



# 위험도 분석

작성자 : ERIC YOON

본 자료는 본인의 학습과 제3자의 자율적 학습의 이해를 높이기 위해 제작 하였습니다.

비영리 목적 이므로, 공개 배포,합니다.

단, 무단 배포, 수정금지 !!

배포시 사전에 (목적,출처)알려주시면 감사 하겠습니다.

잘못된 부분은 피드백 주시면 즉시 수정 하도록 하겠습니다.

해당 자료는 NAVER 와 GOOGLE 의 참조 이미지 ,지식백과와  
한국인터넷진흥원 KISA 의 자료를 검색하여 제작하였습니다.

# 학습 목표

- ▶ 개인정보영향평가PIA,
- ▶ 정보보호 관리체계 ISMS,
- ▶ 개인정보보호 관리체계 PIMS,

에서 수없이 거론되는 사전 평가인

위험도 분석에

대해 자세히 알아 보려고 한다.

# 위험 분석이란 (Risk analysis)??

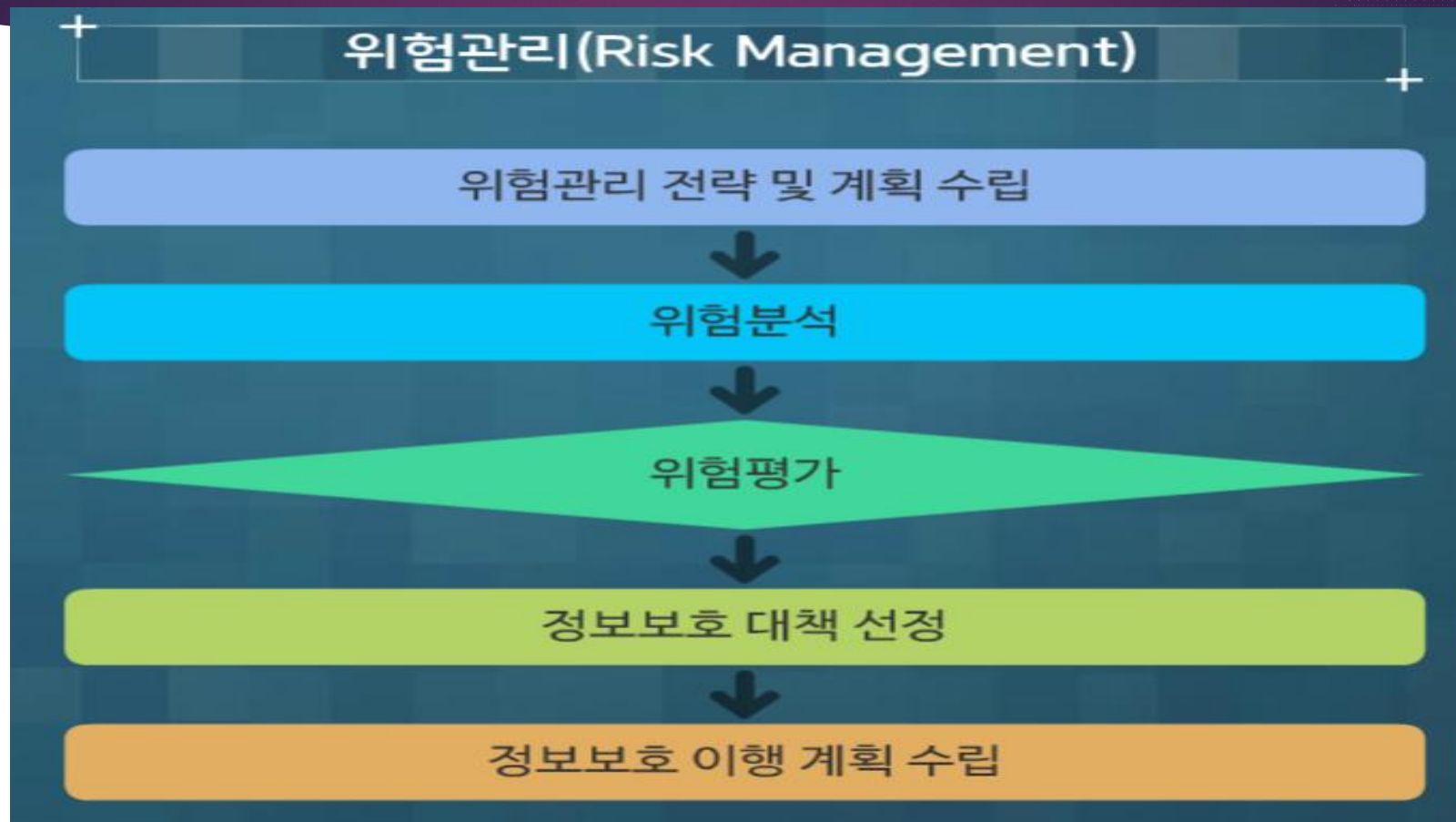
- ▶ 보안 위험을 확인하고 그것들의 중요도를 결정하며 보호 수단을 요하는 부분을 확인하는 과정. 정보 시스템과 관련 자산의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 다양한 위협에 대해 시스템이 취약함을 인식하고, 이로 인해서 예상되는 손실을 분석하며, 안전한 정보 시스템을 구현하고, 정보 자원에 대한 위험 요소를 식별, 평가하여 그러한 위험 요소를 적절하게 통제할 수 있는 수단을 체계적으로 구현하고 운영하는 전반적인 행위 및 절차이다. 위험 분석은 위험 관리의 일부분이다

▶ .[네이버 지식백과] 위험 분석 [risk analysis, 危險分析] (IT용어사전, 한국정보통신기술협회)

# 위험 평가란 (Risk assessment) ?

- ▶ 임의의 시스템, 네트워크, 조직 등에서 발생할 수 있는 손실에 대비한 보안 대책에 드는 비용 효과 분석을 통해 적은 비용으로 가장 효과적인 위험 관리를 수행하는 것.

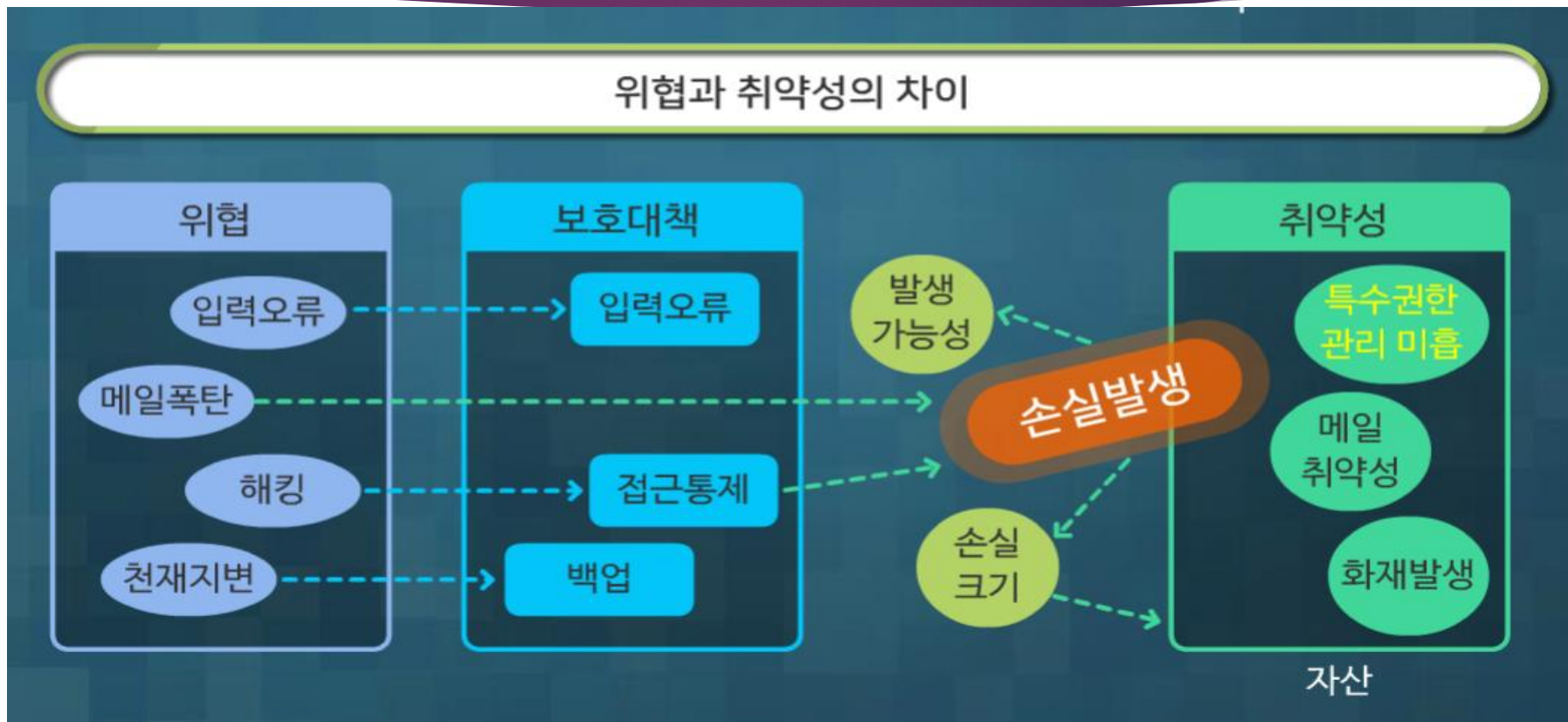
# 1. 위험관리 전략 및 계획 수립



# 1. 위험관리 전략및 계획 수립

- ▶ 정의
- ▶ 기업이 보유한 개인정보 관련 자산에 대한 위험을 수용할수 있는 수준으로 유지하기 위해
- ▶ 자산에 대한 위험을 분석 하고
- ▶ 위험으로부터 자산을 보호하기위해
- ▶ 스스로 판단으로 효과적인 보호대책을 마련하는 일련의 과정

# 위협 과 취약점을 구별 하자

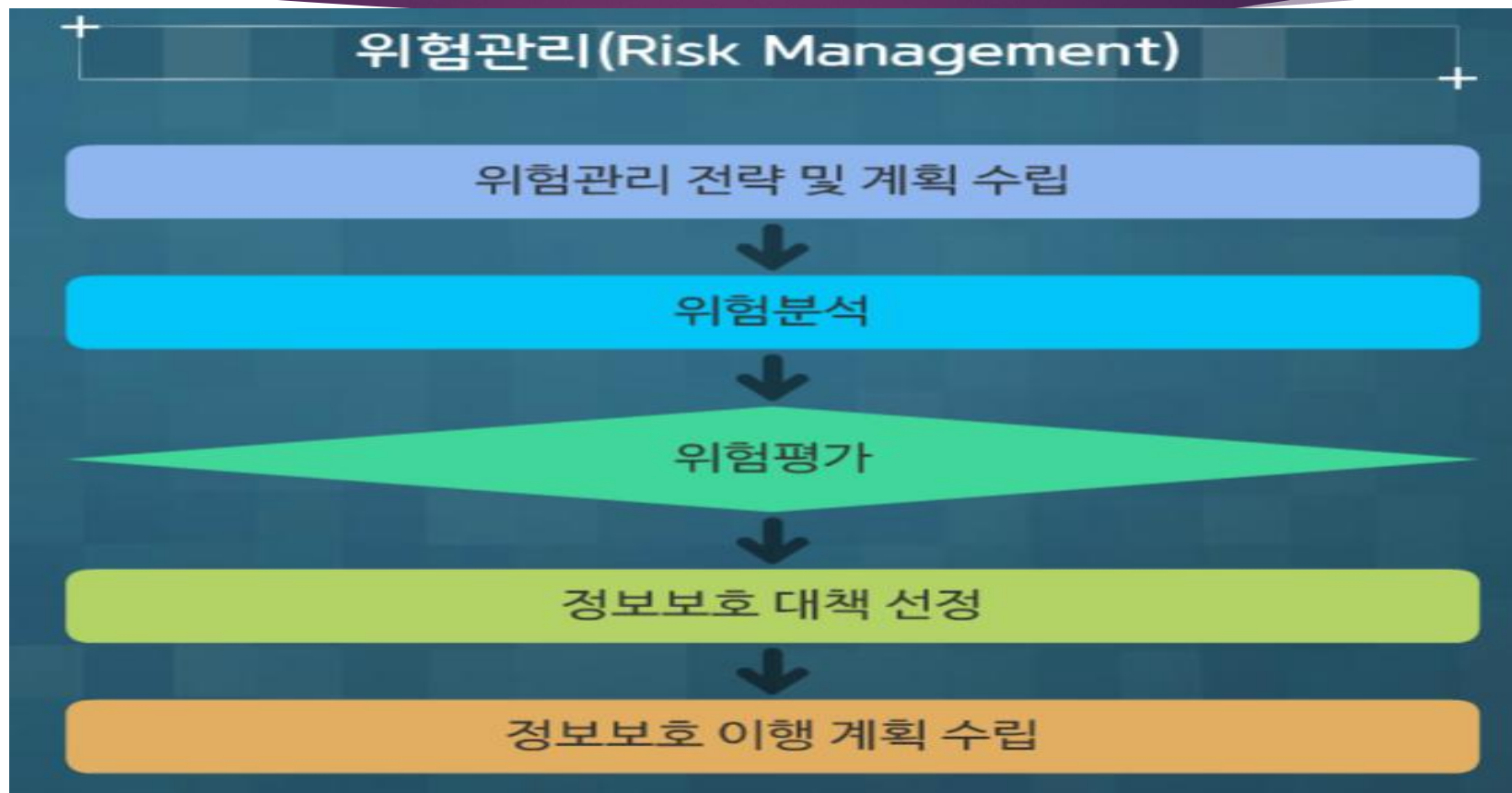




# 1. 위험관리 전략 및 계획 수립

- ▶ 위협 + 취약점 + 위험
- ▶ 위협 = 외부적 손실 원인
- ▶ 취약점 = 자산이 가지고 있는 문제점
- ▶ 위험 = 위협이 취약점을 공격 했을때, 발생하는 사항.
- ▶ 대응책 = 정보보호 대책  
각 사항에 맞게  
위험 분석 계획을 수립한다.

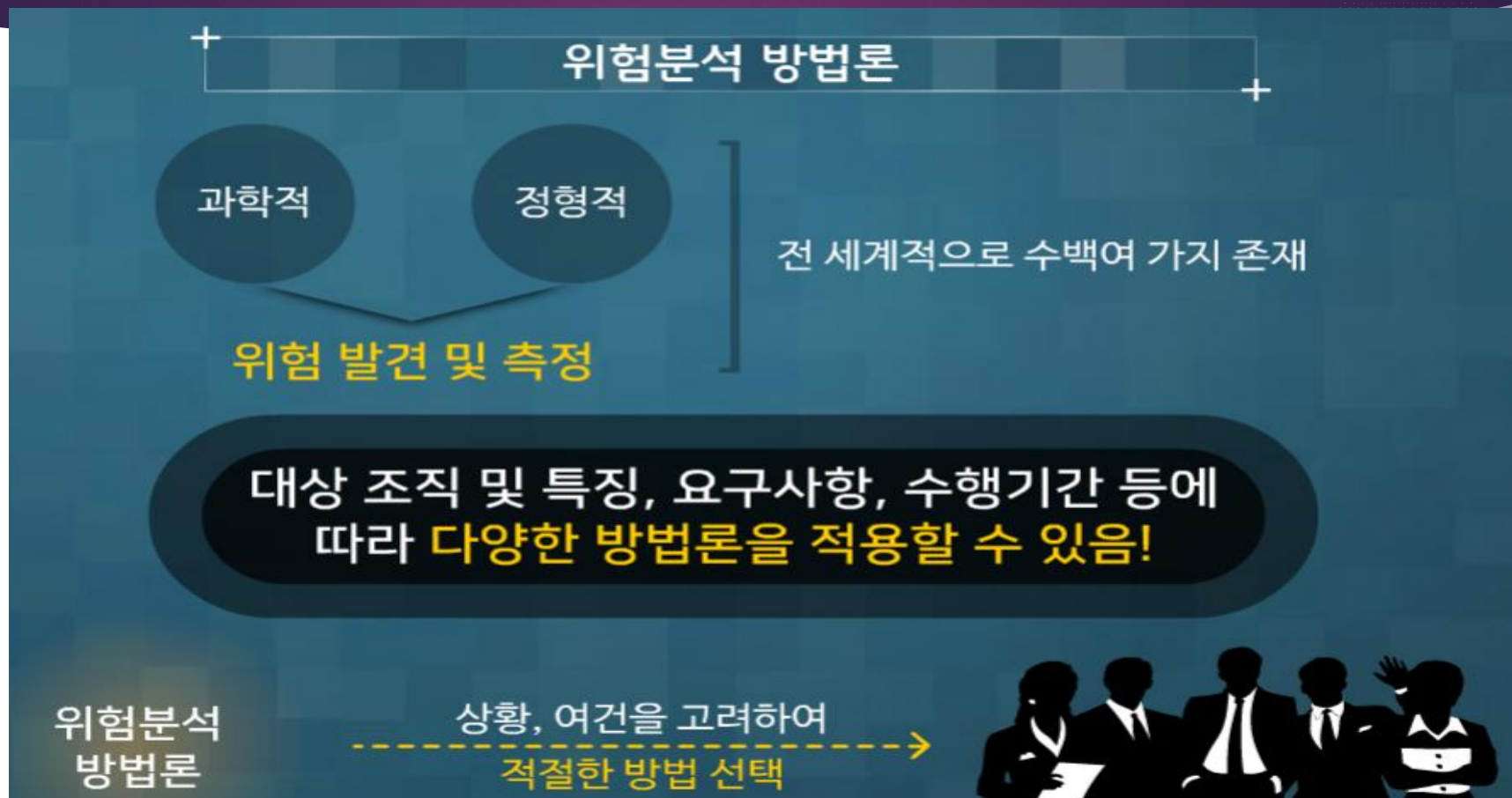
## 2. 위험 분석



## 2. 위험 분석

- ▶ 위험 분석 방법에는 전세계적으로 수백가지가 있다.
- ▶ 위험 분석에는 특정한 방법론이 제기되고 있지 않다.
- ▶ 각 상황에 맞게 설정하여 여러 방법중 적절한것을 선택하면된다

## 2. 위험 분석



## 2. 위험 분석

### + 계량화 여부에 따른 방법 정의 +

#### 정량적 분석

- 손실크기를 화폐 단위로 측정이 가능할 때 사용하는 분석법
- 과거자료 접근법, 수학기초 접근법, 확률분포 추정법

#### 장점

- 정량화된 자료의 사용으로  
비용-효과 분석 및 예산  
계획이 쉬움
- 수리적 방법의 사용으로  
계산이 논리적

#### 정성적 분석

#### 단점

- 정확한 정량의 수치를 구하기  
어려움
- 수리계산에 많은 시간과  
노력이 필요함

- ▶ 위험 분석에는 크게
- ▶ **정량적 분석** 과
- ▶ **정성적 분석** 으로
- ▶ 구별할 수 있다.
  
- ▶ 각 장.단점 을 확인해 보자.

## 2. 위험 분석

### + 계량화 여부에 따른 방법 정의 +

#### 정량적 분석

- 손실크기를 측정할 수 없어서 위험을 구간 및 기술변수로 표현
- 분석자의 경험 및 지식에 기초한 위험분석 방법

#### 장점

- **정량화하기 어려운 정보의 평가에 쉬움**
- 용어의 이해가 쉬움
- 분석의 소요시간이 짧음

#### 정성적 분석

- 주관적 판단의 남용 여지가 있음
- 비용-효과 분석이 어려움

- ▶ 위험 분석에는 크게
- ▶ **정량적 분석** 과
- ▶ **정성적 분석** 으로
- ▶ 구별할 수 있다.
- ▶ 각 장.단점 을 확인해 보자.
- ▶ Tip- 전문가 산정방법인  
델파이 기법,시나리오,순위결정법 이 정성적  
방법이다.



### 3. 위험 평가



### 3. 위험 평가

▶ 전 단계의 위험도 분석을 (정성적,정량적 )방법으로 분석 하였으면  
다음 단계인 위험평가에서는

접근 방식에 따라 위험 평가 를 진행 한다.

대표적인 방법 4 가지에대해 먼저 살펴 보자



### 3. 위험 평가

접근방식에 따른 방법 정의

위험  
분석

위험  
관리

접근방법의 산정 필요!

위험분석 및 평가 대상 조직의 보안요구사항,  
가용자원, 규모 등을 고려

기준선 접근법  
(Baseline Approach)

전문가 판단법  
(Informal Approach)

상세위험 접근법  
(Detailed Risk  
Approach)

복합적 접근법  
(Combined  
Approach)

### 3. 위험 평가

#### 접근방식에 따른 방법 정의

##### 기준선 접근법(Baseline Approach)

- 모든 시스템에 대하여 **보호의 기본수준**을 정하고 이를 달성하기 위한 일련의 보호대책 선택
- 시간과 비용이 많이 들지 않고, 모든 조직에서 **기본적으로 필요한 보호대책의 선택** 가능
- 조직 내에 **부서별로** 적정 보안수준보다도 높게 혹은 낮게 보안통제 적용

### 3. 위험 평가

#### 접근방식에 따른 방법 정의

##### 전문가 판단법(Informal Approach)

- 전문가의 지식과 경험에 따라 위험 분석
- 작은 조직에서 비용 효과적
- 위험을 제대로 평가하기가 어렵고 보호대책의 선택 및 소요비용을 합리적으로 도출하기 어려움
- 계속적으로 반복되는 보안관리의 보안감사 및 사후관리가 제한됨

### 3. 위험 평가

#### 접근방식에 따른 방법 정의

##### 상세위험 접근법(Detailed Risk Approach)

- 자신의 가치를 측정하고 자산에 대한 위협의 정도와 취약성을 분석하여 위협의 정도를 결정함
- 조직 내에 **적절한 보안수준 마련 가능**
- 전문적인 **지식, 시간, 노력이 많이 소요됨**



### 3. 위험 평가

#### 접근방식에 따른 방법 정의

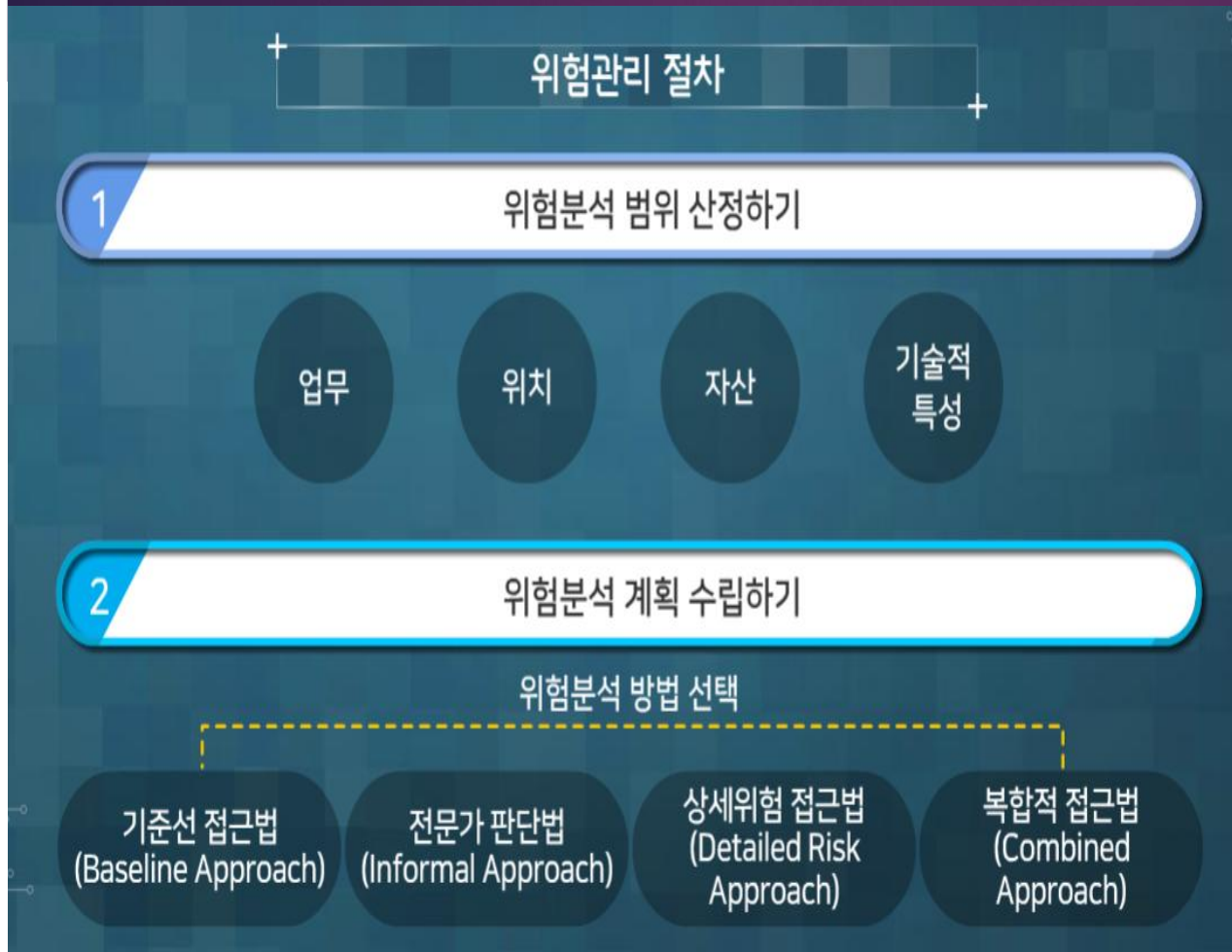
##### 복합적 접근법(Combined Approach)

- 먼저 조직 활용에 대한 필수적인, 위험이 높은 시스템을 식별하고 이러한 시스템에는 '상세위험 접근법'을 그렇지 않은 시스템에는 '기준선 접근법' 등을 각각 적용
- 보안전략을 빠르게 구축할 수 있고, 시간과 노력을 효율적으로 활용 가능
- 두 가지 방법의 적용대상을 명확하게 설정하지 못함으로써 자원의 낭비가 발생할 수 있음

### 3. 위험 평가

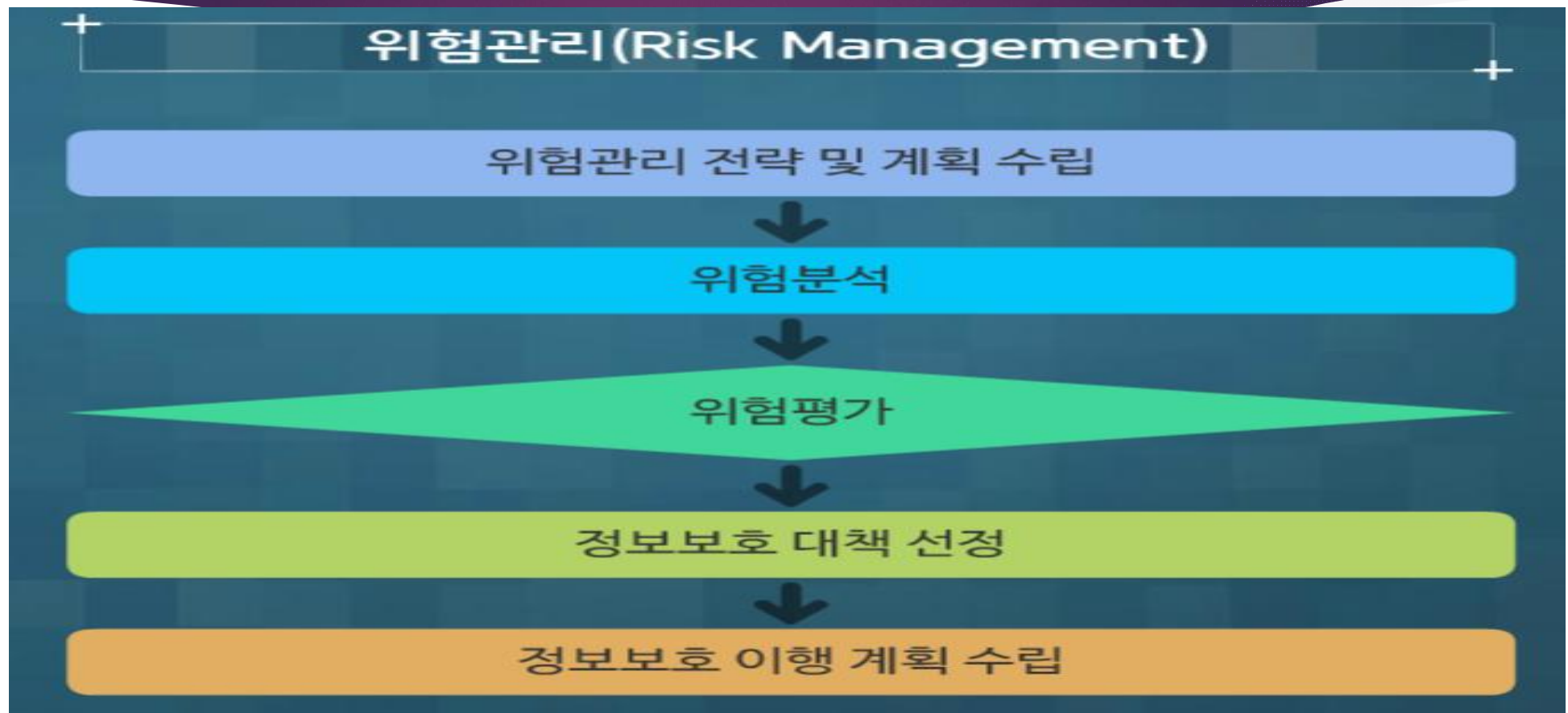
- ▶ 대표적으로 4가지의 평가 접근 방법을 살펴 보았다.
- ▶ 최근에는 **복합적 접근 방법**이 가장 많이 사용되고 있다.

### 3. 위험 평가



- ▶ 지금껏 일련의 과정을 정리해보자
- ▶ 1. 위험관리 계획을 수립하기 위해 위험도를 구별 하였다.
- ▶ 2. 위험 관리 선정
- ▶ 3. 산정된 계획으로 위험 분석을 하였다.
- ▶ 평가 도출된 방법으로 보호 대책을 수립해보자.

## 4. 보호 대책 선정





## 4,5. 보호대책 선정 및 보호대책 수립

### 위험평가 단계

정보 자산별 위험 분석 결과 도출

정보보호 위원회 구성(정보보호 최고 책임자 참여)

수용 가능한 위험수준 결정

관리되어야 할 위험 통제 방안 마련

조직의 수용 가능한 위험수준(DoA)

## 4,5. 보호대책 선정 및 보호대책 수립.

### DoA에 따른 위험처리 방안

위험수용

위험모니터링

위험감소

위험회피

위험전가

# 위험 관리 하는 방법

- 위험 수용: 현재의 위험을 받아들이고 잠재적 손실 비용을 간수하는 것을 말함. 어떠한 대책을 도입하더라도 위험을 완전히 제거할 수는 없으므로, 일정수준 이하의 위험은 감수하고 사업을 진행하는 것
- 위험모니터링: 잠재위험으로 주변 환경의 변화에 따라 위험요인으로 변화가 가능하므로 지속적인 모니터링을 실시함. DoA 주변의 위험도가 위험 모니터링 대상이 될 수 있음
- 위험감소: 직접적인 피해가 발생할 수 있는 중대한 위험을 잠재하고 있어 정보보호대책을 선택하여 구현하는 것
- 위험회피: 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것
- 위험 전가: 보험이나 외주 등으로 잠재적 비용을 제3자에게 이전하거나 할당하는 것

▶ 위험 관리 과정은 자산의 식별과 중요도평가 ,  
개인정보 흐름도 작성,위험평가 (현황분석,취약점 평가) 로 이루어진다.

▶ 허용 위험수준은 위험을 조치하기 위한 기준으로 DoA 가 넘는 위험의 경우 위험감소등 조치를 취하고 DoA  
이하의 위험의  
경우 위험 수용을 하게 됩니다.

▶ 위험 분석은 평가 하는 과정이다.

관리 하는 방법 이 아니다 !!!!

# 정리 하며 생각해보자.

## ▶ 1. 위험 관리 하는 이유

## ▶ 2. 위험관리 시 내부계획 수립 각 업무와,자산,환경에 맞게.....

## ▶ 3. 위험도 분석

정량적 분석

정성적 분석

## ▶ 4. 위험 평가 방법


기준선 접근법

전문가 판단법

상세 위험접근법

복합적 접근법

## ▶ 5. 위험 관리



부족 하고 미흡하실수 있겠지만  
성실히 조사하여 작성 하였습니다.  
잘못된 내용은 피드백 주시면 즉시 수정 하도록 하겠습니다.  
감사합니다.