제8장 정보보호관리

1. 위험관리(risk management)

위험관리는 변화하는 환경에 맞게 지속적으로 **"자산의 취약점과 위험을 분석하고, 위험으로부터 자산을 보호하기 위한 효과적인 보안 대책"**을 마련하는 것이다.

- 위험관리는 위험을 일정 수준 이하로 줄이기 위한 전체적인 절차이다.
- 위험관리는 위험정도를 수용 가능한 수준으로 줄이는 것이 주목적이다.
- 위험을 100% 제거하는 것은 어렵다.

위험관리 과정은 연구자마다 다양하다.
위험관리 과정은 비슷하면서 다양하므로, 주어진 문제를 잘 읽고 답을 찾아야 한다.
본 교재에서는 3가지를 소개한다.

[예제 1] 위험관리 과정

자산분석 – 자산식별 및 평가, 가장 중요한 단계이다.
↓
위협분석 – 자산들이 어떤 위협요소가 있는지를 분석(시스템 결함, 자연재해 등)
↓
취약성분석 – 위협이 이용할 수 있는 취약성 분석
↓
위험평가 – 자산에 대한 손실 평가(정량적, 정성적 방법론)
↓
대책 분석 – 평가한 것을 토대로 대책 선정(비용계산이 필요)
↓
비용효과 분석 – 위험을 줄이기 위한 결과를 정량적, 정성적으로 표현

[예제 2] 위험관리 과정 6단계

전산7급 소프트웨어공학에서 출제되는 유형

위험측정	**위험식별**	• 위험 요인을 식별하고 문서화 • 방법 : 델파이기법, 체크리스트 등
	위험분석	• 식별된 위험의 영향력과 발생 확률 등을 분석한다. • 정성적 위험분석 : 위험영향도, 위험발생가능성 등 • 정량적 위험분석 : 민감도 분석, 의사결정분석 등
	위험우선순위	• 분석된 위험의 정도에 따라 우선순위를 부여한다. • 위험의 정도에 따라 관리할 위험을 선정하기 위하여
위험통제	**위험관리계획**	• 위험우선순위에 따라 각각에 맞는 위험관리계획을 수립한다.
	위험해결	• 실제로 위험이 발생한 경우이다. • 위험관리계획에 따라 문제를 해결한다.
	위험감소	• 정해진 해결책에 따라 모니터링을 통하여 위험을 감소시킨다. • 위험 모니터링이라고도 한다.

[예제 3] 위험관리 5단계

– "한국인터넷진흥원(KISA) 자료" 참고

위험관리 전략 및 계획 수립 ~ 위험관리 전략과 계획을 수립하는 단계

↓

위험분석 ~ 위험을 구성하는 요소들을 분석하는 단계

↓

위험평가 ~ 위험분석에 기초하여 위험을 평가하는 단계

↓

정보보호 대책수립 ~ 필요한 정보보호대책을 선정하는 단계

↓

정보보호 계획수립 ~ 정보보호대책을 구현할 계획을 수립하는 단계

• 위험분석 : 조직의 자산에 대한 위험을 식별하는 단계
• 위험평가 : 조직의 자산에 대한 위험의 규모를 결정하는 단계
• 정보보호계획 수립(위험완화) : 새롭게 필요한 대응책을 식별하는 단계

//-------------------------

용어 정리

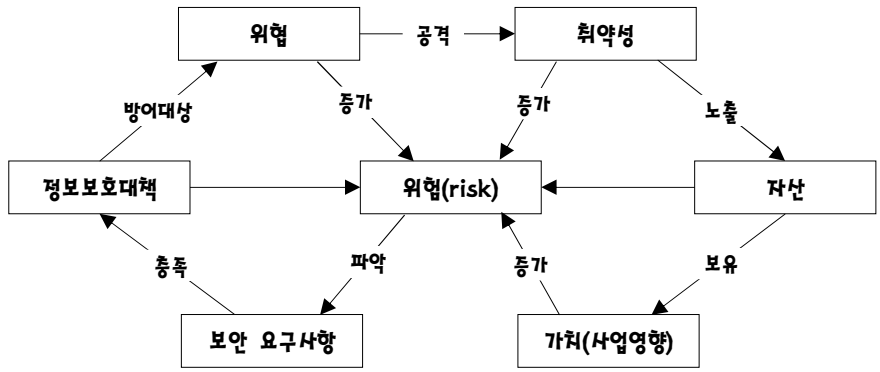
① 위험(risk) – 금액으로 표현 가능

- 위험은 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 **가능성**이다.
- 위험은 발생 가능성이 있다는 것이지, 실제로 발생한 것은 아니다.
- 위험의 유형과 규모를 확인하기 위해서는 위험분석이 필요하다.
- 위험분석은 자산, 위협, 취약성 등을 분석하여 위험의 종류와 규모를 결정하는 것

- 위험은 "**자산, 위협, 취약성**"의 함수로서 정의된다.

위험 = F(자산, 위협, 취약성)
↓하나의 예
위험 = 위협×취약성×자산가치 → 곱한 이유 : 자산, 위협, 취약성이 클수록 위험이 커지므로

◈ 위험 구성요소들 간의 관계



- 위협은 취약성을 공격하고, 취약성은 자산을 노출시킨다.
- 자산은 가치를 보유하고,
- "위협, 취약성, 자산 가치"는 모두 위험을 증가시킨다.
- 위험을 파악함으로써 보안 요구사항을 파악할 수 있고,
- 보안 요구사항을 충족시키는 정보보호대책을 선정. 구현함으로 위협을 방어할 수 있다.
- 정보보호대책은 위협을 방어함으로써 위험을 감소시킨다.

② 자산(asset)
- 자산은 경제적 가치가 있는 유형 · 무형의 재산이다.(조직이 보호해야 할 대상)
- 자산의 우선순위를 정하기 위해서 평가 과정을 거친다.
- 평가 기준으로 보통 기밀성, 무결성, 가용성이 사용된다.
- 자산 : 정보, 문서(서류), 하드웨어, 소프트웨어, 시설, 인력, 기업 이미지 등

③ 위협(threat)
- 위협은 자산에 손실을 입힐 수 있는 원치 않는 사건의 **잠재적인 원인** 또는 **행위자**(agent)
- 위협은 자산의 기밀성, 무결성, 가용성을 위태롭게 할 수 있는 상황이다.
- 위협은 자산의 손상 및 손실을 일으킬 수 있는 외부의 원인 또는 이벤트(사건)
- 자연적 위협 요소 : 자연적 재앙, 에러, 정보관리 부실, 시스템 장애 등
- 고의적 위협 요소 : 해킹, 위조, 서비스 거부, 부인(repudiation), IP spoofing 등

④ 취약성(vulnerability)
- 취약점은 자산의 잠재적 속성으로서 **위협이 이용하는 대상**이 되는 것이다.
- 경우에 따라서, 취약점은 "정보보호대책의 미비"로 정의되기도 한다.
- 취약점은 위협에 대해 자산의 손실이 발생될 수 있는 약점이다,
- 취약점이 있어도 위협이 없으면 손실은 발생되지 않는다.
- 위협이 있어도 자산에 취약성이 없으면, 위협이 발생해도 손실은 발생되지 않는다.

⑤ 위험분석(risk analysis)
- 자산, 위협, 취약성, 기존의 보호대책 등을 분석하여 위험의 종류와 규모를 결정하는 것
- 위험분석 각 자산의 취약점을 분석하고, 위협으로부터 발생 가능한 위험 정도를 결정한다.
- 정보시스템의 취약성으로 인한 예상손실을 분석하는 것이다.

⑥ 위험평가(risk assessment)
- 위험분석 결과를 토대로 위험을 수용 가능한 위험수준과 대비하여 위험의 대응 여부와 우선순위를 결정하는 것이다.
- 각 자산에 대한 위험의 종류와 그 영향을 평가한다.
- 취약점을 분석하여 위협이 주는 위험의 정도를 평가하는 것이다.

⑦ 위험수용
- 위험에 대한 조치를 취하지 않고, 현 상태의 위험을 허용하기로 결정하는 것이다.
- 위험 처리 비용이 과도하면, 일정 수준의 위험은 그냥 받아들이는 것이다.
- 위험이 조직에 발생시키는 결과에 대한 책임을 관리층이 지는 방식이다.

⑧ 위험회피

• 위험이 존재하는 프로세스나 사업을 포기하는 것이다.

⑨ 위험전가

• 잠재적 위험 비용을 제3자에게 이전하거나 할당하는 것이다.
• 위험에 대한 보험을 들거나 다른 기관과의 계약을 통하여 잠재적 손실을 제3자에게 이전하거나 할당하는 방식이다.

⑩ 위험감소

• 위험을 감소시킬 수 있는 효과적인 대책을 채택하여 구현하는 것이다.

⑪ 정보보호대책

• 정보보호관리체계를 수립, 운영하기 위하여 선택한 통제사항이다.
• 정보보호대책은 위협에 대응하여 자산을 보호하기 위한 관리적, 물리적, 기술적 대책이다.
• 대책에는 방화벽, 침입탐지시스템 등의 제품뿐만 아니라 절차, 정책, 교육 등의 모든 통제들이 포함된다.

예제

다음과 같을 때, 위험을 줄임으로써 발생되는 이익은?

• 통제가 없을 때 발생되는 위험 : 5억원 • 통제가 있을 때 발생되는 위험 : 2억원 • 통제 수립 및 유지비 : 1억원

[풀이] 위험을 줄임으로써 발생되는 이익은 다음과 같다.

통제가 없을 때 발생되는 위험을 A
통제가 있을 때 발생되는 위험을 B
통제 수립 및 유지비를 C라 하면

이익 = A - B - C = 5억원 - 2억원 - 1억원 = 2억원

기출문제 분석

1. 위협(threats), 취약성(vulnerability), 자산가치(assetvalue), 위험(risk)의 상관관계 표현으로 가장 옳은 것은? [2018년 서울 7급]

① 위험=자산가치/위협×취약성　② 위험=위협/취약성×자산가치
③ 위험=위협×취약성/자산가치　④ 위험=위협×취약성×자산가치

♤ **위험(risk)**

• 위험은 **"자산, 위협, 취약성"**의 함수로서 정의된다.

위험 = F(자산, 위협, 취약성)
↓하나의 예
위험 = 위협×취약성×자산가치

정답 : ④

2. 보안 요소에 대한 설명과 용어가 바르게 짝지어진 것은? [2016년 국가 9급]

ㄱ. 자산의 손실을 초래할 수 있는 원하지 않는 사건의 잠재적인 원인이나 행위자
ㄴ. 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성
ㄷ. 자산의 잠재적인 속성으로서 위협의 이용 대상이 되는 것

	ㄱ	ㄴ	ㄷ
①	위협	취약점	위험
②	위협	위험	취약점
③	취약점	위협	위험
④	위험	위협	취약점

♤ **위협/위험/취약점**

• 위협은 자산에 손실을 입힐 수 있는 원치 않는 사건의 잠재적인 원인 또는 행위자(agent)
• 위험은 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성이다.
• 취약점은 자산의 잠재적 속성으로서 위협이 이용하는 대상이 되는 것이다.

정답 : ②

3. 조직의 정보자산을 보호하기 위하여 정보자산에 대한 위협과 취약성을 분석하여 비용 대비 적절한 보호 대책을 마련함으로써 위험을 감수할 수 있는 수준으로 유지하는 일련의 과정은? [2017 경기 추가 9급]

① 업무 연속성 계획
② 위험관리
③ 정책과 절차
④ 탐지 및 복구 통제

♤ **위험관리**

• 위험관리는 위험을 일정 수준 이하로 줄이기 위한 전체적인 절차이다.
• 위험관리는 위험정도를 수용 가능한 수준으로 줄이는 것이 주목적이다.
• 위험을 100% 제거하는 것은 어렵다.

정답 : ②

4. ㉠, ㉡에 들어갈 정보보안 위험의 처리 방식을 바르게 연결한 것은? [2018년 국가 7급]

(㉠)은(는) 사업 목적상 위험을 처리하는 데 들어가는 과도한 비용 또는 시간 때문에 일정 수준의 위험을 받아 들이는 것으로, 그 위험이 조직에 발생시키는 결과에 대한 책임을 관리층이 지는 방식이다.
(㉡)은(는) 위험에 대한 책임을 제3자와 공유하는 것으로, 보험을 들거나 다른 기관과의 계약을 통하여 잠재적 손실을 제3자에게 이전하거나 할당하는 방식이다.

	㉠	㉡
①	위험회피	위험전가
②	위험회피	위험감소
③	위험수용	위험전가
④	위험수용	위험감소

♤ **위험 처리 방식**

• 위험수용은 위험 처리 비용이 과도하면, 일정 수준의 위험은 그냥 받아들이는 것이다.
• 위험전가는 잠재적 위험 비용을 제3자에게 이전하거나 할당하는 것이다.

정답 : ③

5. 위험관리 과정에 대한 설명으로 ㉠, ㉡에 들어갈 용어로 옳은 것은? [2017년 지방 9급]

(가)	(㉠)단계는 조직의 업무와 연관된 정보, 정보시스템을 포함한 정보자산을 식별하고, 해당 자산의 보안성이 상실되었을 때의 결과가 조직에 미칠 수 있는 영향을 고려하여 가치를 평가한다.
(나)	(㉡)단계는 식별된 자산, 위협 및 취약점을 기준으로 위험도를 산출하여 기존의 보호대책을 파악하고, 자산별 위협, 취약점 및 위험도를 정리하여 위험을 평가한다.

	㉠	㉡
①	자산식별 및 평가	위험 평가
②	자산식별 및 평가	취약점 분석 및 평가
③	위험 평가	가치평가 및 분석
④	가치평가 및 분석	취약점 분석 및 평가

♤ **위험관리 과정 - 교재마다 표현 차이가 많음**

- 위험관리는 변화하는 환경에 맞게 지속적으로 "자산의 취약점과 위험을 분석하고,
- 위험으로부터 자산을 보호하기 위한 효과적인 보안 대책"을 마련하는 것이다.

◉ **위험관리 과정 - 6단계 예**

자산분석 – 자산식별 및 평가, 가장 중요한 단계이다.

↓

위협분석 – 자산들이 어떤 위협요소가 있는지를 분석(시스템 결함, 자연재해 등)

↓

취약성분석 – 위협이 이용할 수 있는 취약성 분석

↓

위험평가 – 자산에 대한 손실 평가(정량적, 정성적 방법론)

↓

대책 분석 – 평가한 것을 토대로 대책 선정(비용계산이 필요)

↓

비용효과 분석 – 위험을 줄이기 위한 결과를 정량적, 정성적으로 표현

- 위험관리 과정은 비슷하면서 다양하므로, 주어진 문제를 잘 읽고 답을 찾아야 한다.

정답 : ①

6. 정보보호 위험관리에 대한 설명으로 옳지 않은 것은? [2020년 국가 9급]

① 자산은 조직이 보호해야 할 대상으로 정보, 하드웨어, 소프트웨어, 시설 등이 해당한다.
② 위험은 자산에 손실이 발생할 가능성과 관련되어 있으나 이로 인한 부정적인 영향을 미칠 가능성과는 무관하다.
③ 취약점은 자산이 잠재적으로 가진 약점을 의미한다.
④ 정보보호대책은 위협에 대응하여 자산을 보호하기 위한 관리적, 기술적, 물리적 대책을 의미한다.

♤ **정보보호 위험관리**

• 위험은 자산에 손실이 발생할 가능성과 관련되어 있으나 이로 인한 **부정적인 영향을 미칠 가능성과는 무관**하다.(×) → 위험은 원하지 않는 사건이 발생하여 **부정적인 영향을 미칠 가능성**이다.

// 위험(risk) – 금액으로 표현 가능

• 위험은 발생 가능성이 있다는 것이지, 실제로 발생한 것은 아니다.
• 위험분석은 자산, 위협, 취약성 등을 분석하여 위험의 종류와 규모를 결정하는 것

정답 : ②

7. 위험분석 및 평가를 통해 도출된 위험에 대해 적절한 처리를 하고자 할 때, 접근 방법으로 옳지 않은 것은? [2022년 국회 9급]

① 위험수용 ② 위험감소 ③ 위험회피
④ 위험전가 ⑤ 위험검사

♤ **위험분석 및 평가**

// 위험(risk) – 금액으로 표현 가능

• 위험은 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 **가능성**이다.
• 위험은 발생 가능성이 있다는 것이지, 실제로 발생한 것은 아니다.
• 해서, **위험**을 **검사**하는 것은 **불가능**하다.(위험은 원하지 않는 사건이 발생이므로)

① **위험수용** : 위험에 대한 조치를 취하지 않고, 현 상태의 위험을 허용하기로 결정하는 것이다.
② **위험감소** : 위험을 감소시킬 수 있는 효과적인 대책을 채택하여 구현하는 것이다.
③ **위험회피** : 위험이 존재하는 프로세스나 사업을 포기하는 것이다.
④ **위험전가** : 잠재적 위험 비용을 제3자에게 이전하거나 할당하는 것이다.(보험 가입)

정답 : ⑤