재함
2. 조직이 IT에 의존할수록 IT 환경의 취약성은 조직 전체의 문제로 다가옴
   - 의존성이 커짐에 따라, IT 투자를 통한 비즈니스 가치 창출과 IT 관련 리스크 관리, 예방 및 대처를 위해서 IT Governance에 집중하게 됨
3. 사이버 범죄, 부정행위 등 다양한 종류의 외부 위협이 존재함
4. IT 투자에 막대한 자금이 소요되기 때문에 IT Governance를 통한 IT Paradox를 방지할 수 있음

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

정보보호 거버넌스 개념

정보보호 거버넌스	기업 거버넌스의 일환으로써 비즈니스와의 전략적 연계, 관련법과 규정의 준수, 의사결정 권한과 책임의 할당을 위한 프로세스 및 실행체계
거버넌스 프레임워크	보안통제 감시결과를 토대로 점수화된 위험결과에 따라 보안 성능을 판단 · 유지하는 것

- 결국 조직의 사이버보안은 조직 비즈니스에 따라 서로 다른 형태를 보이고 경영보안의 하나가 됨
- 그동안 전산 및 IT 부서가 조직의 경영에 큰 역할을 했다면 이젠 사이버보안이 조직 경영상에 하나의 경영형태로 참여하는 것임

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

정보보호 거버넌스 목표

책임성 (Accountability)	정보보호 활동의 성과에 대해 누가 책임을 지는가?	기업 거버넌스의 책임성과 연계
비즈니스 연계성 (Business Alignment)	정보보호 활동이 기업의 비즈니스 목표 달성에 기여하는가?	기업 거버넌스의 효과성과 연계
준거성 (Compliance)	정보보호 활동이 원칙과 기준 (법, 제도, 기업 내부의 규정 등)에 따라 수행되는가?	기업 거버넌스의 투명성과 연계

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

정보보호 거버넌스 장점

1. 거버넌스에 좋은 보안실무경험(Practice)의 조직 공유를 활성화함
2. 조직의 보안위험을 줄이고 비즈니스 운영과정의 불확실성을 경감할 가능성이 있음
3. 정보의 부정확성, 부재 등으로 인한 법적 문제점이 증가되는 것을 막고 보호함
4. 제한된 보안자원을 최적으로 배치할 수 있는 프레임워크를 제공함

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

정보보호 거버넌스 장점

5 효과적인 정보보안 정책과 법적 적합성을 제공함

6 정보보안을 수행하면서 효과적이고 효율적인 위험관리,
빠른 사고관리 프로세스 개선으로 기업의 단단한 운영기반이 됨

7 정보 부재로 인해 잘못된 결정을 내리지 않도록 보완함

8 기업 합병, 기업 획득, 비즈니스 복구, 법률 변경 등
중요한 기업 활동에 정보의 정확성과 책임 추적 기능을 제공함

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

IT 보안관리 - ISO/IEC 27000 시리즈

ISO/IEC 27000(Overview & Vocabulary)

- 개관 및 용어
  - ✓「정보보안 관리 체계-개관 및 어휘」에서는 정보보안 관리 시스템에 대한 개관 및 27000 계열 표준에서 사용된 어휘를 정의하고 있음

ISO/ ICE 27001(ISMS Requirements Standards)

- 정보보안 ISMS 요구사항
  - ✓「정보보안 관리 체계-요구사항」에서는 정보보안 관리 체계에 대한 문서의 수립, 이행, 운영, 모니터링, 검토, 유지보수, 개선을 위한 요구사항을 명시하고 있음

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

IT 보안관리 - ISO/IEC 27000 시리즈

ISO/IEC 27002(Code of Practice for ISMS)

- 정보보안 관리를 위한 실행규약
  - ✓「정보보안 관리를 위한 실무규약」에서는 조직에서의 정보보안 관리를 위한 지침이 나와 있으며, 정보통제를 위한 최선 실무에 대한 목록도 포함하고 있음
  - ✓ 이것은 예전에 ISO177799로 알려져 있음

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

IT 보안관리 - ISO/IEC 27000 시리즈

ISO/IEC 27003(ISMS Implementation Guide)

- ISMS 구현 지침
  - ✓「정보보안 관리 체계 이행 가이드라인」에서는 정보보안 관리 체계 명세서 및 설계서의 시작부터 제작과정까지 자세히 다룸

ISO/IEC 27004(Measurement)

- 정보보안관리 지표 프레임워크를 위한 지침
  - ✓「정보보안 관리 측정」에서는 조직의 정보보안 관리 체계 프로세스 및 통제 효율성을 측정하고 보고하는 것을 돕는 지침을 제공함

3~4주 수업정리

3주: 정보보호 거버넌스와 관리체계 수립 1

IT 보안관리 - ISO/IEC 27000 시리즈

ISO/IEC 27005(Risk Management)

- 정보보안 위험관리 지침
  - ✓「정보보안 위험 관리」에서는 정보보안 위험 관리 프로세스에 대한 지침을 제공함
  - ✓ 이 문서는 ISO13335-3/4를 대체함

ISO/IEC 27006(Certification or Registration Process)

- 「정보보안 관리 체계를 감사 및 인증하는 기관에 대한 요구사항」에서는 감사 및 인증기관에 대한 요구사항을 명시하고 지침을 제공함

3~4주 수업정리

4주: 정보보호 거버넌스와 관리체계 수립 2

정보보호
거버넌스와
정책구현

인적자원 보안

3~4주 수업정리

4주: 정보보호 거버넌스와 관리체계 수립 2

정보보호 거버넌스와 체계수립

정보보호 거버넌스 등장배경

- 정보보호 투자가 현업부서의 목적과 부합해야 한다는 요구가 증대되고 있음
- 정보기술이 기업의 핵심 운영요소로 자리 잡으면서 정보기술의 가시성(visibility)에 대한 이사회 및 경영진의 요구가 증대되고 있음
- 정보보호 거버넌스는 회사의 이사회 및 경영진 측에서 회사의 위험이 적절한 수준으로 관리되고 있음을 감독할 수 있는 메커니즘을 제공해야 함

정보보안 거버넌스란 정보보안관리체계, 즉 ISMS(Information Security Management System)의 기반이라고 볼 수 있음

3~4주 수업정리

4주: 정보보호 거버넌스와 관리체계 수립 2

정보보호 거버넌스 구현요건

전략적 연계	정보보호 거버넌스는 비즈니스, IT 목표 및 정보보안 전략이 서로 연계되어야 함
위험관리	조직의 정보보안 사고의 잠재적 위험을 줄이기 위해 조직에 적합한 위험 관리 체계를 수립해야 함
자원관리	효율적인 정보 보안 지식과 자원을 관리하기 위해 중요 정보 자산과 인프라를 포함하는 전사적 정보보안 아키텍처를 확보해야 함
성과관리	정보보안 거버넌스의 효과적인 운영 척도로서 모니터링, 보고 및 평가에 따른 성과 평가 체계를 운영해야 하며 비즈니스 측면도 고려하여 성과를 평가해야 함
가치전달	정보 보안 투자를 최적화하기 위해 기업의 구성원에게 정보 보안의 중요성과 가치를 교육시켜야 함

3~4주 수업정리

4주: 정보보호 거버넌스와 관리체계 수립 2

정보보호 거버넌스와 정책구현

정보보호 정책	☑ 문서화된 사업 규칙의 특수한 형태로서 정보보호에 관한 경영진의 목표와 방향을 제시하는 것 ☑ 가장 상위 규정이나, 실무적으론 그 하위의 지침 등을 모두 포괄하는 표현으로 사용되기도 함
표준	☑ 정보보호 정책의 하위의 개념 ☑ 정책 목적을 달성하기 위하여 세부적인 사항을 사규 또는 내규 등으로 정형화하여 조직 내에서 일률적으로 준수하도록 하는 강제성이 있는 규정

3~4주 수업정리

4주: 정보보호 거버넌스와 관리체계 수립 2

정보보호 거버넌스와 정책구현

지침	☑ 정보보호 정책 또는 표준처럼 강제적이지는 않지만, 정보보호의 정책을 달성하기 위해 도움이 될 수 있는 구체적인 사항을 설명한 권고 사항
절차	☑ 정책을 달성하기 위한 단계적 방안을 구체적으로 기술한 것 ☑ 누가 무엇을 어떻게 해야 하는지 세부적으로 규정 ☑ 정책, 표준과 마찬가지로 필수적으로 준수해야 하는 사항
기준선	☑ 일관되게 참조할 포인트

3~4주 수업정리

4주: 정보보호 거버넌스와 관리체계 수립 2

인적 자원 보안

직무순환은 직원공모의 위험을 감소시킴

- 직무순환은 예방, 탐지 목적의 인적 통제임
- 직무분리를 통해 보안 전반에 대한 절대적인 권한 소유가 불가능해짐

최소권한(알 필요성)

직무에 필요한 권한만을 부여함

강제휴가

직무순환과 유사한 효과이며,
탐지통제임

5~6주 수업정리

5주: 정보보호 위험관리 1

정보보호의
위험관리

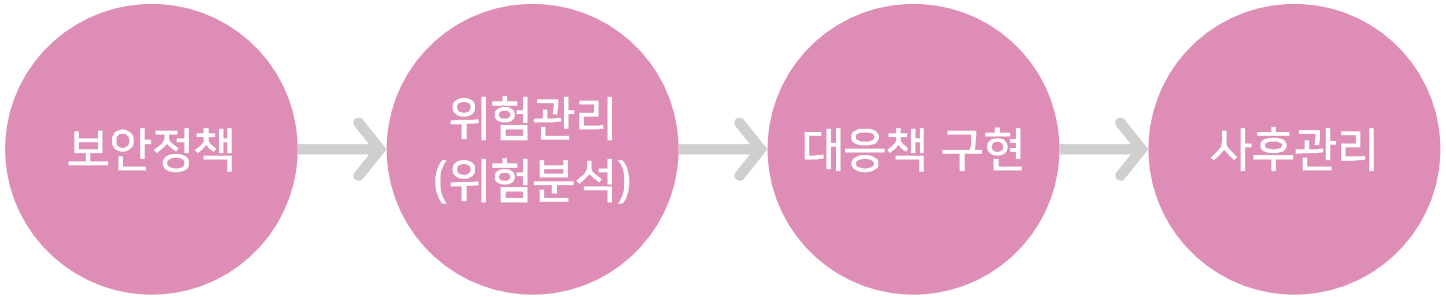
정보보호의
위험분석

5~6주 수업정리

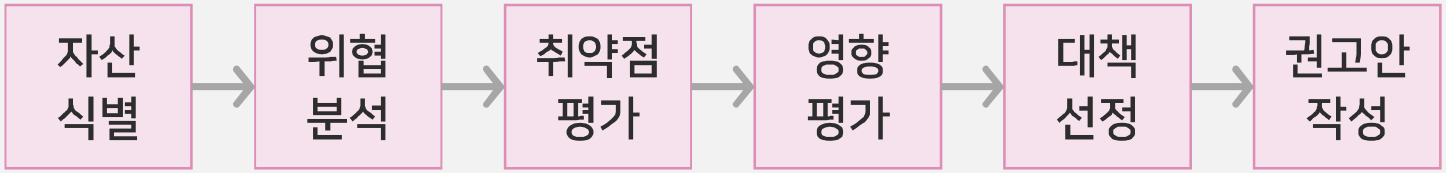
5주: 정보보호 위험관리 1

정보보호의 위험관리란?

조직의 자산에 대한 위험을 수용할 수 있는 수준으로 유지하기 위한 과정



위험관리

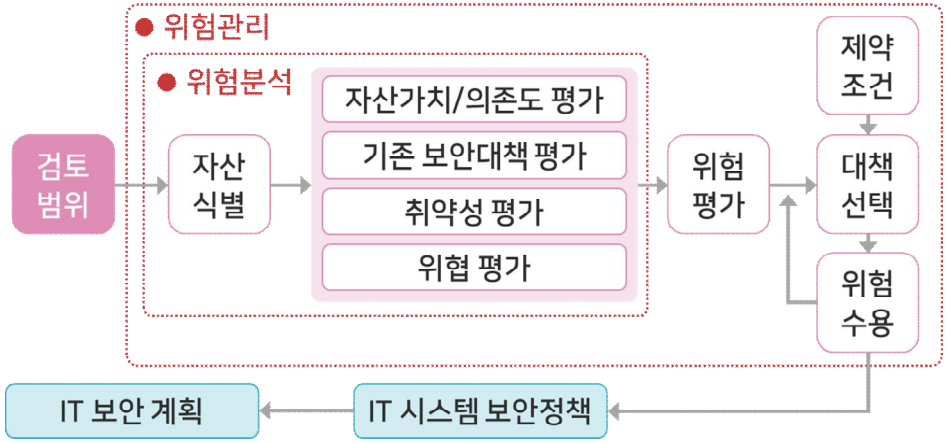


5~6주 수업정리

5주: 정보보호 위험관리 1

위험관리 절차 - 검토 범위

위험분석 범위 선정	조직의 업무, 위치, 자산 및 기술적 특성에 따라 정보보호 관리체계 범위에 근거하여 범위 설정	
위험분석 방법 선정	계량화 여부에 따른 방법	정량적 방법, 정성적 방법
	접근방법에 따른 방법	베이스라인 접근법, 비정형 접근법, 상세 위험분석, 복합 접근법



5~6주 수업정리

5주: 정보보호 위험관리 1

위협분석의 종류

[정보기술 보안관리를 위한 국제 표준 지침(ISO/IEC 13335-1)]

5~6주 수업정리

5주: 정보보호 위험관리 1

위험분석 방법 및 장·단점 비교

기준선 접근법	
특징	☑ 모든 시스템에 대하여 표준화된 정보보호 대책 세트를 제공 ☑ 체크리스트 형태 ☑ 정보보호 대책의 유무를 판단하여 없는 것을 구현
장점	☑ 비용 및 시간절약
단점	☑ 과보호 또는 부족한 보호가 될 가능성 상존 ☑ 보안환경 변화 반영 미비 ☑ 점수에 집착 ☑ 계량화가 어려움

5~6주 수업정리

5주: 정보보호 위험관리 1

위험분석 방법 및 장·단점 비교

비정형화된 접근법	
특징	☑ 모든 정보자산에 기업 이외의 전문가 지식 및 경험을 활용하는 방법(전문가 판단법)
장점	☑ 비용 대비 효과가 우수하며 소규모 조직에 적합 ☑ 상세위험분석보다 빠름
단점	☑ 누락하는 경우가 발생 ☑ 설정의 근거가 희박하여, 검토자의 개인적 경험에 지나치게 의존 ☑ 전문성이 높은 인력이 수행하지 않으면 실패할 위험 ☑ 측정의 완전도 높음

5~6주 수업정리

5주: 정보보호 위험관리 1

위험분석 방법 및 장·단점 비교

상세위험분석 접근법	
특징	☑ 모든 정보자산에 대해 상세위험분석을 하는 방법
장점	☑ 자산가치, 위협, 취약점의 평가에 기초한 위험을 산정하므로 경영상 허용수준까지 위험을 줄이는 근거가 명확 ☑ 계량적 수치화 가능 ☑ 평가의 완전도 높음
단점	☑ 상당한 시간, 노력이 소요 ☑ 고급의 숙련된 인력 필요

5~6주 수업정리

5주: 정보보호 위험관리 1

위험분석 방법 및 장·단점 비교

복합 접근법	
특징	☑ 기준선 접근법과 상세위험분석을 조합하여 분석하는 방법
장점	☑ 비용 및 지원을 효과적으로 사용 ☑ 고위험 영역으로 빠르게 식별하고 처리 ☑ 부분적 계량화
단점	☑ 기준선 접근법이 부정확한 경우 상세위험분석이 필요한 시스템이 누락 ☑ 고위험 영역이 잘못 식별되었을 경우 비용 낭비 및 부적절한 내용

5~6주 수업정리

5주: 정보보호 위험관리 1

기업의 규모에 따른 위험분석 방법

베이스라인 접근법	IT 보안관리에 투자할 자원이 부족한 작은 조직에 적합한 기법임
비정형화된 접근법	IT 시스템이 조직의 목표 달성에 핵심적이지 않은 중소규모 조직에 적합함
상세위험 분석	IT 시스템이 조직의 목표 달성에 핵심적이고 IT 보안관리에 충분한 자원을 투입할 수 있는 큰 조직에 적합함
복합 접근법	베이스라인 접근법, 비정형 접근법 그리고 상세 위험분석을 상황에 맞게 복합적으로 적용하며, 비용대비 효과가 높아 대부분의 조직에 권고되고 있음

5~6주 수업정리

6주: 정보보호 위험관리 2

5~6주 수업정리

6주: 정보보호 위험관리 2

상세 위험분석

자산분석	조직의 자산규모를 파악하고 자산의 가치 및 중요도를 산출하며 자산과 업무처리와의 관계도 알아낼 수 있는 과정
위협분석	자산에 피해를 가할 수 있는 잠재적인 요소인 위협을 파악하고 발생할 가능성 등을 분석하는 과정
취약점분석	자산분석을 통하여 도출된 자산의 속성과 중요도를 바탕으로 자산이 가지고 있는 취약점을 식별하고 취약점이 전체적인 위험에 미칠 수 있는 영향을 분석하는 것

5~6주 수업정리

6주: 정보보호 위험관리 2

상세 위험분석

대응책분석	네트워크 및 시스템을 새로 구축하는 경우와 운영 중인 자산에 필요한 대응책을 조사하여 이들 대응책들의 기본 수행여부를 파악하는 것
위험평가	자산분석, 취약점분석, 위험분석, 대응책분석을 통하여 얻은 데이터와 분석결과를 바탕으로 위험을 측정하고 평가한 후 대응책을 제시해주는 위험분석의 최종 단계
잔류 위험평가	위험분석 결과에 대한 종합적인 평가를 하기 전에 추천한 대응책을 적용할 때 보안 정책에 명시되어 있는 허용 위험수준을 만족하는지 검증하는 것

5~6주 수업정리

6주: 정보보호 위험관리 2

위험처리전략

위험수용	☑ 현재의 위험을 받아들이고 잠재적 손실 비용을 감수하는 것
위험감소	☑ 위험수준을 낮추는 대책은 위험결과를 낮추는 대책과 위험발생 가능성을 낮추는 대책으로 나눌 수 있음 ☑ 취약점이 악용될 가능성을 줄이기 위해 적합한 통제를 이행함으로써 위험감소가 이루어짐

5~6주 수업정리

6주: 정보보호 위험관리 2

위험처리전략

위험전가	✓ 위험에 대한 책임을 제3자와 공유하는 것 ✓ 위험전이는 비용을 동반함
위험회피	✓ 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것

5~6주 수업정리

6주: 정보보호 위험관리 2

정량적·정성적 위험분석의 장·단점

정량적 위험분석		정성적 위험분석
☑ 객관적인 평가기준이 적용됨 ☑ 정보의 가치가 논리적으로 평가되고 화폐로 표현되어 납득이 더 잘 됨 ☑ 위험관리 성능평가가 용이함 ☑ 위험평가 결과가 금전적 가치, 백분율, 확률 등으로 표현되어 이해하기 쉬움	장점	☑ 계산에 대한 노력이 적게 듦 ☑ 정보자산에 대한 가치를 평가할 필요가 없음 ☑ 비용/이익을 평가할 필요가 없음

5~6주 수업정리

6주: 정보보호 위험관리 2

정량적·정성적 위험분석의 장·단점

정량적 위험분석		정성적 위험분석
☑ 계산이 복잡하여 분석하는데 시간, 노력, 비용이 많이 듦 ☑ 수작업의 어려움으로 자동화 도구를 사용할 시 신뢰도가 벤더에 의존됨	단점	☑ 위험평가 과정과 측정기준이 지극히 주관적이어서 사람에 따라 달라질 수 있음 ☑ 측정결과를 화폐가치로 표현하기가 어려움 ☑ 위험완화 대책의 비용/이익 분석에 대한 근거가 제공되지 않고, 문제에 대한 주관적인 지적만 있음 ☑ 위험관리 성능을 추적할 수 없음

5~6주 수업정리

6주: 정보보호 위험관리 2

정량적 위험분석 방법의 종류

과거자료 분석법	✓ 미래 사건의 발생 가능성을 예측하는 방법으로 과거의 자료를 통해 위험발생 가능성을 예측함 ✓ 위협에 대한 과거자료가 많을수록 정확도가 높아짐 ✓ 과거에 일어났던 사건이 미래에도 일어난다는 가정이 필요하며, 과거의 사건 중 발생빈도가 낮은 자료에 대해서는 적용이 어렵다는 단점이 있음
수학공식 접근법	✓ 위협의 발생 빈도를 추정하여 분석하는 데 유용함 ✓ 위험을 정량화 하여 매우 간결하게 나타낼 수 있으나, 기대 손실을 추정하는 자료의 양이 적다는 단점이 있음

5~6주 수업정리

6주: 정보보호 위험관리 2

정량적 위험분석 방법의 종류

확률 분포법	✓ 미지의 사건을 추정하는 데 사용하는 방법 ✓ 확률적 편차를 이용하여 최저, 보통, 최고의 위험 분석을 예측할 수 있음 ✓ 정확성은 낮음
점수법	✓ 위험발생 요인에 가중치를 두어 위험을 추정하는 방법 ✓ 소요되는 시간이 적고 분석해야 할 자원의 양이 적다는 장점이 있으나, 정확도가 떨어지는 단점이 있음

5~6주 수업정리

6주: 정보보호 위험관리 2

정성적 위험분석 방법의 종류

델파이법

- 시스템에 관한 전문적인 지식을 가진 전문가 집단이 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약점을 토론을 통해 분석하는 방법
- 시간과 비용을 절약할 수 있으나, 전문가의 지식과 토론만으로 위협요소 등을 추정하기 때문에 정확도가 낮음

5~6주 수업정리

6주: 정보보호 위험관리 2

정성적 위험분석 방법의 종류

시나리오법

- 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정조간 하의 위협에 대해 발생 가능한 결과를 추정하는 방법임
- 적은 정보를 가지고 전반적인 가능성을 추론할 수 있음
- 위험분석팀과 관리층 간의 원활한 의사소통도 가능케 함

BUT 발생 가능한 사건의 이론적인 추측에 불과하고 정확성, 완성도, 이용 기술 수준 등이 낮음

5~6주 수업정리

6주: 정보보호 위험관리 2

정성적 위험분석 방법의 종류

순위 결정법

- 비교 우위 순위 결정표에 위험 항목들의 서술적 순위를 결정하는 방법
- 이 방법은 위험 분석에 소요되는 시간과 분석해야 하는 자원의 양이 적다는 장점이 있으나, 위험 추정의 정확도가 낮다는 단점이 있음

퍼지 행렬법

- 자산, 위험, 보안체계 등 위험 분석 요소들을 정성적인 언어로 표현된 값을 사용하여 기대손실을 평가하는 방법
- 자산 가치의 크고 적음을 화폐가치로 표현하고 위협발생확률의 높고 낮음을 변수로 표현하여 수학적으로 계산하는 방법임

퀴즈 풀어보기

1~6주 관련 문제풀이

Q1 다음 중 정보화 시대의 특징이 아닌 것은?

1. 산업 경제에서 지식 기반 경제로 전환되었다.
2. 통신 및 정보 교환을 위한 정보통신 기술(ICT)에 대한 의존도가 높다.
3. 통신 및 정보 교환을 위해 인터넷을 광범위하게 사용한다.
4. 자동화와 디지털화가 증가함에 따라 전통적인 직업과 산업이 붕괴되었다.

1~6주 관련 문제풀이

Q2 다음 중 정보보호 거버넌스 구현요건이 아닌 것은?

1. 표준설립
2. 자원관리
3. 위험관리
4. 전략적 연계

1~6주 관련 문제풀이

Q3 다음 중 정보시스템에서 보호해야 할 대상으로 가장 거리가 먼 것은?

1. 소프트웨어
2. 데이터
3. 네트워크
4. 물적요소

1~6주 관련 문제풀이

Q4 송신자 A가 수신자 B에게 메시지를 보낼 때 발생할 수 있는 보안위협에 대응하는 보안기술에 대한 설명으로, 각 보안서비스로 알맞은 것은?

> 가. A로부터 B에게 전송된 메시지가 변경 없이 전송되었는지를 확인하는 보안 서비스는?
>
> 나. 수신자 B가 받은 메시지가 분명히 송신자 A가 보낸 것인가를 확인하는 보안서비스는?
>
> 다. 전송 중의 메시지가 공격자에게 노출되는 것에 대응하는 보안서비스는?

1. (가) 기밀성, (나) 인증, (다) 무결성
2. (가) 가용성, (나) 무결성, (다) 기밀성
3. (가) 부인봉쇄, (나) 가용성, (다) 무결성
4. (가) 무결성, (나) 인증, (다) 기밀성

1~6주 관련 문제풀이

Q5 다음 암호 공격 중 능동적 공격에 해당되지 않는 것은?

1. 메시지 변조: 전송되는 메시지들의 순서를 바꾸거나 또는 메시지의 일부분을 다른 메시지로 대체하여 불법적인 효과를 발생시키는 공격
2. 전송되는 파일을 도청: 불법적인 공격자나 전송되는 메시지를 도중에 가로채어 그 내용을 외부로 노출시키는 공격
3. 삽입 공격: 불법적인 공격자가 정당한 송신자로 가장하여 특정 수신자에게 메시지를 보내어 불법적인 효과를 발생시키는 공격
4. 삭제 공격: 정상적인 통신시설의 사용이나 관리를 방해하는 서비스 거부 공격에 해당되며, 특정 수신자에게 전송되는 메시지의 전부 또는 일부가 공격자가 의해 삭제되는 것

1~6주 관련 문제풀이

Q6 다음 중 위험도 산정 시 고려할 구성 요소가 아닌 것은?

1. 자산
2. 위협
3. 취약점
4. 직원

1~6주 관련 문제풀이

Q7 다음 정보보호 거버넌스 프로세스에 대한 설명으로 틀린 것은?

1. 최고경영층은 실행조직의 보고 내용을 검토 및 완료한다.
2. 실무 조직은 실행 조직에게 직접 보고하고 경영진 보고에 참여한다.
3. 최고경영층은 실행조직이 수행한 결과를 관찰하여 평가한다. (실행조직에는 정보보호 조직과 정보보호 업무를 일부 수행하는 다른 조직이 포함)
4. 최고경영층은 보안활동이 잘 되고 있는지를 객관적으로 전문적인 기관에 검토 의뢰 및 결과를 검토한다.

1~6주 관련 문제풀이

Q8 다음 중 정보보호와 비즈니스와의 관계를 설명한 내용으로 올바르지 않은 것은?

1. 신규 비즈니스를 운영하는 데 있어서 비즈니스와 정보보호가 서로 상충되는 경우 정보보호를 최우선적으로 고려해야 한다.
2. IT 인프라에 대한 정보보호는 곧 비즈니스 보호와 비즈니스 가치를 증대시키는 중요한 활동으로 인식되어야 한다.
3. 자산의 위협, 취약점, 공격 등으로부터 보호하기 위해서 정보보호 관리가 요구된다.
4. 비즈니스를 운영함에 있어서 법률 준거성을 우선적으로 고려하여 정보보호 대책을 구현하여야 한다.

1~6주 관련 문제풀이

Q9 정보보호를 위한 통제(대책)은 예방(Prevention)통제,
탐지(Detective)통제, 교정(Corrective)통제로 분류 할 수 있다.
다음 기술한 해당 통제별 사례로 적절하지 않은 것은?

1. 예방통제: 관리자 외에는 특정 시설이나 설비에 접근할 수 없게 하였다.
2. 예방통제: 비인가자가 정보통신망을 통해 자산에 접근하지 못하도록 하였다.
3. 탐지통제: 데이터 파일의 복구를 위해 트랜잭션 로그를 남기도록 하였다.
4. 탐지통제: 불법적인 접근 시도를 발견하기 위해 접근 위반 로그를 남기도록 하였다.

1~6주 관련 문제풀이

Q10 보기의 설명은 보안서비스 중 어느 항목을 나타내는 것인가?

> 수신된 데이터가 인증된 개체가 보낸 것과 정확히 일치하는지에 대한 확신을 주는 서비스

1. 데이터 기밀성
2. 데이터 무결성
3. 부인봉쇄
4. 가용성

1~6주 관련 문제풀이

Q11 다음 중 무결성(Integrity)에 대한 설명으로 틀린 것은?

1. 네트워크를 통하여 송신 · 수신되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질을 말한다.
2. 정보가 이미 변경되었거나 변경 위험이 있을 때에는 이러한 변경을 탐지하여 복구할 수 있는 침입 탐지, 백업 등의 기술이 필요하다.
3. 무결성을 보장하기 위한 보안 기술에는 접근 제어, 메시지 인증 등이 있다.
4. 정보는 지속적으로 변화하며, 이는 인가된 자가 접근할 수 있어야 함을 의미한다.

1~6주 관련 문제풀이

Q12 보기의 빈 칸 안에 들어갈 가장 적합한 보호보호 서비스는?

> 전자상거래 업체인 A사는 최근 홈페이지에서 전자결제서비스를 B사의 결제시스템 장애로 인하여 12시간 동안 고객들이 A사 홈페이지에서 결제를 하지 못해 물건을 구매할 수 없게 되었고, A사는 막대한 금전적 손실을 보게 되었다. A사는 B사에게 정보보호 기본요건인 ( ) 강화를 요청하고 손해에 대한 배상의 책임을 지도록 하였다.

1. 기밀성 서비스
2. 가용성 서비스
3. 무결성 서비스
4. 접근제어 서비스

1~6주 관련 문제풀이

Q13 다음 중 정보보호의 목표와 개념에 관한 설명으로 알맞지 않은 것은?

1. 정보보호는 정보처리영역에 있어서 가용성, 기밀성, 무결성을 보장하는 데 있다.
2. 가용성이란 승인 또는 허가받은 사람의 경우 언제든지 접근과 이용을 보장받는 것이다.
3. 기밀성이란 승인 또는 허가받지 아니한 사람이나 프로세스에 의한 데이터의 변경 또는 훼손을 방지하는 것이다.
4. 최근에는 정보보호영역에서 부인방지, 책임성, 진정성, 신뢰성의 중요성이 날로 커지고 있다.

1~6주 관련 문제풀이

Q14 보기의 설명에 대해 가장 적합한 것은?

> 정보보호 목적과 구성, 기본 방침, 정보보호 실행계획 수립,
> 보안에 대한 역할과 책임, 정보자산/정보시스템의 보안,
> 규정의 준수, 보안정책 운용 정보를 포함한 문서

1. 위험분석서
2. 정보보호정책서
3. 업무연속성계획서
4. 업무영향 평가서

1~6주 관련 문제풀이

Q15 정보보호 정책에 대한 설명으로 옳지 않은 것은?

1. 정보보호 정책의 의미, 유형, 수립과정, 포함될 내용을 이해하여야 한다.
2. 정보보호 정책은 어떤 조직의 기술과 정보자산에 접근하려는 사람이 따라야 하는 규칙의 형식적인 진술이다.
3. 정보보호 정책은 조직의 정보보호에 대한 방향과 전략 그리고 정보보호 프로그램의 근거를 제시하는 매우 중요한 문서이다.
4. 정보보호 정책은 특정 부서에서라도 참고하는 내용이 있어야 하며 구체적이고 명확하게 서술되어야 한다.

1~6주 관련 문제풀이

Q16 다음 정보보호 관리체계에 대한 설명 중 적절하지 못한 것은?

1. 정보보호 관리체계는 경영과 IT 영역의 중요한 위험관리 활동의 하나이다.
2. 정보보호 관리체계는 정보보호에 관한 경영관리 시스템이다.
3. 정보보호 관리체계는 기업에 있는 정보자산 보호를 목적으로 주로 기술적인 면을 고려하며, 일반적으로 정보보호 운용 또는 인적관리라는 관리대상에서 배제한다.
4. 정보보호 관리체계는 통상적으로 PDCA(Plan-Do-Check-Act)사이클을 기반으로 실행된다.

1~6주 관련 문제풀이

Q17 위험관리 절차를 순서대로 배열한 것은?

1. 자산식별
2. 정보보호계획 수립
3. 정보보호대책 수립
4. 위험 분석 및 평가
5. 주기적 재검토

❶ 1-2-3-4-5

❷ 1-4-3-2-5

❸ 1-2-4-3-5

❹ 1-4-2-3-5

1~6주 관련 문제풀이

Q18 다음 중 위험분석 전략의 장 · 단점에 대한 설명으로 옳지 않은 것은?

1. 기준선접근(Baseline Approach) 방법은 일반적으로 기본적이 보호대책을 확인하기 위해 어떤 중요한 자원도 필요하지 않다.
2. 상세위험분석(Detailed Analysis) 방법은 가시적인 결과를 얻기 위해 많은 시간, 노력, 전문성이 필요하다.
3. 복합접근(Combined Approach) 방법은 자원과 비용은 가장 큰 이익이 있는 곳에 사용될 수 있고, 높은 위험은 미리 다루어질 수 있다.
4. 비공식 접근(Informal Approach) 방법은 중요한 자원이 투입되기 전에 필요한 정보를 얻기 위한 간단한 고수준 접근을 사용하는 것으로 위험관리 프로그램에 더 적합하다.

1~6주 관련 문제풀이

Q19 위험분석 방법론은 보통 정량적 위험분석과 정성적 위험분석으로 분류되는데, 다음 중 정량적 위험분석 방법이 아닌 것은?

1. 연간예상손실 계산법
2. 과거 통계자료 분석법
3. 수학공식 접근법
4. 시나리오 기반 분석법

1~6주 관련 문제풀이

Q20 보기에서 설명하는 보안공격은 무엇인가?

> 암호화되어 전송되는 메시지를 도청하여 메시지의 내용을 파악하는 것이 불가능하더라도, 메시지의 송신자와 수신자의 신원에 대한 정보를 파악하거나 메시지 존재 자체에 대한 정보를 획득할 수 없다.

1. 삭제공격
2. 트래픽 분석
3. 메시지 변조
4. 재생 공격

1~6주 관련 문제풀이

Q21 보기의 빈 칸 안에 들어갈 알맞은 단어는?

( )(이)란 메시지의 생성, 전송, 수신, 이용, 저장 등의 일련의 과정에 관련되어 있는 송수신자, 전송자, 이용자, 관리자들이 제3자에게 자신이 적법한 사용자라는 것을 증명할 수 있도록 하는 기능

1. 암호화
2. 인증
3. 복호화
4. 프로토콜

1~6주 관련 문제풀이

Q22 다음 중 정보보호의 주요 목적이 아닌 것은?

1. 무결성
2. 부인방지
3. 기밀성
4. 정합성

1~6주 관련 문제풀이

Q23 다음 중 물리적 접근 통제 방법으로 옳지 않은 것은?

1. 네트워크 장비들의 물리적 위치 분리
2. 직원들의 보안구역 출입통제
3. 컴퓨터 도난 또는 파괴 방지
4. 정보보안 정책 및 절차

1~6주 관련 문제풀이

Q24 보기의 설명은 정보보호 관리 측면에서 무엇에 대한 정의인가?

> 비정상적인 일이 발생할 수 있는 가능성을 말함

1. 위협
2. 위험
3. 취약점
4. 통제

1~6주 관련 문제풀이

Q25 보기의 설명은 정보보호 대책의 통제 방법 중 어느 것에 해당되는가?

> 발생 가능한 모든 유형의 오류나 악의적 행위를 예측하고 이에 대한 예방책을 마련한다 하더라도 예방 통제로만 완전히 막을 수는 없다. 예방 통제를 우회하여 발생되는 문제점들을 찾아내기 위한 통제가 필요하다.

1. 대응 통제
2. 탐지 통제
3. 교정 통제
4. 잔류 위험

1~6주 관련 문제풀이

Q26 정보보호의 예방대책을 관리적 예방대책과 기술적 예방대책으로 나누어 볼 때 관리적 예방대책에 해당하는 것은?

1. 안전한 패스워드 사용을 강제
2. 침입차단시스템을 이용하여 접속을 통제
3. 문서처리 순서의 표준화
4. 가상 사설망을 이용하여 안전한 통신환경 구현

1~6주 관련 문제풀이

Q27 정보보호 내부 감사 시 고려해야 할 사항으로 가장 부적합한 것은?

1. 내부감사를 수행하는 구성원은 정보보호 전문가들로 제한한다.
2. 감사의 범위는 다양한 위험을 분석 및 검토할 수 있도록 가능한 포괄적이어야 한다.
3. 감사활동은 기업 내외부로부터 독립성을 유지할 수 있도록 해야 한다.
4. 내부감사는 조직의 위험을 파악하여 개선사항을 제시할 수 있다.

1~6주 관련 문제풀이

Q28 정보보호 조직은 정보보호 정책을 수립하는 데 있어 사용자, 관리자, 기술요원에 대한 책임영역을 명확히 정의할 필요가 있다.
다음 보기는 누구에 대한 책임을 설명한 것인가?

> 정보시스템에 저장된 데이터의 정확성과 무결성을 유지하고 데이터의 중요성 및 분류를 결정할 책임이 있다.

1. 정보시스템 정보보호 관리자
2. 데이터 관리자
3. 프로세스 관리자
4. 정보시스템 관리자

1~6주 관련 문제풀이

Q29 위험관리 과정에서 구현된 정보보호 대책의 적용 후에도 조직에 남아 있을 수 있는 잔류 위험도(또는 잔여 위험, Residual Risk)에 대한 설명 중 적절하지 않은 것은?

1. 위험관리는 위험평가를 통해 조직이 수용할 수 있는 수준을 유지하는 것이 목적이기 때문에 잔류위험이 존재할 수 있다.
2. 적절한 위험평가를 통한 보호대책의 적용 후에도 남아 있는 위험이 있을 수 있다.
3. 잔류 위험은 위험회피, 이전, 감소 그리고 수용 등으로 처리된다.
4. 위험평가 및 보호대책의 적용 후에도 잔류위험이 존재할 경우 이를 완전히 제거하기 위하여 상세위험분석을 수행하는 것이 일반적이다.

1~6주 관련 문제풀이

Q30 다음 중 정보보호 위험의 구성 요소가 아닌 것은?

1. 자산(Assets)
2. 위협(Threats)
3. 취약점(Vulnerability)
4. 정책(Policy)

1~6주 관련 문제풀이

Q31 위험관리 과정에는 다양한 위험분석 방법이 존재한다.
다음 보기에서 설명하는 위험분석 방법은 무엇인가?

> 자사의 가치를 측정하고 자산에 대한 위협의 정도와 취약점을 분석한다. 정보시스템의 업무 중요도가 높거나 자산 가치가 높은 경우에 적용된다.

1. 기준선 접근법
2. 전문가 판단법
3. 상세위험 접근법
4. 복합적 접근법

1~6주 관련 문제풀이

Q32 정량적 위험분석과 정성적 위험분석에 대한 설명 중 틀린 것은?

1. 정량적 분석은 객관적인 평가기준이 적용된다.
2. 정량적 분석은 위험관리 성능평가가 용이하다.
3. 정성적 분석은 계산에 대한 노력이 적게 소요된다.
4. 정성적 분석은 비용과 이익에 대한 평가가 필수적으로 요구된다.

1~6주 관련 문제풀이

Q33 위험분석의 방법론 및 관련 사항에 대해 알맞게 설명한 것은?

1. 복합적 접근법: 기준선 접근법, 상세(세부족)위험 접근법, 전문가 판단법을 병행 활용
2. 정성적 위험분석: 델파이법, 시나리오법, 순위결정법, 연간예상손실(ALE)
3. 정량적 위험분석: 수학공식 접근법, 확률 분포 추정법, 과거자료 분석(접근)법
4. 전문가 판단법(Informal Approach): 큰 조직에 적합

1~6주 관련 문제풀이

Q34 다음 중 위험분석 시 정량적 분석의 단점으로 올바른 것은?

1. 객관적인 평가 기준이 적용된다.
2. 위험관리 성능 평가가 용이하다.
3. 위험관리 성능을 추적할 수 없다.
4. 계산이 복잡하여 분석하는 데 시간, 노력, 비용이 많이 든다.

1~6주 관련 문제풀이

Q35 다음 중 보기에 해당하는 위험분석 방법론으로 가장 적합한 것은?

- 위험의 발생빈도를 계산하는 식을 이용하여 위험을 계량하는 방법
- 과거자료의 획득이 어려울 경우 위험 발생 빈도를 추정 · 분석하는 것에 유용
- 위험을 정량화하여 매우 간결하게 나타낼 수 있음
- 기대손실을 추정하는 자료의 양이 적음

1. ALE(연간예상손실) 분석법
2. 과거자료 분석법
3. 수학공식 접근법
4. 확률 분포법

1~6주 관련 문제풀이

Q36 위험관리 개념에서 위험 완화 방법에 대한 설명으로 옳지 않은 것은?

1. 회피(Avoidance)는 특정 위험으로부터의 손실 부담 또는 위험 획득을 수용하는 것이다.
2. 이전(Transfer)은 잠재적 비용을 제3자에게 이전하거나 할당하는 것이다.
3. 감소(Reduction)는 위험을 감소시킬 수 있는 대책을 채택하여 구현하는 것이다.
4. 수용(Acceptance)는 위험을 받아들이고 비용을 감수하는 것이다.

1~6주 관련 문제풀이

Q37 보기에서 (가)~(라)에 들어가야 할 내용으로 올바르게 나열된 것은?

> 정보보호관리를 이행하기 위해서 조직은 (가) 및 조직수립,
> 범위설정 및 (나), (다), 구현, 사후관리활동으로 구성된 5단계의
> 논리적이고 체계적인 정보보호관리 (라)를 수립하고,
> 기획 · 관리하여야 한다.

1. (가) 프레임워크, (나) 정보자산 식별, (다) 위험관리,
   (라) 정보보호 정책
2. (가) 정보보호정책, (나) 취약점, (다) 정보자산 식별,
   (라) 프레임워크
3. (가) 프레임워크, (나) 취약점, (다) 정보자산 식별,
   (라) 정보보호 정책
4. (가) 정보보호정책, (나) 정보자산 식별, (다) 위험관리,
   (라) 프레임워크

1~6주 관련 문제풀이

Q38 정보보호정책 수립 시 정보보호 목표를 선정함에 있어 고려해야 할 사항으로 적절하지 않은 것은?

1. 사용자에게 제공하는 서비스의 이점이 위험의 위중보다 크다면 정보보호 관리자는 사용자들이 위험으로부터 서비스를 안전하게 사용할 수 있도록 보호대책을 수립해야 한다.
2. 누구나 쉽게 시스템에 접근하여 사용할 수 있다면 사용하기에 편리할 수 있도록 해야 한다. 다만 각종 위협으로부터 완전히 노출되어 있어서 정보보호관리자는 시스템의 안전성을 고려하는 것보다는 시스템의 사용의 용이성을 최우선 과제로 선정해야 한다.
3. 정보보호를 하기 위해서는 비용이 많이 소요되므로 프라이버시 침해에 따른 손실, 서비스 침해에 따른 손실 등을 고려하여 신중하게 결정해야 한다.
4. 정보보호정책의 적용 영역은 정보기술, 저장된 정보, 기술에 의해 조직된 정보의 모든 형태를 포함한다.

1~6주 관련 문제풀이

Q39 조직이 수행하는 모든 정보보호 활동의 근거가 되는 최상위 수준의 정보보호 정책 수립 시, 포함해야 할 사항과 가장 거리가 먼 것은?

1. 조직의 정보보호 활동을 실행하기 위한 절차, 주기, 수행 주제 등에 관한 사항
2. 조직의 정보보호에 대한 최고경영자 등 경영진의 의지 및 방향
3. 조직의 정보보호를 위한 역할과 책임, 대상과 범위에 관한 사항
4. 조직이 수행하는 관리적, 기술적, 물리적 정보보호 활동의 근거

1~6주 관련 문제풀이

Q40 문장의 정보보호대책 선정 시 영향을 주는 제약사항으로 옳은 것은?

> 많은 기술적 대책들이 직원의 능동적인 지원에 의존하기 때문에 이러한 제약사항을 고려하여야 한다. 만약 직원이 대책에 대한 필요성을 이해하지 못하고 문화적으로 수용할 만하다는 것을 알지 못한다면 대책은 시간이 지날수록 비효율적인 것이 된다.

1. 환경적 제약
2. 법적 제약
3. 시간적 제약
4. 사회적 제약

1~6주 관련 문제풀이

Q41 정보보호관리체계 구축 시 발생가능한 문제점과 해결방안에 대한 설명으로 틀린 것은?

1. 관련 부서와의 조정이 곤란하다.
2. 직원들이 일상 업무에 바빠 관리체계 구축작업에 시간을 내기 어렵다.
3. 직원들은 자신의 책임을 피하기 위해 문제점이 발생하면 즉시 상사에게 보고하는 경향을 보인다.
4. 관리체계 구축에는 경영자의 리더십이 필수적으로 요구된다.

1~6주 관련 문제풀이

Q42 다음 중 정보보호 교육 및 훈련에 대한 설명으로 적절하지 않은 것은?

1. 위험분석을 통해 구현된 정보보호 대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육한다.
2. 정책, 지침 및 절차 등이 개정된 사항에 대해서는 모두 모이기 어렵기 때문에 집합 또는 온라인 교육보다 게시판 등을 통해서 알리는 것이 보다 효과적이다.
3. 타사의 침해사고 사례, 최근 발생한 보안위험 등에 대한 최근 동향을 지속적으로 교육함으로써 보안인식 제고를 위해 노력한다.
4. 출장, 휴가 등의 사정으로 정기 정보보호 교육을 받지 못한 인력에 대해서 전달교육, 추가교육, 온라인 교육 등의 방법으로 정보보호 교육을 수행한다.

1~6주 관련 문제풀이

Q43 보기에서 (가)~(다)에 들어갈 용어를 순서대로 나열한 것은?

> 조직은 (가)의 과정을 통해 보호를 받을 가치가 있는 자산에 대해 정보 자산의 형태, 소유자, 관리자, 특성 등을 포함한 (나)를(을) 만들고, 자산의 (다)를 산출하며, 정보자산과 업무처리와의 관계를 알아낼 수 있다.

1. (가) 자산가치 산정, (나) 목록, (다) 가치
2. (가) 자산가치 산정, (나) 분류, (다) 가치
3. (가) 정보자산의 식별, (나) 목록, (다) 가치와 중요도
4. (가) 정보자산의 식별, (나) 분류, (다) 가치와 중요도

1~6주 관련 문제풀이

Q44 다음 중 정량적 위험분석의 장점이 아닌 것은?

1. 위험평가 결과가 금전적 가치, 백분율, 확률 등으로 표현되어 이해가 쉽다.
2. 위험관리 성능평가가 용이하다.
3. 정보자산의 가치가 논리적으로 평가되고 화폐로 표현되어 이해가 쉽다.
4. 위험분석 작업을 위한 시간과 비용이 절약된다.

1~6주 관련 문제풀이

Q45 보기는 어떤 기업에서 식별한 위험을 설명한 것이다. 이러한 위험에 대해 기업이 취할 위험 처리 전략(방법)으로 가장 부적절한 것은?

> 해당 조직은 위험을 수용 가능한 수준으로 감소시키기 위해 정보보호 대책을 선정하고 그 보호대책의 구현 우선순위, 일정, 담당부서 및 담당자 지정, 예산 등을 포함한 이행 계획을 수립하여 경영진의 승인을 받았다.
>
> 그런데 이러한 위험관리 과정에서 식별된 위험 중에서 식별된 법률 위반사항에 대해 해당 조직 자체적으로 해결하지 못할 경우, 매년 1천만 원의 과태료가 지속적으로 부과될 수 있다.
> (단, 대책비용은 매년1천만 원을 초과하지 않음)

❶ 위험수용 ❷ 위험회피 ❸ 위험감소 ❹ 위험전가