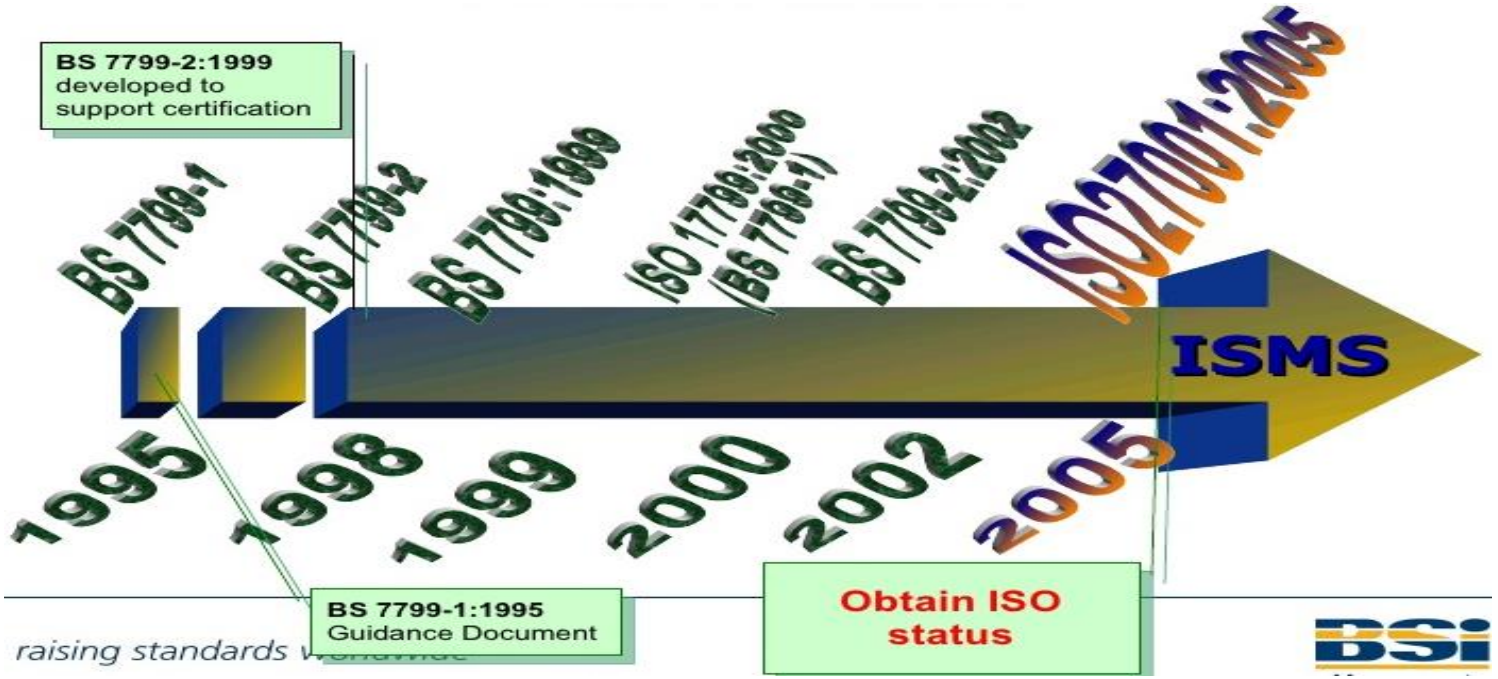
n1.2 정보보호 관리체계 분류

1. 해외 정보보호 관리체계

(1) ISO/IEC 27001(국제표준 정보보호 관리체계)의 이해

- ISO/IEC 27001은 1995년에 영국이 자체 개발한 BS7799(Part1, Part2)를 국제표준으로 상정하여 2005년에 국제 표준인 ISO/IEC27001과 ISO/IEC27002로 표준화됨.
- ISO/IEC 27001:2013 개정판에서는 기존 ISO/IEC 27001:2005의 통제항목 11개 영역 137개에서 통제항목 14개 영역 114개로 개정



n1.2 정보보호 관리체계 분류

국내ISMS와 ISO27001 프레임워크 비교

국내 ISMS	ISO27001(2013 개정안)
정보보호 정책 수립 및 범위설정	Policy
경영진 책임 및 조직 구성	Leadership, Context of the organization
위험관리	Planning
구현	Support
	Operation
사후관리	Performance evaluation
	Improvement

n1.2 정보보호 관리체계 분류

2. 국내 정보보호 관리체계

(1) 정보보호 관리체계(ISMS) 개요

- 국내 공통 표준 관리체계 프레임워크는 슈하트 사이클 또는 데밍 사이클이라고 하는 PDCA 경영관리 순환주기(Management 사이클) 기법을 정보보호에 적용

- 이는 어떠한 일이든 계획을 세우고 실행하면서 그 일이 잘 되었는가를 평가하고, 그 결과를 새로운 계획에 반영하거나 개선활동을 통한 환류 체계가 이루어져 조직 성과가 좋아진다는 개념으로
  - PDCA 모델을 기반으로 정보보호 관리 순환 주기를 개발 하여 S PDCA (Security PDCA)로 5개 프로세스를 설계

- 개발된 관리체계 모델은 국내 보안관리 공통 표준 및 정보보호 컨설팅 방법론으로 활용하게 됨.

n1.2 정보보호 관리체계 분류

국내 보안관리의 표준, 기본 틀, 공통 프레임워크

- ISMS는 정보통신망의 안전성 및 정보의 신뢰성을 확보하고, 조직의 정보보호 수준 제고를 위하여 관리적 · 기술적 · 물리적 보호조치를 종합한 것으로, 2001년 모델을 개발하여 국내 표준으로 제정되었으며 관리체계의 기본 틀이자 공통 프레임워크로 활용되고 있다.

- 이는 새로운 정보보호 위협 및 취약점이 점차적으로 증가하는 시점에서, 조직의 주요 정보자산을 보호하기 위해 정보보호 관리 절차 및 과정을 전사적인 차원에서 체계적이고 지속적으로 관리하기 위한 국내 보안관리 모델의 효시이며 구축 지침서, 컨설팅 방법론으로 활용되고 있다.

- 그 동안 국내 조직에서 단편적이고 일회적이며 산발적으로 대응하던 침해사고 예방에 대해 보다 체계적이고 종합적이고 균형적인 관리체계가 시급하였다. 이에 방법론을 제시하고자 개발되어 국내조직에 적합한 표준적인 정보보호 관리 모델을 제시하여 국내 정보보호 수준제고와 정보보호 서비스 산업 활성화를 가져왔다.

- ISMS는 현재 국내관리체계 ISMS, PIMS, 개인정보 영향평가 등의 공통 프레임워크로 기본 틀이 되었다.

n1.2 정보보호 관리체계 분류

관리체계 공통 표준 프레임워크

- 경영이론인 경영 사이클(Plan-Do- Check-Act)에 기초한 5단계 정보보호 관리과정인 S(Security) -PDCA를 고안 개발하여 관리체계 공통 프레임워크로 활용되고 있으며, 현재의 국내 표준 모델인 ISMS가 2013년 개정을 통해 그림 <1-11>이 탄생

- 기본적으로 정보보호 관리체계는 5개 보안 관리사이클(S-PDCA)의 정보보호 관리 전 과정을 정의하고 있으며, 관리과정의 각 단계별 구현 전략과 통제항목 선택 등 누구나 쉽게 각각의 과정별 단계별 구축 방법을 제시

n1.2 정보보호 관리체계 분류

국내 ISMS 인증 체계

- 현재의 국내 ISMS 인증체계는 과학기술정보통신부가 인정기관 역할을 수행하며 한국인터넷진흥원(KISA)이 인증기관의 역할을 수행.
- 인증심사원은 KISA에서 양성 · 관리하며, 인증기관(KISA)이 인증위원회를 운영

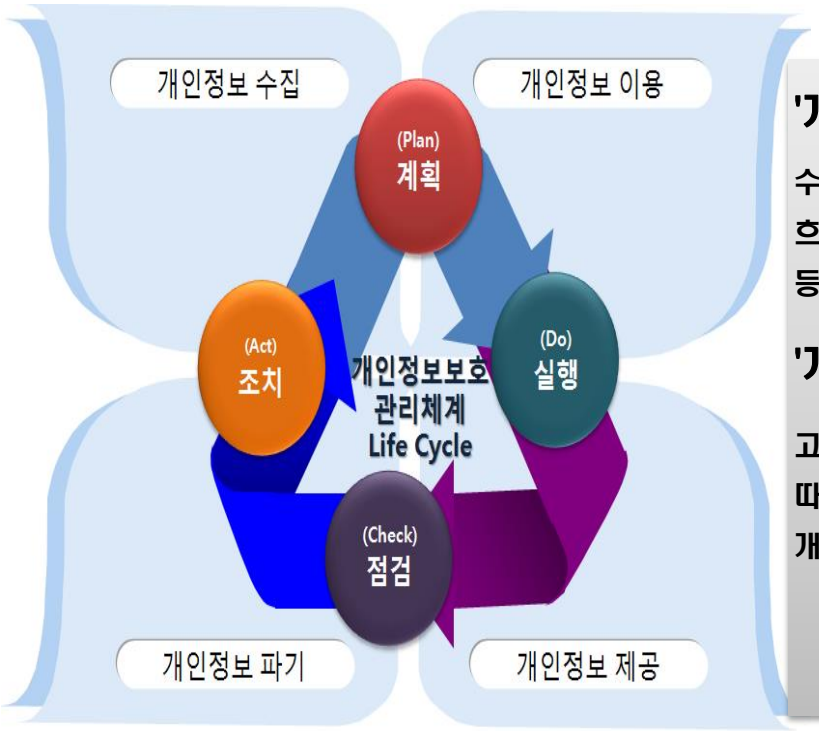
n인증제도 비교

구분	ISO 27001	ISMS	PIMS
인증 기관	BSI, DNV, DQS, TUV 등	KISA	KISA
근거	국제표준	정통망법 제 47조	망법 제47조2
제도성격	권고	권고 + 의무('13.2.18)	권고
인증 대상	민간, 공공기업	민간기업 (통신, 금융, 운송, 제조, 병원, 학교 등)	개인정보를 수집 취급하는 자 (별도 기준 마련)
인증 기준	ISO 27001	방통위고시ITA표준	PIMS 인증기준
구조	정보보호대책 114개 통제항목	관리과정 5단계 12개 통제항목, 정보보호대책 15개 도메인 92개 통제항목 (총 104개 통제항목에 253개 세부항목)	관리과정 5단계 13개 통제항목, 생명주기 4개 도메인 32개 통제항목, 보호대책 9개 도메인 79개 통제항목 (총 124개 통제항목에 310개 세부항목)
시행시기	2013.5	2013.5	2011.11
심사원	ISO 27001 심사원	KISA 교육 및 평가 후 선정	KISA 교육 및 평가 후 선정
인증 유효기간	3년	3년	3년
사후관리 심사주기	매년 2회	매년 1회	매년 1회

n개인정보보호 관리체계(PIMS)

- 조직이 수집, 이용, 제공, 파기하는 모든 고객 개인정보의 안전성과 신뢰성 제공 및 이용자 권리보호를 위해 체계적이고 지속적인 개인정보보호 활동 수행 여부를 확인하고 인증을 부여
- [법적근거] 정보통신망법 제 47조3
  ※ PIMS : Personal Information Management System

개인정보 생명주기에 따른 자율적 보호대책 마련



'개인정보 생명주기'

수집/이용/제공/파기의 개인정보 흐름에 따른 위험관리가 보안위협 등의 효과적인 대응 체계 제공

'개인정보보호 관리체계'

고객의 개인정보 생명주기 특성에 따른 종합적 개인정보 관리를 통해 개인정보 침해 가능성 최소화 필요

➢ **[점검 항목] : 124개**
- 관리과정 요구사항 13개
- 정보보호대책 79개
- 생명주기 요구사항 32개

➢ **[인증 효과]**
- 조직의 개인정보보호 활동에 대한 객관적 자료제시 및 사회적 책임이행
- 경영진의 개인정보보호 정책수립 의사결정 지원

➢ **[인증 혜택]**
- 인증 취득기업이 개인정보 사고 발생 시 과징금, 과태료 경감

(근거 : 정보통신망법 시행령 및 방통위 고시)

n1.2 정보보호 관리체계 분류

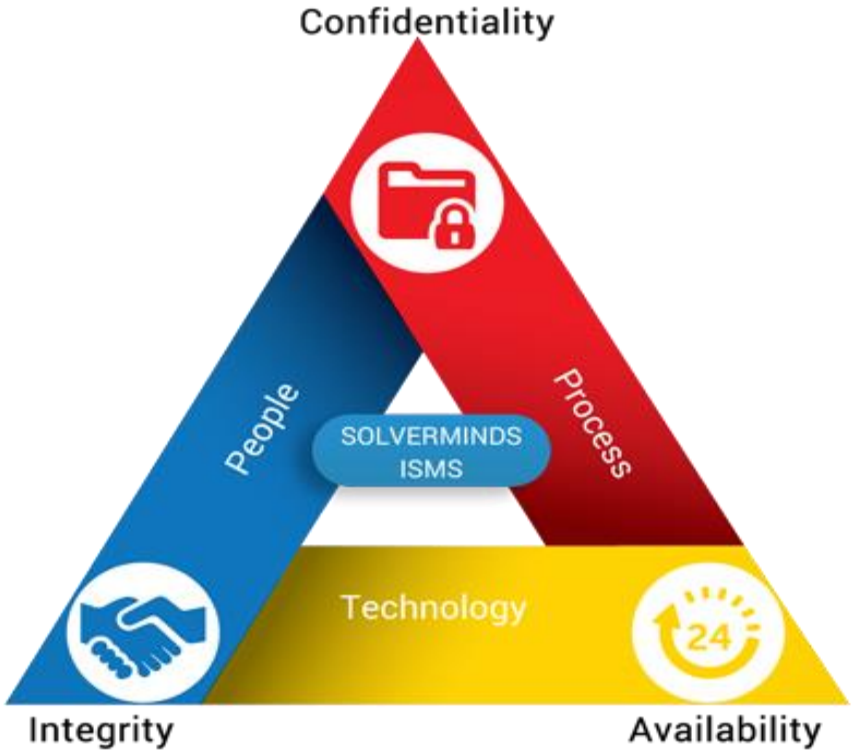
2. 국내 정보보호 관리체계

(2) 개인정보보호 관리체계(PIMS) 개요

- PIMS(Personal Information Management System) 란 개인정보를 안전하게 관리하는 조직을 객관적으로 식별할 수 있는 기준을 제시하여 조직 스스로 개인정보 유·노출 및 개인정보의 수집·보관·이용 등 취급 절차상에서 발생할 수 있는 침해 요인을 파악하고 이를 미연에 방지하도록 하는 체계적이고 종합적인 관리체계

- 개인정보를 취급하는 조직이 전사차원에서 개인정보 보호활동을 체계적이고 지속적으로 수행하도록 하기 위해 필요한 보호체계로서
  - 정보통신망법에 명시된 최소한의 보호조치만으로 개인정보 침해사고 방지에 어려움을 겪었던 조직들에게 체계적인 개인정보 보호활동을 위한 세부 기준 및 방법을 제시

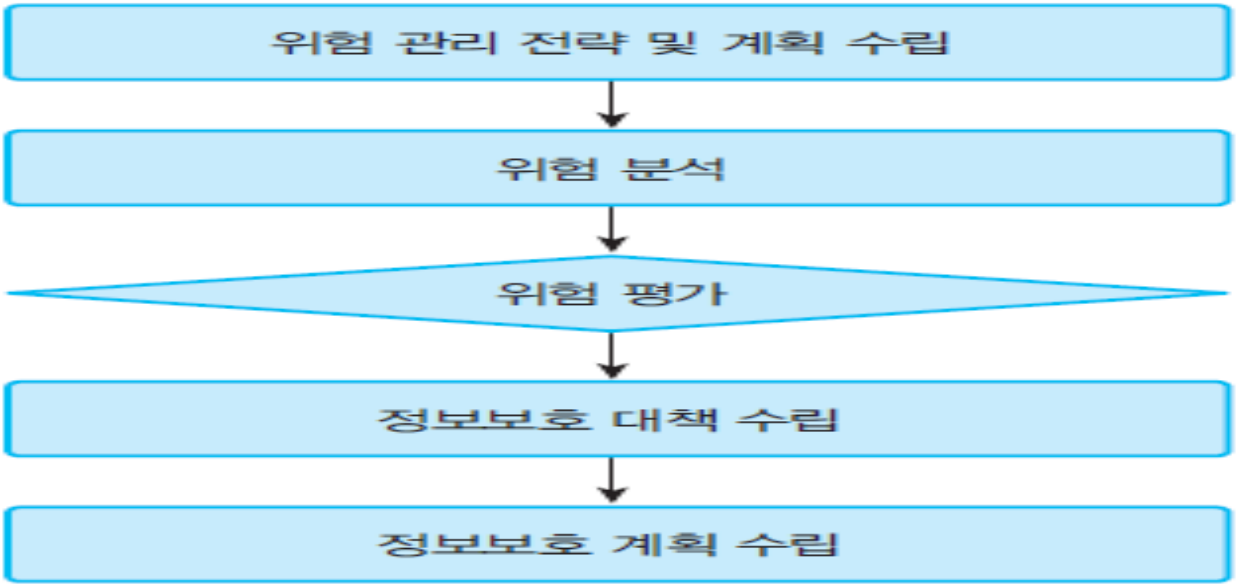
2장. 정보보호 관리체계 개론



1.3 정보보호 위험관리

1. 위험 관리 정의

- ISO/IEC 13335에서의 정보보호 위험 관리(Risk Management) 정의
조직의 정보자산에 대한 위험을 수용할 수 있는 수준으로 유지하기 위하여 정보자산에 대한 위험을 분석하고, 이 위험으로부터 정보자산을 보호하기 위해 비용대비 효과적인 정보보호 대책을 마련하는 일련의 과정



[그림 1-19] 위험 관리 세부과정(ISO/IEC 13335)

1.3 정보보호 위험관리

2. 위험관리의 필요성과 구성요소

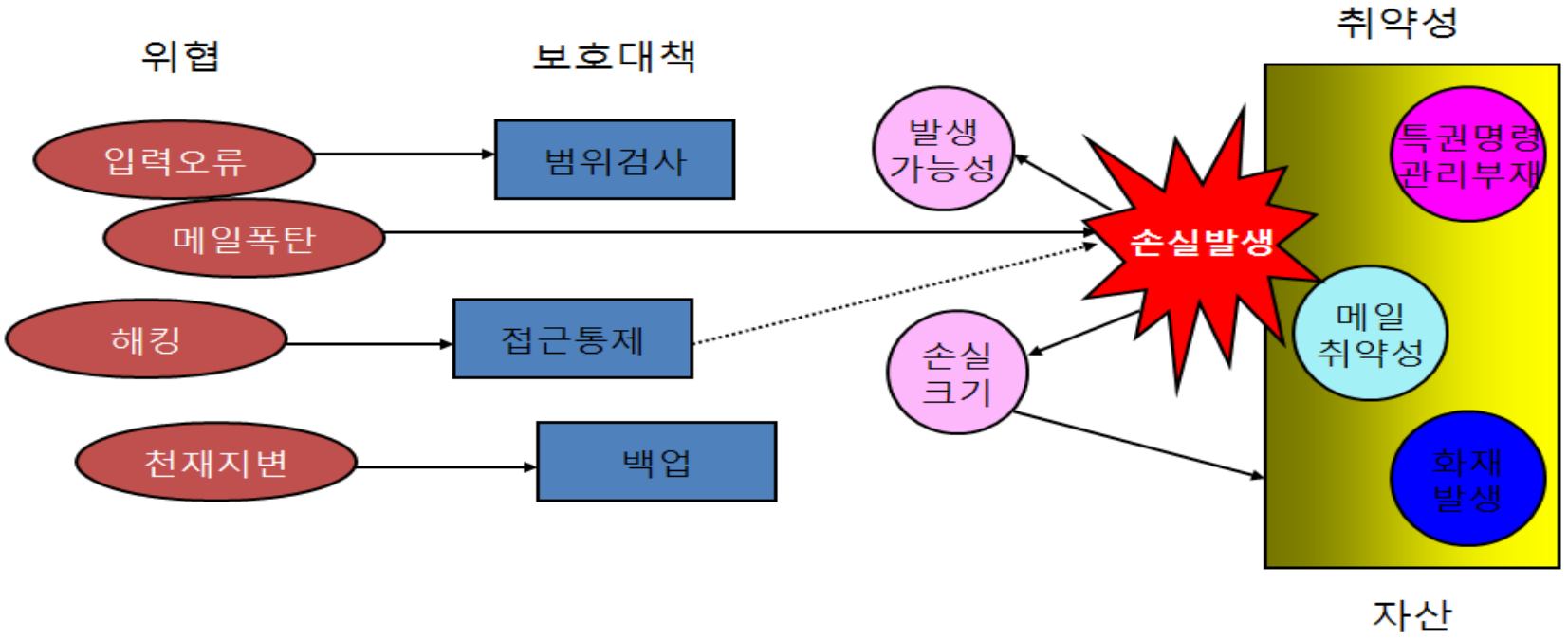
- 위험관리(Risk Management) 목적
  - 위험관리는 자산의 가치와 손실을 측정하여 위험을 평가하고 이를 조직이 수용할 수 있는 수준으로 감소시키기 위하여
  - 적절한 보호대책을 우선순위에 따라 효율적으로 세워서 과도하거나 과소의 투자를 예방하는데 목적이 있음.
  - 따라서 효과적이고 효율적인 보안을 위해서는 위험관리가 반드시 요구

- 우선순위에 따른 효율적 투자
  - 체계적인 위험분석과정 없이 보호대책을 수립할 경우 보호대책 수립에 불필요하거나 과도한 투자 발생
  - 보호대책의 수립에도 불구하고 위협에 대처하지 못하는 경우 발생, 즉 적절한 수준의 보호대책을 필요한 곳에 마련하기 위함

- 위험을 수용할 수 있는 수준으로 유지
  - 위험을 조직이 수용할 수 있는 수준으로 감소시키고 그 수준을 지속적으로 유지하기 위함

1.3 정보보호 위험관리

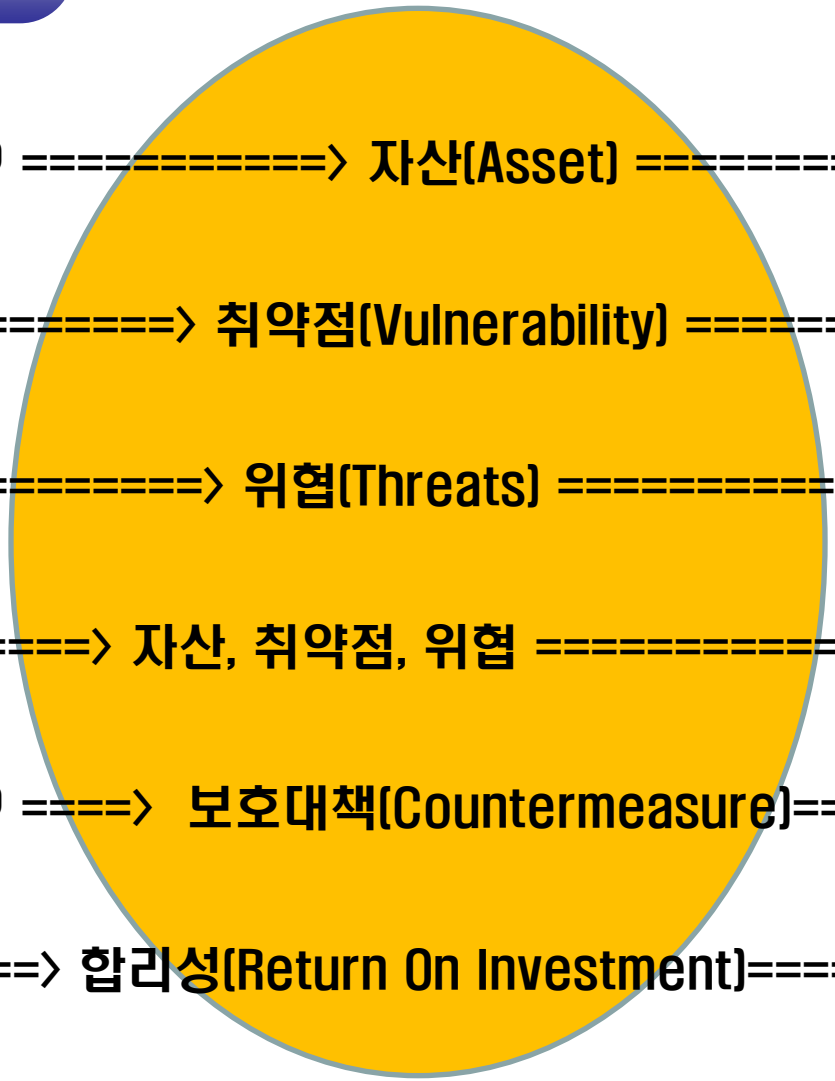
위험관리의 핵심개념



- ✓ 감기바이러스는 어디에나 존재하지만 감기에 걸리는 사람이 있고 안걸리는 사람이 있으며, 그것은 그 사람의 건강상태에 의해서 결정
- ✓ 마찬가지로 위협(감기 바이러스)은 어디에나 있지만 취약점(건강상태)여부 및 정도에 따라 위험(감기에 걸리는 상태)으로 바뀌어 지는지의 여부가 결정

1.3 정보보호 위험관리

정보보호 위험(RISK)이란?

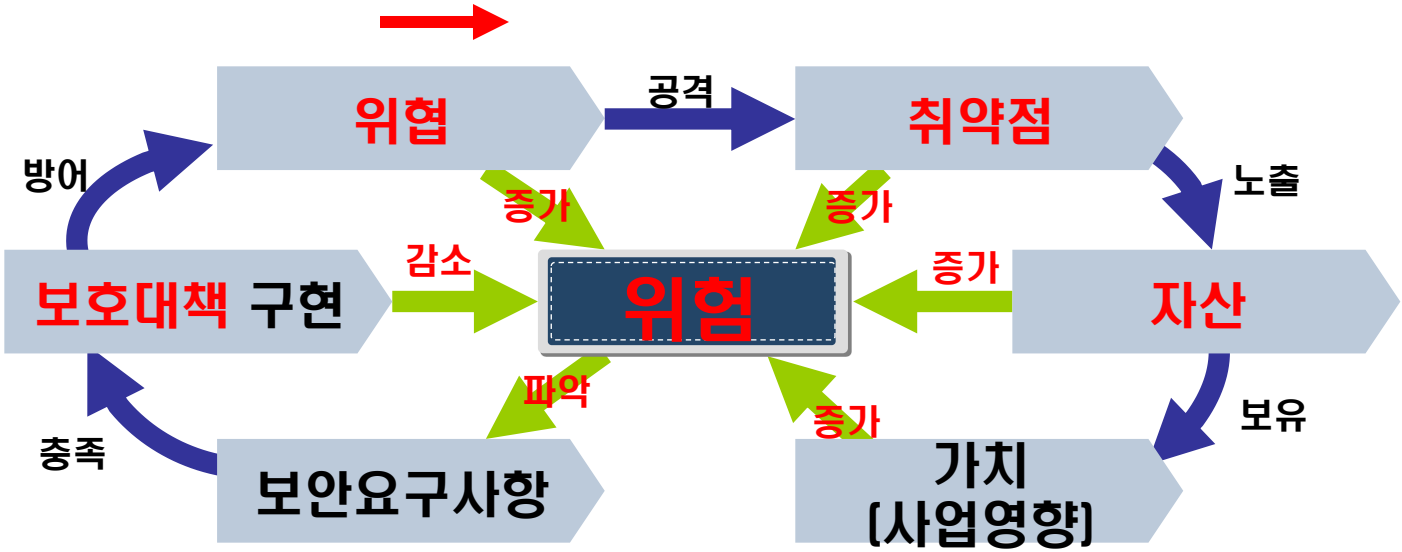


- 무엇을 보호할 것인가? ==========> 자산(Asset) ==========신체
- 얼마나 취약한가 ? =========> 취약점(Vulnerability) ========면역체계
- 어떤 위협이 있나? ==========> 위협(Threats) ==========각종 병원균
- 위험은? ==========> 자산, 취약점, 위협 ==========질병 발생
- 어떤 대책이 필요한가? ====> 보호대책(Countermeasure)====예방접종, 정기검진
- 대책이 합리적인가? ===> 합리성(Return On Investment)=====예방 및 치료수준

1.3 정보보호 위험관리

위험 구성요소들과의 관계

- 위협은 취약점을 공격하여 이용하게 되며 취약점은 자산을 노출시킴
- 자산은 가치를 보유하는데 이러한 위협, 취약점, 자산 가치는 모두 위험을 증가시킴
- 위험을 파악함으로써 보안 요구사항을 파악할 수 있고 보안 요구사항을 만족시키는 정보보호대책을 선정하여 구현함으로써 위협을 방어할 수 있음
- 정보보호대책은 위협을 방어함으로써 위험을 감소시킴



1.3 정보보호 위험관리

(1) 자산 (Assets)

- 자산은 조직이 보호해야 할 대상으로서 정보, 하드웨어, 소프트웨어, 시설 등을 말하며 관련 인력, 기업 이미지 등의 무형 자산을 포함하기도 한다.
- 자산의 유형에 따라 위협과의 관계, 즉 취약점이 분류될 수 있으므로 자산을 분류하여 파악하는 것이 위험을 평가하는데 효과적이다.

(2) 위협 (Threats)

- 위협은 자산에 손실을 초래할 수 있는, 원치 않는 사건의 잠재적 원인이나 행위자로 정의된다.
- 방법론에 따라서 '비인가된 노출' 과 같이, 위협이 발생했을 때 나타나는 결과로 표현 되기도 하고, '패킷의 인터넷 주소위장(IP spoofing) 위협' 처럼 위협사건이 일어나는 방식으로 표현되기도 한다.

1.3 정보보호 위험관리

(3) 취약점(Vulnerability)

- 취약점이란 자산의 잠재적 속성으로서 위협의 이용 대상으로 정의하나, 때로는 정보보호대책의 미비로 정의되기도 한다. 자산에 취약점이 없다면 위협이 발생해도 손실이 나타나지 않는다는 점에서, 취약점은 자산과 위협 사이의 관계를 맺어 주는 특성으로 파악할 수 있다.

- 자산과 위협 간에 어느 정도의 관계가 있는지, 즉 특정 위협이 발생할 때 특정 자산에 자산의 가치와 관련하여 어느 정도의 피해가 발생할 지를 취약점, 노출 정도 또는 효과라는 값으로 나타낸다.

1.3 정보보호 위험관리

(4) 정보보호대책 (Countermeasure)

- **정보보호대책이란 위협에 대응하여 자산을 보호하기 위한 관리적, 물리적, 기술적 대책으로 정의된다.** 이러한 대책에는 방화벽, 침입탐지시스템 등의 제품뿐 아니라 절차, 정책, 교육 등의 모든 통제들이 포함된다.

- 일반적으로 보호대책은 다양한 측면에서 역할을 하게 되는데, 패치 프로그램이나 항온 항습기처럼 취약점을 보호하기도 하고, 감사나 침입탐지시스템처럼 사고를 발견하도록 하거나, 침해사고대응체계 구축처럼 침해사고의 영향을 줄이기도 하고, 백업처럼 복구를 지원하기도 하며 교육이나 훈련처럼 위협의 발생 자체를 억제하기도 한다.

1.3 정보보호 위험관리

(5) 위험구성 요소들 간의 관계

- 위험을 구성하는 요소인 자산, 위협, 취약점, 보호대책간의 관계

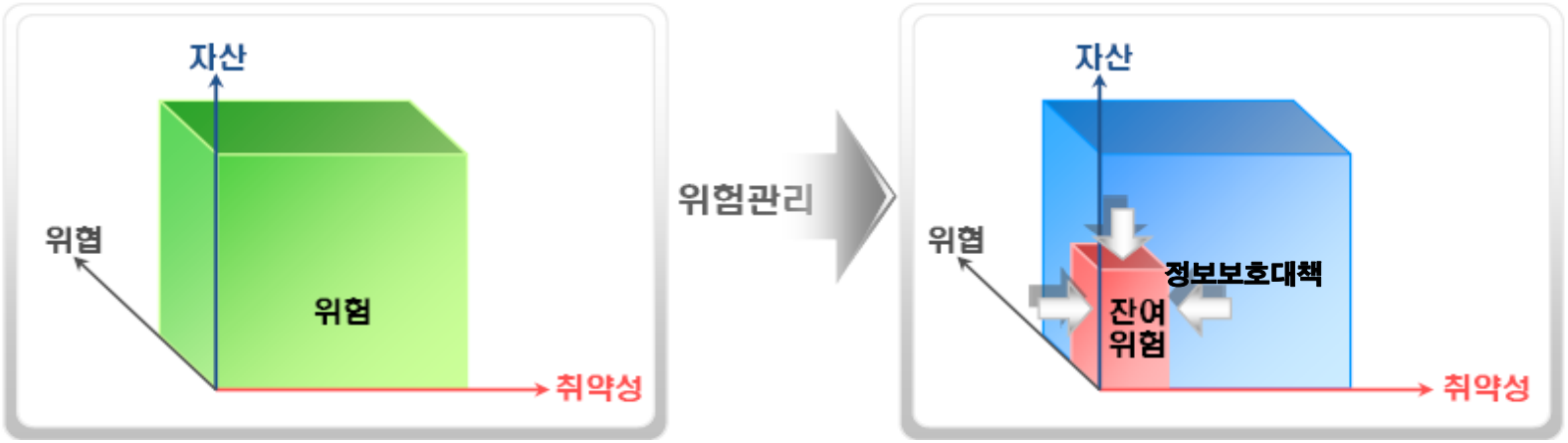
- 이러한 요소들은 서로 영향을 미치게 되는데 위협은 취약점을 공격하여 이용하게 되며 취약점은 자산을 노출시킨다. 또한 자산은 가치를 보유하는데 이러한 위협, 취약점, 자산, 가치는 모두 위험을 증가시킨다.

- 한편 위험을 파악함으로써 보안요구사항을 파악할 수 있고 보안 요구사항을 만족시키는 정보보호대책을 선정하여 구현함으로써 위협을 방어할 수 있다. 정보보호대책은 위협을 방어함으로써 위험을 감소시켜야 한다.

1.3 정보보호 위험관리

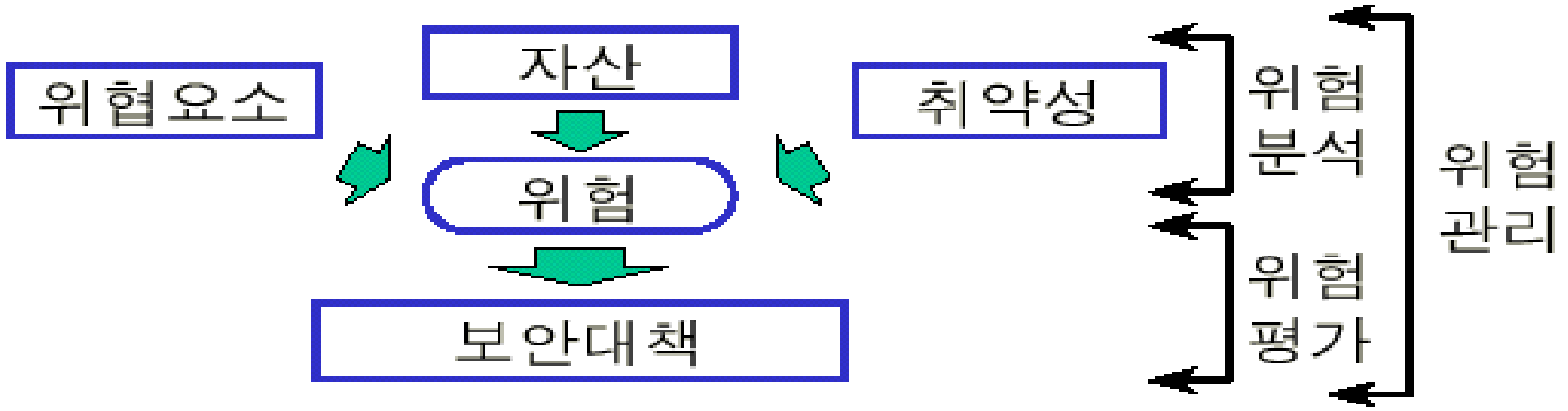
위험의 구성요소

- 자산(Asset) : 조직이 보호해야 할 대상으로서 정보, 하드웨어, 소프트웨어, 시설 등을 말하며 관련 인력, 기업 이미지 등의 무형자산 포함
- 취약점(Vulnerability) : 위협에 의해 보안에 부정적 영향을 줄 수 있는 정보자산의 속성이나 상태
- 위협(Threats) : 정보자산의 보안에 부정적 영향을 줄 수 있는 외부의 환경 또는 사건(이벤트)
- 위험(Risk) : 자산의 취약한 부분에 위협요소가 발생하여 자산의 손실, 손상을 유발한 잠재성(가능성)
- 정보보호대책(Safeguard, Countermeasure) : 위험에 대응하여 자산을 보호하기 위한 관리적,물리적, 기술적 대책
- 잔여위험(Residual Risk) : 대책을 구현한 후 남아 있는 위험



1.3 정보보호 위험관리

위험 관리란?



- 위험분석 : 위험을 분석하고 해석하는 과정으로 자산의 취약점을 식별하고 발생 가능한 위험의 내용과 정도를 결정하는 과정
  - 합리적이고 효율적인 정보보호가 이루어지도록 정보 시스템에 대한 자산 분석, 보호할 가치가 있는 유·무형 자산을 분류, 분류된 자산에 대한 취약점과 위협을 파악

- 위험평가 : 조직에서 발생할 수 있는 손실에 대비한 보안 대책에 드는 비용 효과 분석을 통해 적은 비용으로 가장 효과적인 위험관리를 수행하기 위한 과정
  - 분석결과를 기초로 보안현황을 평가하고, 적절한 방법을 선택하여 효과적으로 위험수준을 낮추기 위한 과정

1.3 정보보호 위험관리

3. 위험 분석

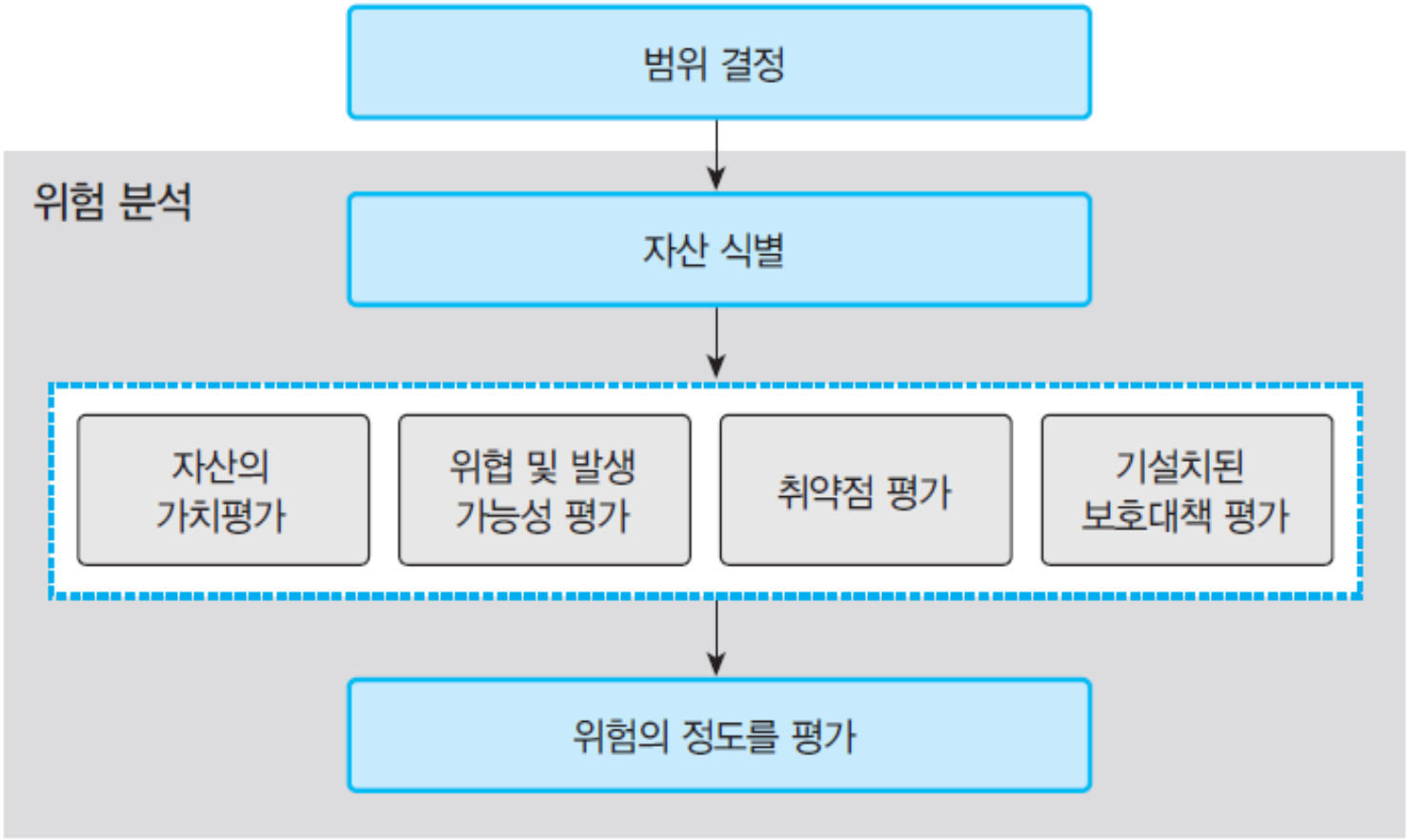
- 위험 분석은 자산의 취약점을 식별하고, 존재하는 위협을 분석하여 이들의 발생 가능성 및 위협이 미칠 수 있는 영향을 파악해서 보안 위험의 내용과 정도를 결정하는 과정이다.

- 위험 분석의 결과는 적절한 보호 대책을 선정할 수 있는 근거가 된다.

- 위험 분석의 절차는 자산식별 및 평가, 위협평가, 취약점 평가, 기존 정보보호대책의 평가를 통해 잔여 위험을 평가하는 단계로 나눌 수 있다.

1.3 정보보호 위험관리

3. 위험 분석



[그림 1-21] 위험 분석의 절차(ISO/IEC 13335)

1.3 정보보호 위험관리

(1) 자산식별 및 평가

자산을 유형별로 분류하여 목록을 작성하고 각 자산에 대하여 가치를 평가한다. 각 자산에 대하여 기밀성, 무결성, 가용성의 요구 정도를 평가한다. 이 세 가지 측면의 정보보호 속성과 해당 자산의 가치에 기초하여 각 위협에 따른 보안사고가 각 자산에 미치는 영향(손실)을 판단하게 된다.

(2) 위협 및 취약점 분석

발생 가능한 위협을 목록화하고 각각의 발생 가능성을 예측한다. 또한 위협에 대한 취약점을 자산 별로 확인하여 그 정도를 결정한다.

(3) 위험 평가
해당 정보자산의 가치와 위협 및 취약점의 정도에 따라 기밀성, 무결성, 가용성 손상에 따른 잠재적 손실의 규모를 평가한다. 위험평가 방법론 중에서 정량적 방식에서는 자산의 가치는 금액으로 평가되고 위협은 연간 발생 횟수로 평가된다.

연간예상손실(A,T) = 자산 A의 가치(원) x 위협 T의 연간 발생횟수(n) x T에 대한 A의 취약점(%)

1.3 정보보호 위험관리

- 방법론에 따라서 약간의 차이는 있지만 자산, 위협, 취약점의 값을 곱하거나 더해서 위험 값을 산출한다. 어떠한 방식을 사용하든지 위험평가 결과는 “수용 가능한 목표 위험수준” 과 비교할 수 있는 형태로 표현되어야 한다.

〈표 1-22〉 3단계 정성적 위험평가 기준 예시

위협		1			2			3		
취약점		1	2	3	1	2	3	1	2	3
자산	1	3	4	5	4	5	6	5	6	7
	2	4	5	6	5	6	7	6	7	8
	3	5	6	7	6	7	8	7	8	9

1.3 정보보호 위험관리

① 목표 위험수준 및 위험 우선순위 설정

모든 위험을 완전히 제거하는 것은 불가능하며 또한 불필요하다.
예, 100원짜리 정보를 보호하기 위하여 200원을 투자하는 것은 무의미하다.

또는 적은 규모의 손실은 일상적인 비용으로 처리할 수도 있다. 따라서 미리 조직에서 수용 가능한 목표 위험수준을 설정하고 이 이상의 위험에 대해서만 적절한 대응을 강구하는 것이 필요하다.

② 목표 위험수준의 설정 책임

수용 가능한 목표 위험수준(DoA)은 조직의 책임자가 결정해야 한다. 예산에 맞추어 가장 우선순위가 높은 위험부터 대응하는 것은 실질적인 대응 방안이기는 하지만, 조직의 책임자는 현재 조직의 위험수준과 목표 위험수준을 알아야 하고, 어느 정도의 투자를 통해서 언제 위험수준이 목표 수준에 도달 가능한 지를 예상할 수 있어야 한다.

추가투자를 통해 위험을 목표 수준 이하로 관리할 것인지, 또는 위험 부담을 감수하고 장기 계획을 세울 것인지는 조직의 경영책임자가 결정할 문제이다.

1.3 정보보호 위험관리

(4) 위험 처리

현재의 위험이 조직에서 수용할 수 있는 수준을 넘어선다면, 이 위험을 처리해야 한다. 처리방식은 위험수용, 위험감소, 위험회피, 위험전가 네 가지로 나눌 수 있다.

① 위험 수용(Risk acceptance)
현재의 위험을 받아들이고 잠재적 손실 비용을 감수함을 말한다. 어떠한 대책을 도입하더라도 위험을 완전히 제거할 수는 없으므로, 일정수준 이하의 위험은 감수하는 것이다.

② 위험 감소(Risk reduction, mitigation)
위험을 감소시킬 수 있는 대책을 채택하여 구현하는 것이다. 대책의 채택 시에는 이에 따른 비용이 소요되기 때문에 이 비용과 실제 감소되는 위험의 크기를 비교하는 비용효과 분석을 실시한다. 즉, 아래의 식으로 양(+)의 효과를 갖는 정보보호대책을 선택한다.

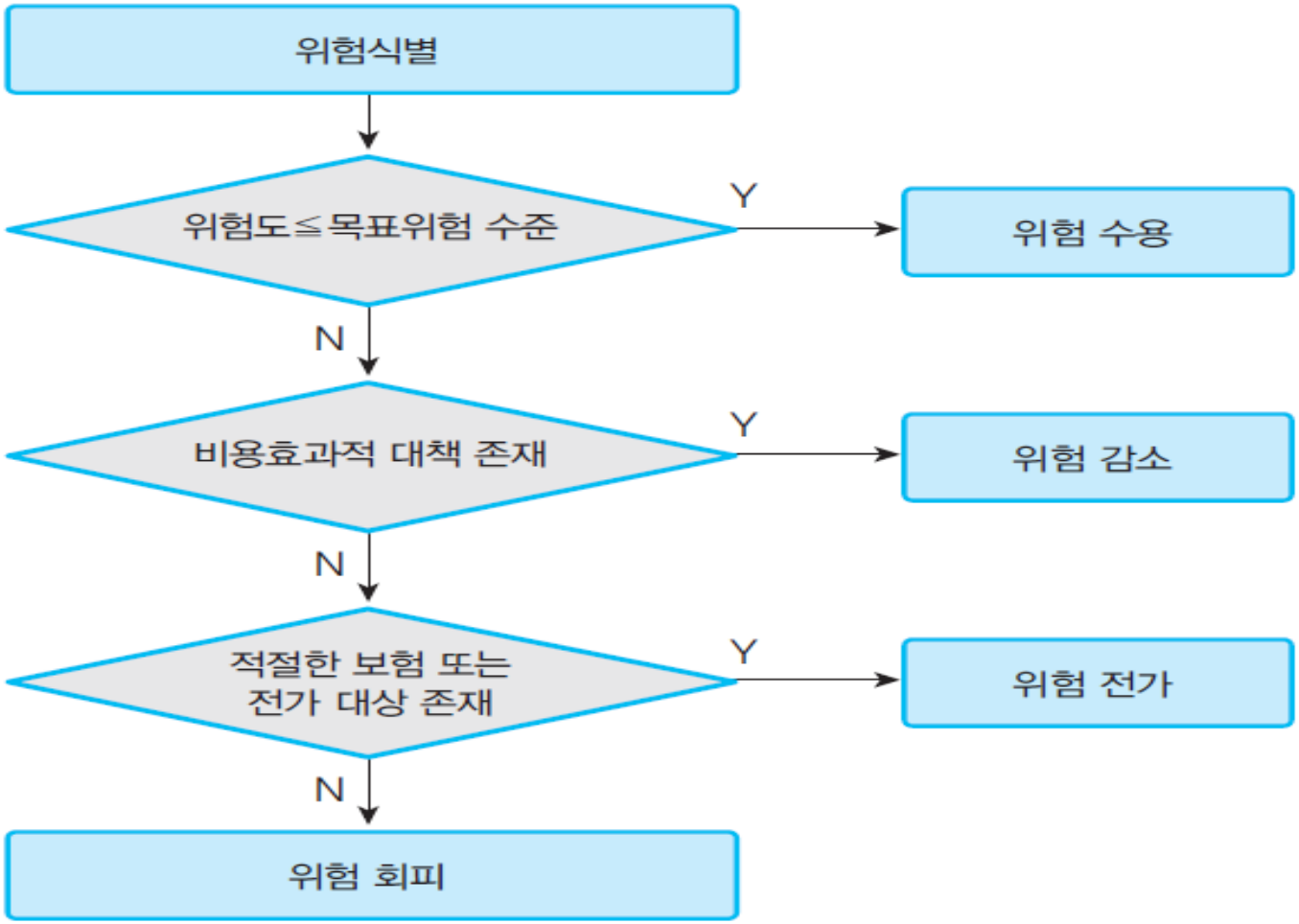
정보보호대책의 효과 = 기존 ALE – 대책 구현 후 ALE – 연간대책 비용

* 연간 예상 손실액(ALE: Annualized Loss Expectancy)

③ 위험 회피 (Risk avoidance)
위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것이다.

④ 위험 전가 (Risk transfer)
보험이나 외주 등으로 잠재적 비용을 제3자에게 이전하는 것이다.

1.3 정보보호 위험관리



[그림 1-22] 위험 처리 절차(ISO/IEC 13335)

1.3 정보보호 위험관리

4. 정보보호대책 선정

대책 수립을 통한 위험감소 방안을 선택하게 되면 통제사항과 이에 따른 대책을 선정한다.

해당 통제사항들은 각종의 실제적인 대책을 대부분 포함하고 있다. 그러나 위험의 내용과 규모에 따라서는 제시된 통제사항의 내용 중에서도 더 세부적이고 강력한 대책이 필요할 경우가 있다.

정보보호 관리체계 인증을 염두에 두고 있다면 이런 경우에는 관련된 통제사항을 선택하고 구체적인 대책을 명시해야 한다.

선택된 각 통제사항은 비용 · 효과 분석을 통해 정당화되어야 한다. 즉, 통제의 구현과 유지에 들어가는 비용이 해당 위험의 감소량보다 적어야 한다.

위험 = 위험이 성공할 가능성 x 위협 성공 시의 손실(영향) 크기

B > PL

B: 보호대책을 구현하는 데 필요한 비용

P: 손실이 일어날 확률, L: 특정 사건에 의한 총체적 손실

1.3 정보보호 위험관리

5. 이행계획 수립

(1) 프로젝트 구성
위험을 목표 위험수준 이하로 감소시키기 위해, 필요한 대책들을 선택하고 유사한 대책들은 하나의 프로젝트로 통합하여 이 프로젝트들에 대한 우선순위를 설정한다.
유사한 대책들은 즉시 교정 가능한 취약점 제거, 정책 및 절차 수립, 분야별 정보보호 시스템 도입 및 관련 교육 수행, 모니터링 및 감사 관련사항 등으로 통합, 분류될 수 있다.

(2) 즉시 교정 가능한 취약점 제거
기술적 취약점 점검을 통해 즉시 교정 가능한 취약점 제거는 주로 시스템이나 장비의 구성 설정 변경, 파일 등의 권한 변경, 취약한 패스워드 변경 등으로 빠른 시간 내에 처리할 수 있는 사항들이다.

(3) 정책 및 절차 수립
정책 및 절차를 수립하는 작업은 일반적으로 다른 업무보다 높은 우선순위를 갖는다. 해당 정책이나 절차의 내용에 따라 사업 연속성 계획처럼 규모가 크고 최종 완료 시까지 오랜 시간이 소요되므로 장기 프로젝트로 수행해야 하는 것도 있다.

1.3 정보보호 위험관리

5. 이행계획 수립

(4) 정보보호 시스템 도입 및 관련 교육
원칙적으로 정보보호 시스템은 기 수립된 정보보호 정책과 절차를 준수해야 한다. 따라서 정보보호 시스템 도입 시 시스템 요구사항에는 정책 요구사항이 반드시 반영되어야 한다.

(5) 모니터링 및 감사
모니터링이나 감사의 수행은 전체 정보보호 관리과정의 마지막 단계인 사후관리 단계에서 이루어진다. 그러나 모니터링이나 감사를 위한 정책, 절차, 책임 설정, 모니터링 또는 감사용 시스템 도입 등과 같이 모니터링 및 감사에 필요한 사항들은 정보보호계획 수립단계에서 결정되어야 한다.

(6) 구현 계획 수립
프로젝트 별로 예산, 구현 일정, 프로젝트의 세부 내용, 해당 프로젝트 수행에 관한 책임 등이 포함된 정보보호 계획을 수립한다.

(7) 정보보호 대책명세서 작성
정보보호 대책명세서는 위험 평가 및 위험처리 프로세스의 결과와 결론에 근거하여 조직의 관리체계에 적절하고 적용 가능한 통제 목표 및 통제항목을 기술한 문서이다.

1.4 기업 보안관리 전략

1. 체계적이고 효과적인 보안관리 전략 수립

- 체계적인 정보보호 프로세스를 정립하라.
- 비용효과적인 방법을 염두에 둔 전략을 수립하라.
- 사람에 대한 보안에 관심을 가져라.
- 정보공유와 정보보호 사이의 균형을 맞춰라.
- 정보보호 활동을 조직 문화로 정착시켜라.
- 보안관리 전략은 기업의 비즈니스 목표를 지원하도록 한다.

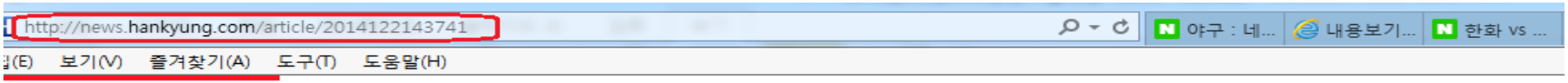
1.4 기업 보안관리 전략

4. 관리체계 인증 관련 오해와 진실

- 인증을 받았는데 왜 침해사고가 발생하나?
- 관리체계 구축 시에는 반드시 컨설팅을 받아야 한다?
- 관리체계 운영은 정보보호 조직에게 업무가중만 준다?
- 관리체계 인증기준은 획일적이며 중소기업에는 맞지 않다?
- 인증 심사 시 문제점 발견 시 신청기관 담당자 등이 문책을 받게 된다?
- 인증심사원에 정보를 최대한 제공하지 않아도 인증 취득에 지장 없다?

해커에 농락당한 '보안 양호' 한수원

출처: http://news.hankyung.com/article/2014122143741



한국수력원자력의 원자력발전소 설계 도면 일부가 또다시 인터넷에 공개됐다. 국가 핵심 시설이자 기간산업인 원전의 설계 도면이 무방비로 유출되고 있는데도 한수원과 전력당국, 수사기관은 해킹 경로와 방식 등에 대한 실마리조차 잡지 못하고 있다.

그럼에도 한수원의 정보보안 실태를 점검하는 국가정보원은 2012년과 2013년 두 해에 걸쳐 한수원의 보안 관리등급을 80점 이상(100점 만점)인 '양호'로 판정한 것으로 나타났다.

한수원 원전 도면 유출 사건 일지

12월15일	한수원 임직원 1만799명의 사번, 휴대폰 번호 등이 담긴 엑셀 파일
18일	월성 1호기 배관설치도면 2장, 고리 1·2호기 배관계측도면 1장, 고리 1·2호기 보조건물 냉각수계통도면 등 6건
19일	원자로 냉각시스템의 밸브 도면 등 9건
21일	고리 1·2호기 공기제어 시스템, 방사선 확산 계산용 프로그램 매뉴얼 등 8건
25일	원전 도면 전면 공개 예고

한수원을 해킹했다고 주장하는 '원전 반대그룹 후엠아이(WHO AM I)'는 21일 오전 1시30분께 트위터를 통해 한수원의 무능력한 보안 시스템을 조롱하는 글과 함께 월성 1호기의 밸브 도면, 고리 2호기의 공조기와 냉각 시스템 도면, 고리 1·2호기 공기제어 시스템 등 8개 자료를 추가 공개했다. 지난

1.4 기업 보안관리 전략

관리체계 인증 관련 오해와 진실

- 인증의 범위 내 정보자산 누락 여부는 인증심사원이 파악해야 한다?
- 인증 심사시에 통제항목만 심사한다?
- 위험분석 및 평가는 최초 관리체계 구축 시에만 하면 된다?

감사합니다^^
Happinessisnowhere!

조 병 철
bcho@naver.com 010-5247-5178