5. 정보보안관리 및 법규

2. 위험관리

위험관리 개념,절차,요소,위험분석 접근기법,방법 등에 대해 학습합니다.

✓ 위험관리

- 조직이 정보자산에 대한 위험을 수용할 수 있는 수준으로 유지하기 위해 정보자산에 대한 위험을 분석하고 이에 대한 비용 대비 효과적인 보호 대책을 마련하는 일련의 과정

위험

- 위험 – 비정상적 결과가 일어날 확률로서 주어진 위협에 의해 자산의 취약점이 악용되어 결국 자산에 손실을 끼칠 가능성을 의미 ➔ 위협 * 취약점 * 자산= 전체위험(total risk)
- 잔여위험(Residual risk) – 기업이 위험에 대비하여 시스템이나 환경을 개선하여도 남겨진 위험은 존재함.

→(위협*취약점*자산)* 통제격차=잔여위험

위험관리 과정

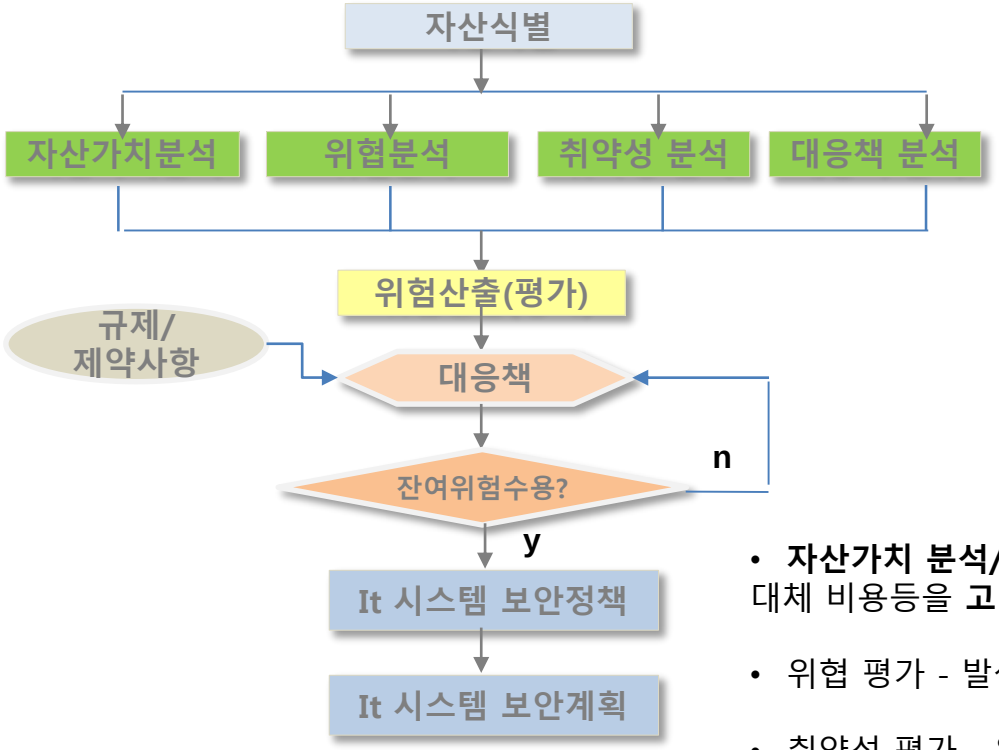
위험의 처리방법

- 위험수용(Risk Acceptance) : 현재 위험을 받아들이고, 해당 위험의 잠재적 손실 비용을 감수 즉, 위험을 완전히 제거할 수는 없으므로, 일정 수준 이하의 위험은 어쩔 수 없는 것으로 인정하고 사업 진행.
- 위험감소(Risk Mitigation) : 위험을 감소시킬 수 있는 대책을 채택하여 구현하는 것으로 대책 채택 시 이에 따른 비용이 발생. 이 비용과 감소되는 위험의 크기를 비교하는 비용효과 분석 실시.
- 위험회피(Risk Avoidance) : 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기
- 위험전가(Risk Transfer) : 보험이나 외주 등으로 잠재적 비용을 제3자에게 이전하거나 할당

✓ 위험분석

개요 및 목적

- 조직과 정보자산의 위험을 측정하고 측정된 위험의 허용여부를 판단 근거를 제공하며, 이를 통해 비용 효과적 대응책 수립 보호되어야 할.
- 기업에게 위험의 우선순위 정하는 것을 도와주고, 이러한 위험에 대한 보호를 적용함에 있어 소요되는 비용을 이치에 맞는 방식으로 제시



- **자산가치 분석/평가** - 획득 및 개발 비용, 관리 비용, 지적 재산권 가치, 대체 비용등을 **고려하여 평가 /평가이유**- 보안 대책에 대한 비용/효과 분석
- 위협 평가 - 발생가능한 위협을 식별하고, 각 위협의 발생가능성을 예측
- 취약성 평가 - 위협의 이용 대상으로 실제 자산에 끼치게 될 손실을 평가

1. 위험 분석 접근법

기준 접근법(Baseline Approach)

- 기준 문서, 실무 규약, 업계 최신 실무를 이용하여 시스템에 대한 가장 기본적이고 일반적인 수준에서의 보안 통제 사항들을 구현하는 것을 목표로 함.
- 모든 시스템에 대해 표준화된 보호대책을 체크리스트 형태로 제공
- 소규모조직이나, 대규모조직의 중요치 않은 일반 자산에 대하여 사용하는 접근법
- 장점 – 정형화된 위험평가를 수행하는데 있어서 추가로 자원이 요구되지 않으며, 다른 시스템에도 똑같은 평가가 쓰일 수 있다
- 단점 - 조직의 위험 노출에 있어서 조직의 특성이나 시스템의 사용용도 등에 대해 고려하지 않음.

비정형화된 접근법(Informal Approach)

- 구조적인 방법론에 기반하지 않고, 전문가의 지식과 경험에 따라 위험을 분석
- 소규모에서 중급 규모의 조직에서 효과적
- 장점 – 분석을 행하는 개인들에게 추가적 기술이 요구되지 않으므로, 비교적 신속하고 저비용으로 수행될 수 있다
- 단점 – 정형화된 프로세스가 사용되지 않으므로, 특정 위험요소가 고려되지 않아 조직을 위험으로부터 잠재적으로 취약하게 할 수 있다. / 결과가 분석을 수행하는 사람들의 견해 및 편견에 따라 왜곡될 수 있다.

상세한 위험 분석(Detailed risk analysis)

- 정형화되고 구조화된 프로세스를 사용하여 조직의 it 시스템에 대해 상세한 위험을 분석
- 자산분석 → 자산에 대한 위협 → 취약성평가 → 위험이 일어날 가능성 및 조직에 미칠 결과 → 잔여 위험 평가등 여러 단계를 거침
- 장점 – IT 시스템이 계속 발전하고 변화함에 따라 이러한 시스템을 연속적으로 관리하는 데 필요한 가장 좋은 정보를 제공
- 단점 – 많은 시간과 노력이 필요하고, 분석에 있어서 전문인력이 필요. 분석에 따라 적절한 수준의 보안을 제공하는데 지연이 발생할 수 도 있다.

통합된 접근법(Combined Approach)

- 고위험(high risk) 영역을 식별하여 상세 위험분석을 수행하고, 그 외 다른 영역은 베이스라인 접근법만을 사용하는 방식
- 장점 – 비용과 자원을 효율적으로 사용할 수 있음, 고위험 영역을 빠르게 식별하고 적절하게 처리할 수 있다.

2. 위험분석 방법론

정성적 위험 분석(Qualitative Risk Analysis)

- 위험의 구성 요소와 손실에 대하여 정확한 숫자나 화폐적 가치를 부여하지 않고, 위험 가능성의 시나리오에 자산의 중요성, 위협 및 취약성의 심각성을 등급 또는 순위에 의해 상대적으로 비교하는 방법.
- 특징
  - 진단 및 결과가 주관적
  - 비용/효과 분석시 기회비용을 일반적으로 고려하지 않음

*** 위험, 자산가치, 취약성 5점 척도 이용(낮음-1,약간낮음-2,보통-3 , 높음-4 , 매우높음-5)**
위험 –고위험 100

자산	위험	자산가치	취약성	위험	위험우선순위
A	1	3	2	45	3
B	3	4	4	80	2
C	4	5	4	90	1

<정성적 위험분석 예>

정성적 위험 분석(Qualitative Risk Analysis) 종류

- 델파이법 : 전문가 집단을 구성하고 위험을 분석 및 평가하여 설문조사를 실시해 의견을 정리하는 분석 방법. 시간과 비용을 절약할 수 있으나 전문가의 지식과 토론만으로 위협요소를 추정하기 때문에 정확도 낮음.

- 시나리오법 : 어떤 사실도 기대대로 발생되지 않는다는 사실에 근거하여 일정조건하에서 위협에 대한 발생가능한 결과들을 추정하는 방법. 적은 정보만으로도 전반적 가능성을 추론할 수 있고 위험분석 팀과 관리팀간의 원활한 의사소통도 가능. 정확성/완성도/이용기술수준이 낮음

- 순위결정법 : 비교우위 순위 결정표에 위험 항목의 서술적 순위를 결정하는 방법. 각각의 위협을 상호 비교하여 최종 위협 요인의 우선순위를 도출하는 방법. 위험분석에 소요되는 시간,자원이 적게 듦, 정확도는 낮음.

정량적 위험 분석(Quantiative Risk Analysis)

- 위험 구성 요소에 실제 의미가 있는 숫자 혹은 금액을 명시하여 위험의 크기를 금전적 가치로 산정하는 것이 가능하게 하는 방법.
- 특징
  - 정량적 위험평가 통해 위험비용이 보안대책의 비용을 초과하는지 분석하는 것으로 많은 시간과 경험 많은 인력을 필요로 함.
  - 복잡한 계산으로 인해 관리자들은 결과값이 어떤 방법으로 도출되었는지 알 수 없음
  - 자동화 도구에 의존(작업량이 많은 관계로)
  - 환경에 대한 자세한 정보수집이 필요

정량적 위험 평가 수행단계

자산에 가치 부여	자산가치 결정(Asset Value)
각각의 위협에 대한 잠재적 손실 계산	노출(Exposure Factor)계수(%) 계산 SLE(Singl Loss Expectancy)계산 ➔ SLE = AV x EF
위협 분석 수행	ARO(Annualized Rate of Occurance) 계산
개별 위협들마다 전체 손실 예상액 도출	ALE(Annualized Loss Expectancy) 계산 ➔ ALE = SLE x ARO

정량적 위험 분석(Quantiative Risk Analysis) 종류

- 과거자료 분석법 – 미래 사건의 발생 가능성을 예측하는 방법으로 과거의 자료를 통해 위험발생 가능성을 예측.
- 수학공식 접근법 – 위협의 발생 빈도를 계산하는 식을 이용하여 위험을 계량하는 방법으로 과거 자료 획득이 어려울 경우 위협 발생 빈도를 추정하는데 유리
- 확률 분포법 - 확률적 편차를 이용하여 최저, 보통, 최고의 위험 평가를 예측할 수 있다.
- 점수법 – 위험 발생 요인에 가중치를 두어 위험을 추정하는 방법으로 소요되는 시간이 적고 분석해야 할 자원의 양이 적다는 장점.

정성적, 정량적 위험 분석 비교

특 징	정성적	정량적
복잡한 계산	X	O
Cost/Benefit 분석	X	O
추측 작업 요구	O	X
자동화 지원 (Tool)	X	O
대량의 정보와 관계됨	X	O
객관적 Metrics	X	O
주관적 의견 사용	O	X
상당한 시간과 노력을 요구	X	O

잠깐!!

체크포인트문제1

1. 다음 중 위험관리 계획의 과정에 대한 설명으로 옳지 않은 것은?

가. 일반적으로 효과적인 보안에는 자산에 대한 보안 계층이 단일화 되어 있는 하나의 단일화 된 대책의 조합이 요구된다.

나. 위험관리는 크게 위험분석, 위험평가, 대책설정 3가지의 과정으로 구분된다.

다. 위험분석은 모든 시스템에 대한 간단한 초기분석을 통해 불필요한 시간과 자원의 투자없이 실행할 수 있다.

라. 위험평가의 목적은 적절하고 정당한 보안 대책을 선정하고 식별하기 위하여 시스템 및 그 자산이 노출된 위험을 평가하고 식별하기 위한 것이다.

2. 다음 지문은 위험 관리와 위험 분석에 대한 설명이다. 괄호 안에 들어갈 단어는?

위험관리는 위험분석과 위험평가가 주된 활동이다. 위험관리는 보호대상, 위험요소,(a)등을 통한 위험 분석, 적절한 메커니즘의 선택, 선택된 메커니즘의 구현과 시험, 구현된 메커니즘의 보안성 평가, 종합적인 보안의 재평가를 포함한다. 위험평가는 분석 결과를 기초로 현황을 평가하고 적절한 방법을 선택하여 효과적으로 위협 수준을 낮추기 위한 과정으로 적절한 (b)을 결정하는 단계이다.

가. A- 취약성 분석, B- 보안대책

나. A- 위기대응능력, B- 보호관리대책

다. A- 위기대응능력, B- 관리대책

라. A- 취약성 분석, B- 위기대응능력

3. 다음 중 위험관리의 순서로 가장 적절한 것은?

ㄱ. 위험분석
ㄴ. 정보보호 대책 수립
ㄷ. 위험평가
ㄹ. 정보보호계획 수립
ㅁ. 위험관리 전략 및 계획 수립

가. ㄱ - ㄴ – ㄷ – ㄹ – ㅁ
나. ㄱ – ㄷ – ㄴ – ㄹ – ㅁ
다. ㅁ – ㄱ – ㄴ – ㄹ – ㄷ
라. ㅁ – ㄱ – ㄷ – ㄴ - ㄹ

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

가. 위험관리는 위험평가를 통하여 조직이 수용할 수 있는 수준을 유지하는 것이 목적이기 때문에 잔류위험이 존재할 수 있다.

나. 적절한 위험평가를 통한 보호대책의 적용 후에도 남아있는 위험이 있을 수 있다.

다. 잔류위험은 위험회피, 이전, 감소 그리고 수용 등으로 처리된다.

라. 위험평가 및 보호대책의 적용 후에도 잔류위험이 존재할 경우 이를 완전히 제거하기 위하여 상세위험분석을 수행하는 것이 일반적이다.

5. 도출된 위험이 해당 사업에 심각한 영향을 주는 관계로 보험에 가입하였다. 이런 식으로 위험을 경감 또는 완화시키는 처리 유형은 무엇인가?

가. 위험 감소(reduction) **나. 위험 전가(transfer)**

다. 위험 수용(acceptance) **라. 위험 회피(avoidance)**

6. 다음 중 위험처리 전략에 대한 설명으로 가장 거리가 먼 것은?

가. 위험수용(risk acceptance)은 위험을 받아들이고 비용을 감수하는 것을 의미한다.

나. 위험감소(risk reduction)는 위험을 감소시킬 수 있는 대책을 채택하여 구현하는 것을 의미한다.

다. 위험회피(risk avoidance)는 수용 가능한 위험 수준 경계의 위험을 모니터링 하는 것을 의미한다.

라. 위험전가(risk transfer)는 잠재적 손실 비용을 제3자에게 이전하거나 할당하는 것을 의미한다.

7. 다음 중 용어에 대한 설명이 옳지 않은 것은?

가. 정성적 기준 : 자산 도입 비용, 자산 복구 비용, 자산 교체 비용이 기준이 됨

나. 정보보호 관리체계 : 정보보호의 목적인 정보자산의 기밀성, 무결성, 가용성을 실현하기 위한 절차 및 과정을 수립하고 문서화하여 지속적으로 관리.운영하는 것을 의미

다. 정보보호의 정책 : 어떤 조직의 기술과 정보자산에 접근하려는 사람이 따라야 하는 규칙의 형식적인 진술을 의미

라. 위험분석 : 위험을 분석하고, 해석하는 과정으로 조직 자산의 취약성을 식별, 위협분석을 통해 위험의 내용과 정도를 결정하는 과정을 의미

8. 위험관리의 핵심은 위험분석이며, 이를 위해 다양한 위험분석 방법론이 존재한다.. 다음 중 위험분석의 기본 요소가 아닌 것은?

가. 자산 나. 취약성 다. 보호대책 라. 경제지수

9. 다음 중 정성적 위험분석 방법으로 짝지어진 것은?

가. 연산예상손실 – 수학공식 접근법 나. 확률분석법 – 델파이법

다. 델파이법 – 순위결정법 라. 수학공식 접근법 – 순위결정법

10. 다음 중 위험분석시 정량적 분석의 단점으로 올바른 것은?

가. 객관적인 평가 기준이 적용된다. 나. 위험관리 성능 평가가 용이하다.

다. 위험관리 성능을 추적할 수 없다. 라. 계산이 복잡하여 분석하는데 시간, 노력, 비용이 많이 든다.

11. 다음은 위험 분석 방법론에서의 정량적 위험 분석 방법과 정성적 위험 분석 방법의 장단점을 비교 설명한 것이다. 가장 부적절한 것은?

가. 정량적 분석은 정보의 가치를 화폐로 표현하기도 하며, 정성적 분석은 정보자산에 대한 가치를 평가할 필요가 없다.

나. 정량적 분석은 위험관리 성능평가가 용이하며, 정성적 분석은 비용/이익을 평가할 필요가 없다.

다. 정량적 분석은 수작업이 용이하며, 정성적 분석은 측정 기준의 객관성을 확보하기가 용이하다.

라. 정량적 분석은 계산이 복잡하여 비용이 많이 들며, 정성적 분석은 위험관리 성능을 추적할 수 없다.

12. 위험분석 방법 중 객관적인 평가기준을 적용할 수 있고 위험관리 성능평가가 용이한 정량적 분석 방법은?

가. 델파이법　　나. 시나리오법　　다. 확률분포법　　라. 순위결정법