클라우드 서비스 위험 관리

QA를 통한 보안, 품질, 성능 수준 유지

클라우드 산업 육성 유공 장관 표창

한국소비자만족지수 1위

대한민국 서비스만족 대상

5년 연속 랭키닷컴 선정 IDC분야 1위

코리아서버호스팅은 보다 차별화된 유지관리로 기업과 개인의 전략적 파트너가 되겠습니다.
본사 : 서울시 서초구 서초대로250 3층 (스타갤러리브릿지 빌딩) / 전산실IDC : 서울시 서초구 법원로1길 6 SK브로드밴드 IDC 센터
TEL : 02-593-8320 FAX : 02-6264-8321

KS클라우드

소개

- ㈜코리아서버호스팅 전략사업본부 본부장

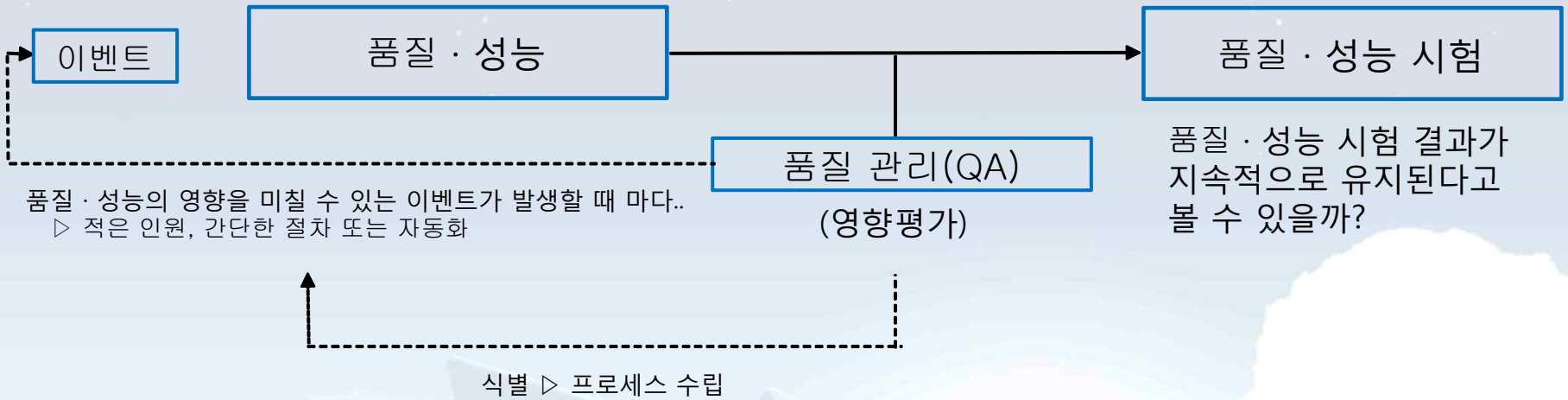
  KS클라우드 서비스 및 운영 PM
  클라우드 보안 인증, 정보보호관리자
  Microsoft CSP BPM

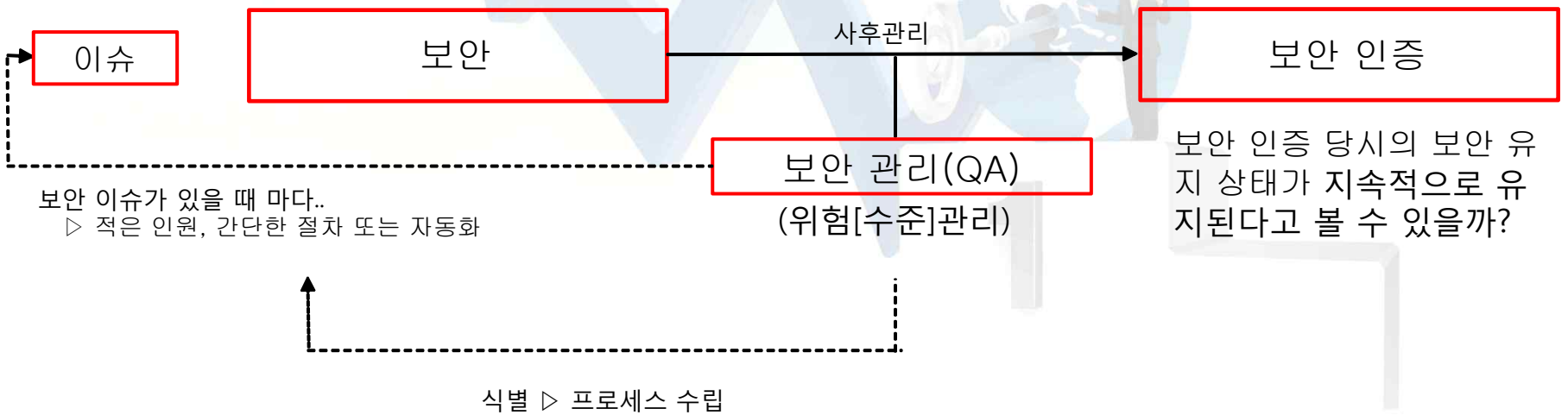
- IITP R&D 연구과제 클라우드 자문단 자문위원
- 클라우드 상호운용성 협의체 위원
- 클라우드 품질·성능 고시안 개정 연구반 포럼
- 클라우드 서비스 실증 연구반
- 상명대학교 일반대학원 공학석사과정

  국내 클라우드 정책 현황과 클라우드 해외 진출 정책 방안
  (2018년 대한안전경영과학회 춘계 학술대회)

- 이메일 : cloud@ksidc.net

영향 평가, 위험관리를 통한 QA (품질보증) 절차를 서비스에 반영


이벤트
품질 · 성능
품질 · 성능 시험
품질 관리(QA)
(영향평가)
품질 · 성능의 영향을 미칠 수 있는 이벤트가 발생할 때 마다..
▷ 적은 인원, 간단한 절차 또는 자동화
품질 · 성능 시험 결과가 지속적으로 유지된다고 볼 수 있을까?
식별 ▷ 프로세스 수립


이슈
보안
사후관리
보안 인증
보안 관리(QA)
(위험[수준]관리)
보안 이슈가 있을 때 마다..
▷ 적은 인원, 간단한 절차 또는 자동화
보안 인증 당시의 보안 유지 상태가 지속적으로 유지된다고 볼 수 있을까?
식별 ▷ 프로세스 수립

서비스의 의미

- Who : 이용자
- What : 필요한 제품, 기능, 관리 등
- When : 필요한 때
- Where : 원하는 곳에서
- How : 필요한 만큼 사용
- Which : 사용한 만큼에 대한 비용을 지불하는 것

▷ 서비스는 항상 가용 상태여야 한다는 요구조건이 발생

서비스 환경, 품질, 성능, 보안...

업무 영향 평가

- 업무 중 발생할 수 있는 위협 요인과 업무 연속성과의 관계를 평가하여 수치화하고 등급으로 분류하여 관리

예] 클라우드 서비스 포탈기능 업데이트 / 새로운 취약점의 발견
▷ 서비스 단절의 위협이 발생 / 새로운 위협의 발생
▷ 운영, 개발, 영업, 경영지원 등 업무 식별하고 업무 가용성과 상관관계 분석
▷ 위협과 업무의 상관관계 평가를 수치화
▷ 수치화된 영향 평가를 범위에 따라 등급화
▷ 등급에 따른 대응 방안 마련

(자산) 위험 관리

- 서비스를 위한 자산을 식별하고 유사 용도 및 목적에 따라 분류한 다음, 자산의 보안성, 관리 중요도를 회사가 정한 기준에 따라 평가하고 위험 노출도를 산출한 다음 등급으로 분류하여 관리

예] 네트워크 그룹으로 분류된 백본 장비
▷ 자산의 보안성과 관리 중요도 평가의 기준 : 가용성, 무결성, 기밀성, 법적 요구사항 등
▷ 해당 자산의 보안성 및 관리 중요도와 해당 자산의 위험 발생 시 예측 피해 정도, 발생 가능 빈도 등의 상관관계
▷ 수치화된 위험 노출도를 범위에 따라 등급화
▷ 등급에 따른 대응 방안 마련

- 실증을 통한 서비스 수준 관리

  ▷ 품질, 성능 / 보안 우수성
  ▷ 고객만족
  ▷ 서비스 이미지 가치 상승
  ▷ 서비스 경쟁력, 매출 증대

- 법적 요구사항

  ▷ 클라우드 서비스 보안 인증 (CSAP) : 공공서비스 필수 요건
  ▷ 정보보호관리체계 인증 (ISMS) : 일정 요건 이상 기업 의무
  ▷ 기타 정보보호관련 법률의 정의

- 1회성이 아닌, 이벤트 마다 반복 · 지속 관리

CSAP 통제항목 요약 (IaaS)

1. 정보보호 정책 및 조직
2. 인적 보안 : 내부 인력, 외부 인력, 교육
3. 자산 관리 : 식별, 변경, 시설 모니터링, 위험관리
4. 서비스 공급망을 관리 : 관리, 계약
5. 침해사고 관리 : 대응체계, 훈련, 보고, 처리, 복구, 사후관리
6. 서비스 연속성 관리
   : 장애 대응, 보고, 처리, 복구, 재발 방지, 가용성, 이중화, 백업, 연속성 (영향평가)
7. 준거성 : 법적 요구사항, 보안감사, 감사기록 모니터링
8. 물리적 보안
   : 물리적 보호 구역, 출입통제, 사무실 및 설비 공간, 공공장소 및 운송 하역 구역,
   모바일 기기, 배치, 설비, 케이블, 반출입, 유지보수, 폐기
9. 가상화 보안
   : 자원 관리, 자원 모니터링, Hypervisor 보안, 공개 서버 보안, 상호 운용성 및 이식성, 악성코드 통제,
   인터페이스 및 API,데이터 이전, 가상 소프트웨어 보안
10. 접근통제 : 정책, 권한 관리
11. 네트워크 보안
    : 네트워크 보안 정책, 모니터링 및 통제, 운영, 암호화, 분리, 무선 접근통제
12. 데이터 보호 및 암호화 : 분류, 소유권, 무결성, 보호, 추적성, 폐기, 저장매체 관리, 이동 매체 관리, 암호화 관리
13. 시스템 개발 및 도입 보안
    : 보안 요구사항 정의, 인증 및 암호화 기능, 보안 로그, 접근 권한, 시각 동기화, 구현 및 시험, 개발과 환경 분리,
    시험 데이터 보안, 외주 개발 보안, 시스템 도입 계획, 시스템 인수
14. 공공기관 보안요구사항
    : 보안 서비스 수준 협약, 전산 장비 안정성, 보안 관리 수준, 사고 및 장애 대응, 물리적 보호조치, 물리적 위치 및 분리,
    중요 장비 이중화 및 백업 체계, 검증필 암호화 기술, 보안관제 제반 환경 지원

상세 위험 접근법과 기준선 접근법

- 상관관계 등 위험을 평가하여 내부 기준을 수립하기 위한 접근법

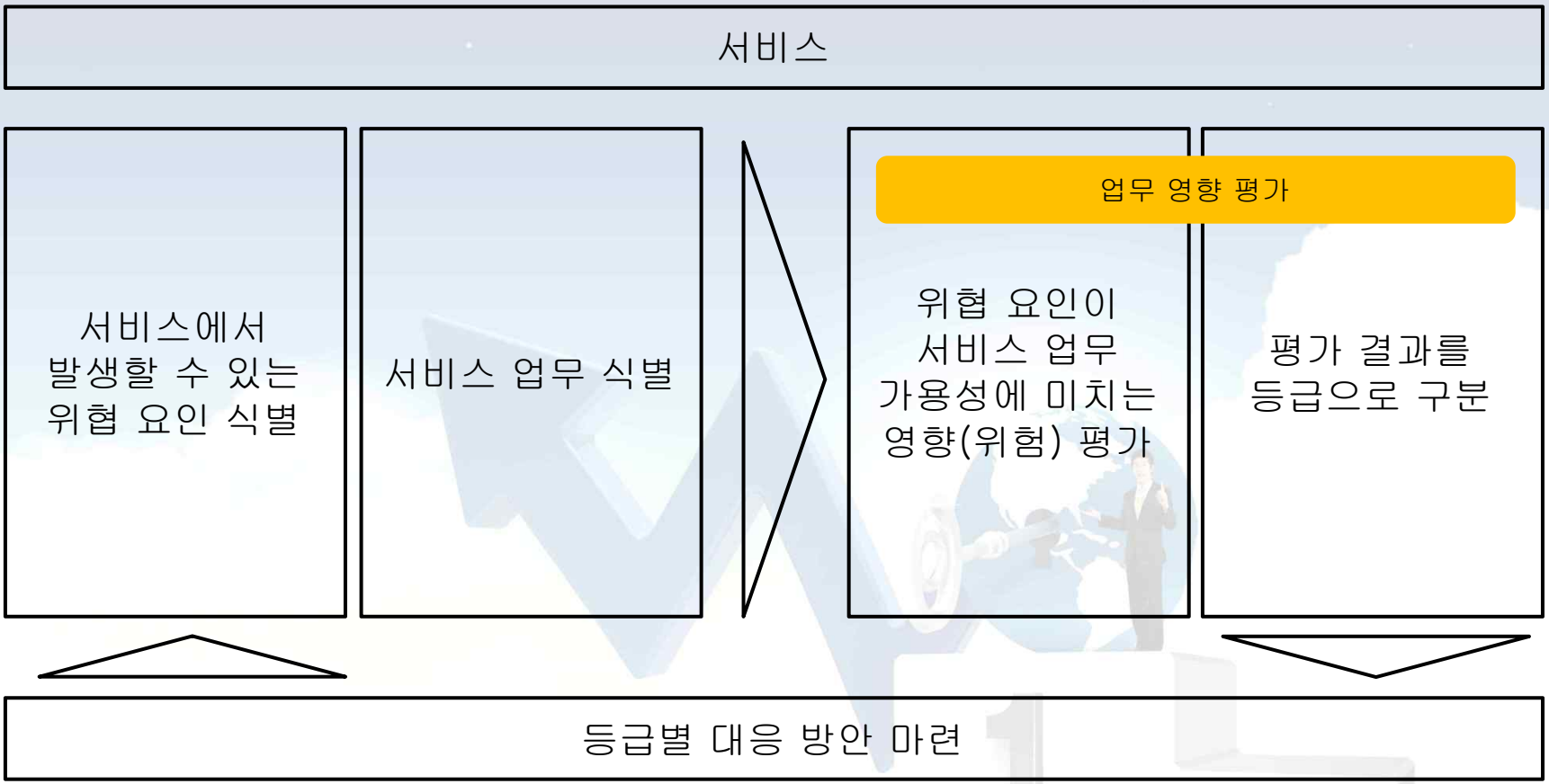
기준선 접근법

- 기준선 접근법은 정보시스템에 대하여 보호의 기본 수준을 정하고 이를 달성하기 위하여 일련의 보호대책을 선택하는 방법
- 시간이 많이 들지 않고 모든 조직에서 기본적으로 필요한 보호대책의 선택이 가능하다.
- 조직의 특성을 고려하지 않았기 때문에, 조직 내에 부서별로 적정 보안수준보다 높게 혹은 낮게 보안 통제가 적용 될 수 있는 단점이 있다.

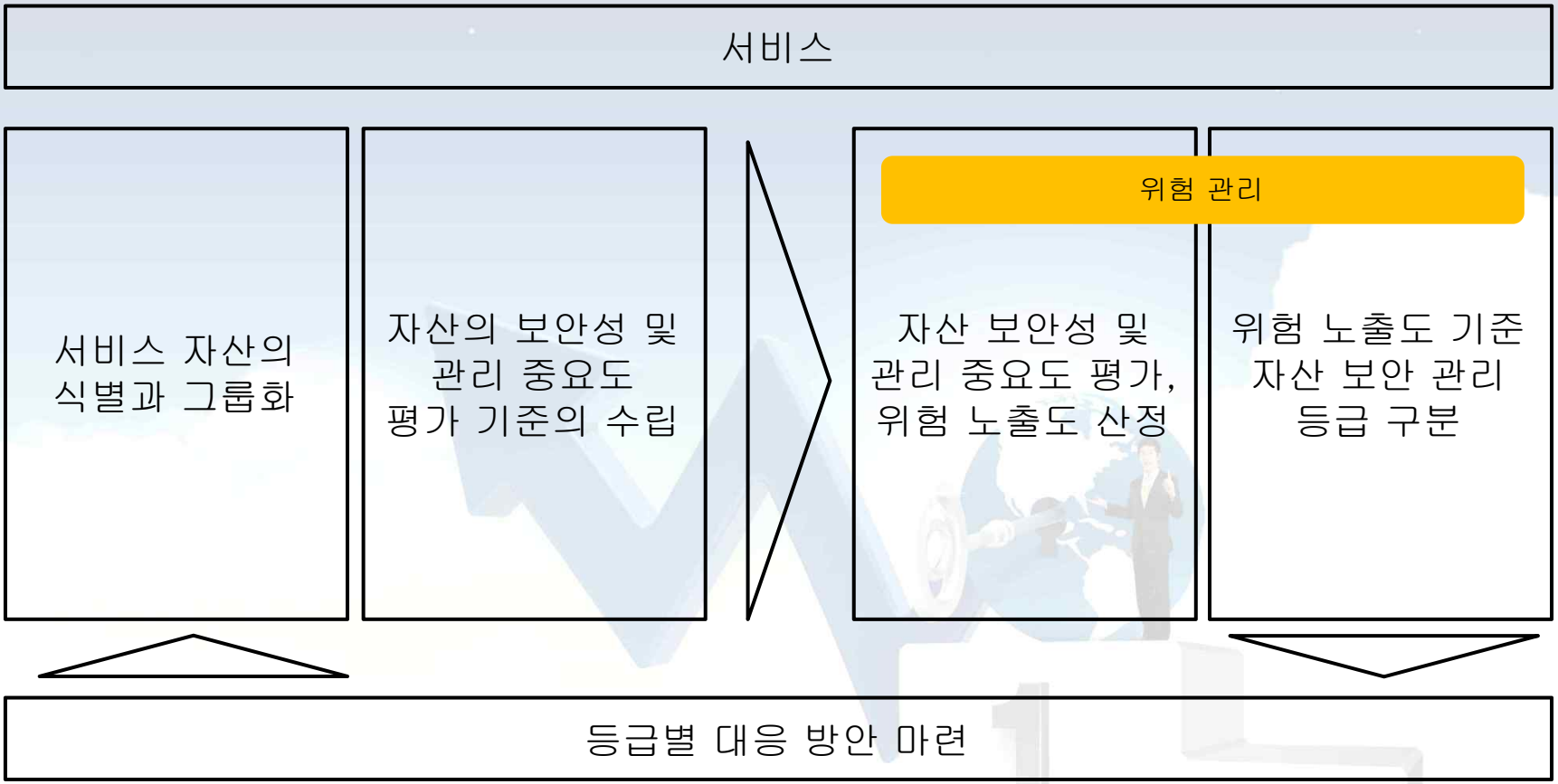
상세 위험 접근법

- 상세 위험 접근법은 자산의 가치를 측정하고 자산에 대한 위협의 정도와 취약성을 분석하여 위험의 정도를 결정하는 방법
- 조직 내에 적절한 보안 수준 수립이 가능하다.
- 전문적인 지식과 시간과 노력이 많이 소요되고, 그 결과가 항상 객관적이거나 정확한 것은 아니라는 단점이 있다.

업무 영향 평가


서비스
서비스에서 발생할 수 있는 위협 요인 식별
서비스 업무 식별
업무 영향 평가
위협 요인이 서비스 업무 가용성에 미치는 영향(위험) 평가
평가 결과를 등급으로 구분
등급별 대응 방안 마련

(자산) 위험 관리


서비스
서비스 자산의 식별과 그룹화
자산의 보안성 및 관리 중요도 평가 기준의 수립
위험 관리
자산 보안성 및 관리 중요도 평가, 위험 노출도 산정
위험 노출도 기준 자산 보안 관리 등급 구분
등급별 대응 방안 마련

발생할 수 있는 위협 요소로부터 업무 연속성 관리

◎ 위협의 식별

취약점 도구
소스코드점검도구
운영 통계, 로그, 경험

→ 위협 요소 식별 → 연관성을 고려 Grouping

[영향 평가]

◎ 업무 연관성

서비스 관련 업무 식별 → 업무 연속 실패 시 영향

→ 금전적 영향
→ 비금전적 영향

◎ 영향 평가 결과

영향도에 따라 등급화
(위협이 위험으로 등급화)
→ 수용 가능한 위험 수준의 식별
→ 위험의 처리
(등급에 따른 위험 조치)

※ 보통 중급, 상급은 조치

클라우드 서비스 자산의 위험 관리

KS클라우드

◎ 자산의 식별

서비스를 구성하는 모든 자산의 식별 → 연관성을 고려하여 자산의 Grouping → 보안 요구사항, 관리 중요도 평가

- 가용성,
- 기밀성,
- 무결성,
- 법적 요구사항

◎ 위험 시나리오의 작성 및 평가

우려사항

기술적 위험
(취약점 도구 등)

→ 위험 시나리오 →

보호 대책의 수립
(관리, 통제 등의 지침)

[위험 수준 평가]

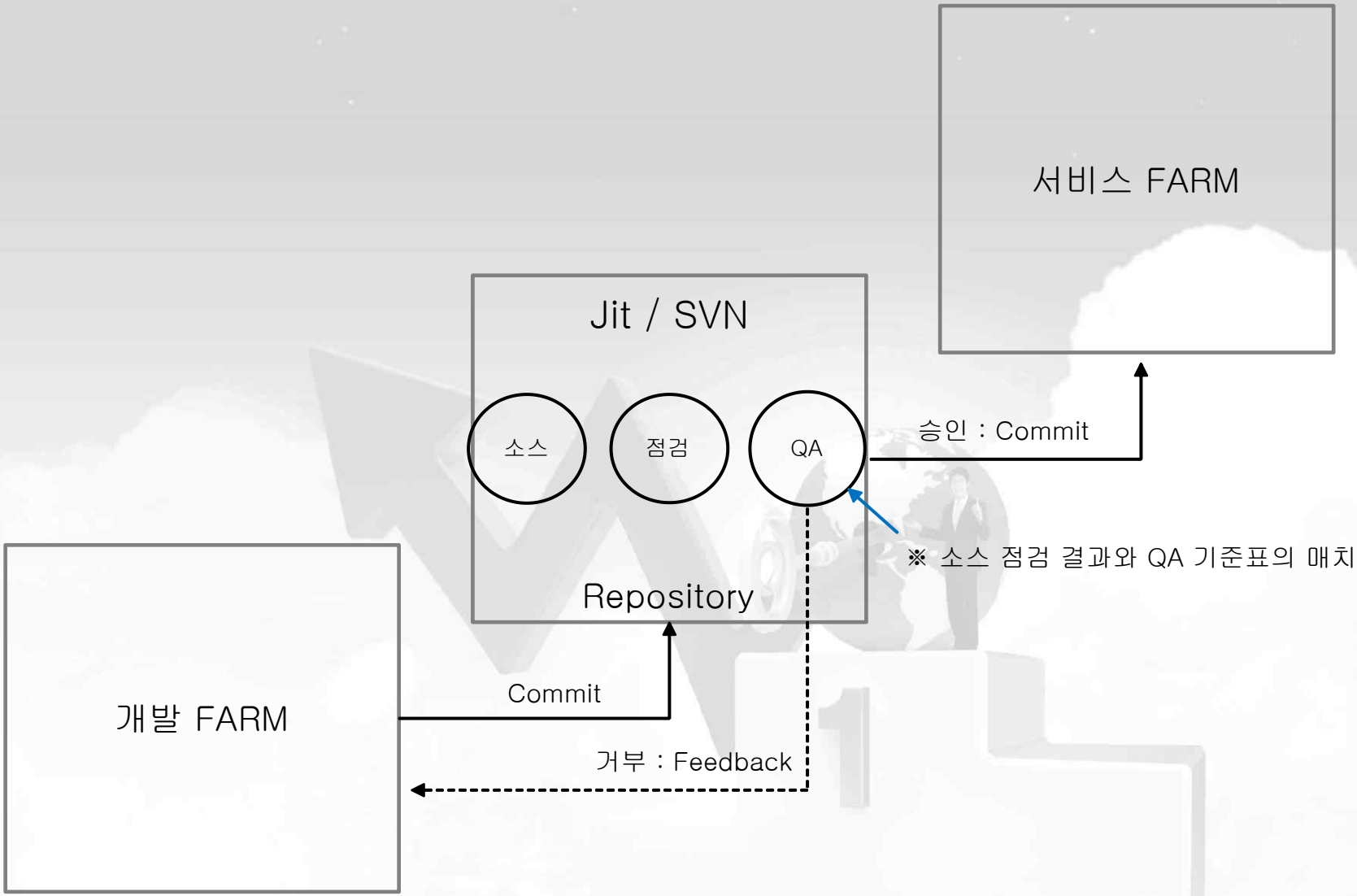
기존 보호 대책의 평가

◎ 위험 수준 평과 결과

위험도에 산정에 따라 등급화 → 수용 가능한 위험 수준의 식별 → 위험의 처리
(등급에 따른 위험 조치)

※ 보통 중급, 상급은 조치

※ 노출위험도(ERV) = (우려사항 값 – (우려사항 값 x 기존 보호대책 값)) x 2
※ 위험도 = 자산 보안등급 + 노출위험도


서비스 FARM
Jit / SVN
소스
점검
QA
승인 : Commit
※ 소스 점검 결과와 QA 기준표의 매치
Repository
개발 FARM
Commit
거부 : Feedback

Thank you!

클라우드 산업 육성 유공 장관 표창

한국소비자만족지수 1위

대한민국 서비스만족 대상

5년 연속 랭키닷컴 선정 IDC분야 1위

코리아서버호스팅은 보다 차별화된 유지관리로 기업과 개인의 전략적 파트너가 되겠습니다.
본사 : 서울시 서초구 서초대로250 3층 (스타갤러리브릿지 빌딩) / 전산실IDC : 서울시 서초구 법원로1길 6 SK브로드밴드 IDC 센터
TEL : 02-593-8320 FAX : 02-6264-8321

KS클라우드