클라우드 환경에서 보안의 중요성

이건복
마이크로소프트


Microsoft
Linux

클라우드에서 보안의 중요성과 혜택

클라우드 기반 보안의 장점

94%

온프레미스에서
구축하기 어려웠던
보안표준의 장점의 활용

62%

클라우드로 이전하여
이전보다 향상된 데이터
프라이버시 보호를 운영

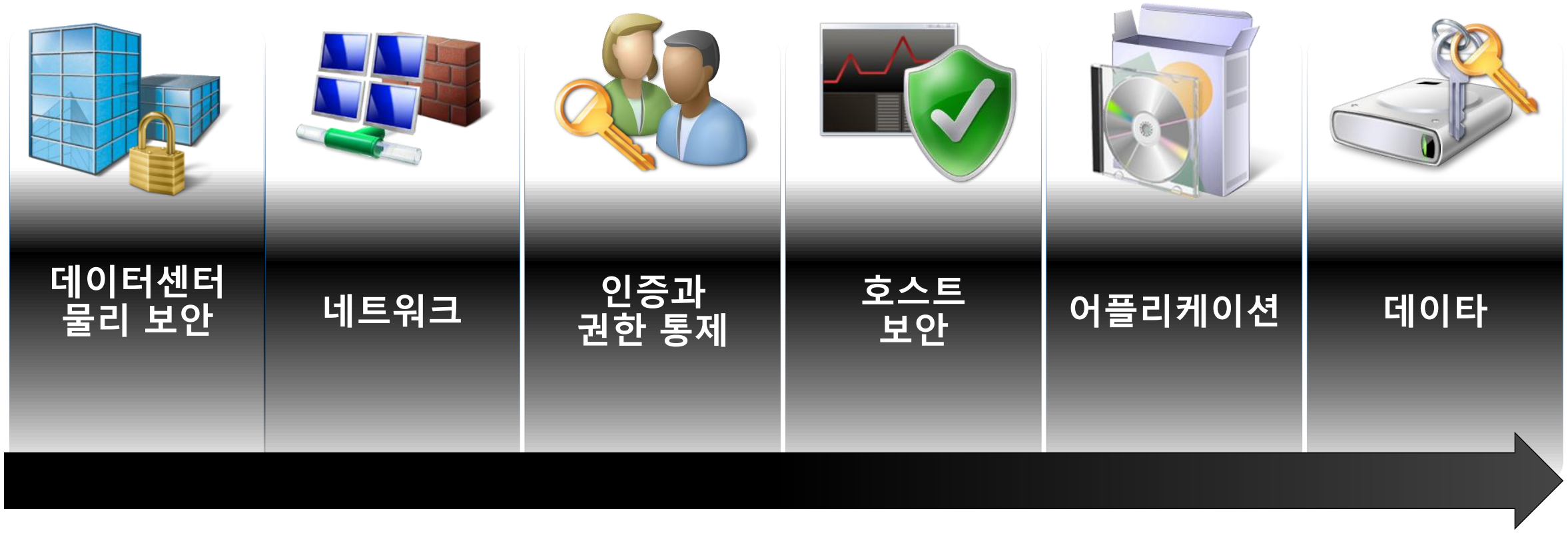
보안

- Design/Operation
- Infrastructure
- Network
- Identity/access
- Data

프라이버시

표준인증

클라우드 보안 영역



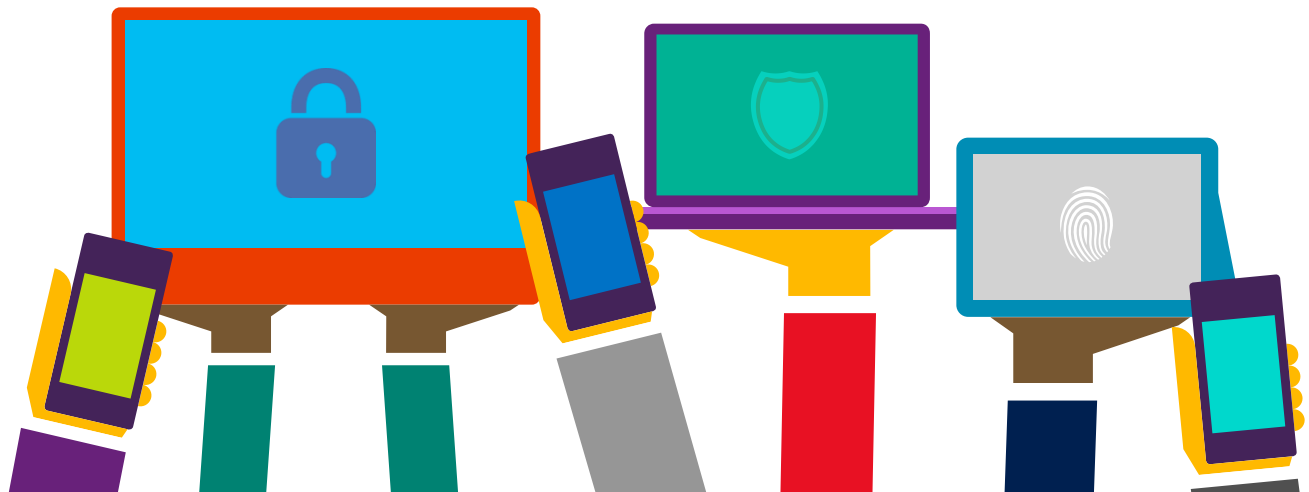
데이터 센터 물리적 보안

서비스 보안은 완벽한 데이터 센터 보안에서 시작

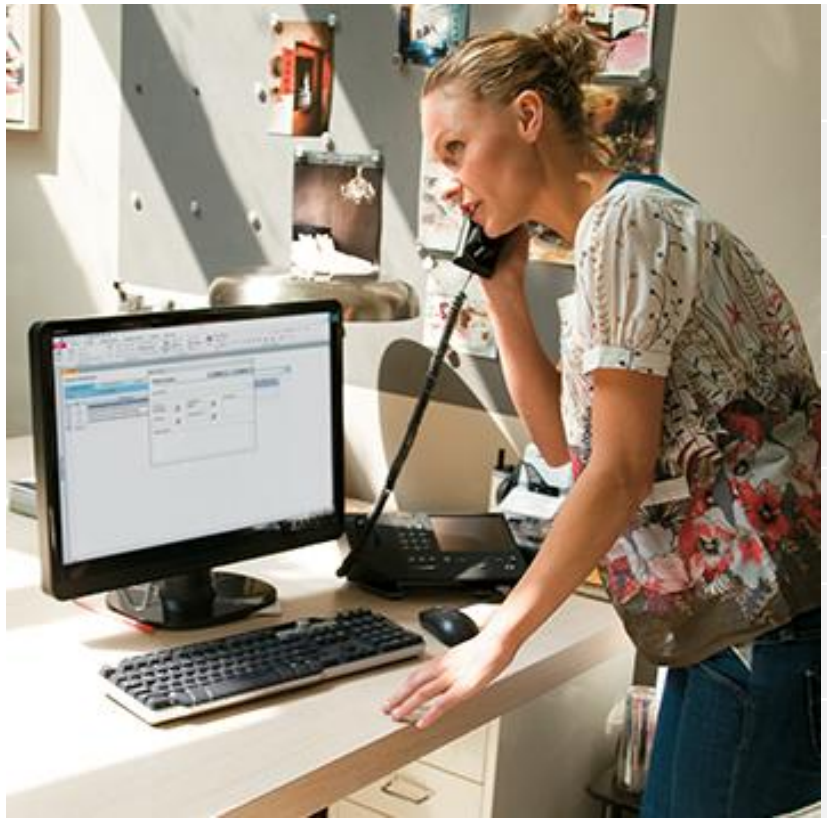
- 24 x 7 물리적 접근 통제
- 동작 감시기
- 생체정보 기반 시설 접근 통제
- 24시간 감시 카메라 가동
- 물리적 침입 탐지

보안의 핵심

Software Development Lifecycle (SDL)	운영환경에 대한 보안 제어	Assume breach	사고의 대응



Infrastructure 보호



- 24시간 모니터링 및 물리적 보호
- 시스템 모니터링 및 로깅
- 긴급 수정 관리
- Anti-Virus/Anti-Malware 보호
- 침입탐지 /DDoS
- 침투 테스트 (Penetration Test)
- 정부 데이터의 분리 (예: US정부)

네트워크 보호

분리된 네트워크

암호화된 연결

가상 네트워크

별도의 인터넷 연결성

계정 인증과 접근

- 기업용 클라우드 인증
- 접근 모니터링
- Single sign-on
- Multi-Factor Authentication
- Role based access 제어

데이터의 보호

- 암호화된 데이터 전송
- 데이터 저장 시 암호화 옵션
- 데이터의 구분
- 데이터 저장 위치에 대한 선택
- 데이터 가용성
- 데이터의 파기

클라우드에서 데이터 프라이버시

클라우드에서 데이터 프라이버시

디자인 단계에서의 프라이버시 적용	계약상의 규제	제한된 데이터 접근 및 사용	광고용도로의 데이터 사용

계약상의 규정 준수

EU Data Privacy Approval

- EU 고객의 데이터 보호 규정
- EU Data Privacy의 마이크로소프트 데이터전송 허용
- 오직 마이크로소프트만이 EU Article 29 승인

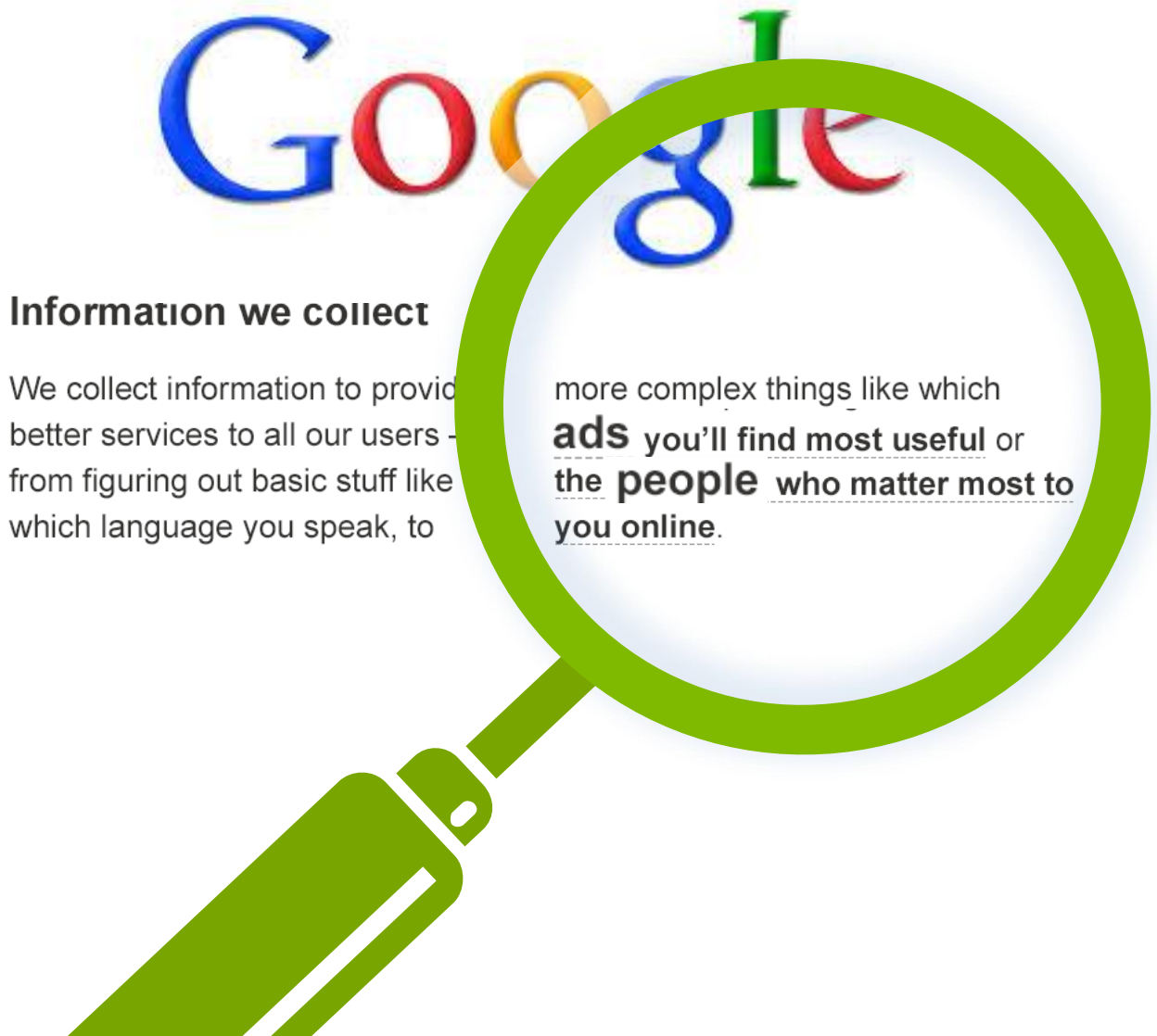
데이터 프라이버시 보호

- 규제 인증: HIPAA BAA, Data Processing Agreement, & E.U. Model Clauses
- 기업의 데이터 보호에 대한 규제의 해결방안으로 제시

제한된 사용과 접근

광고목적의 데이터 접근의 차단

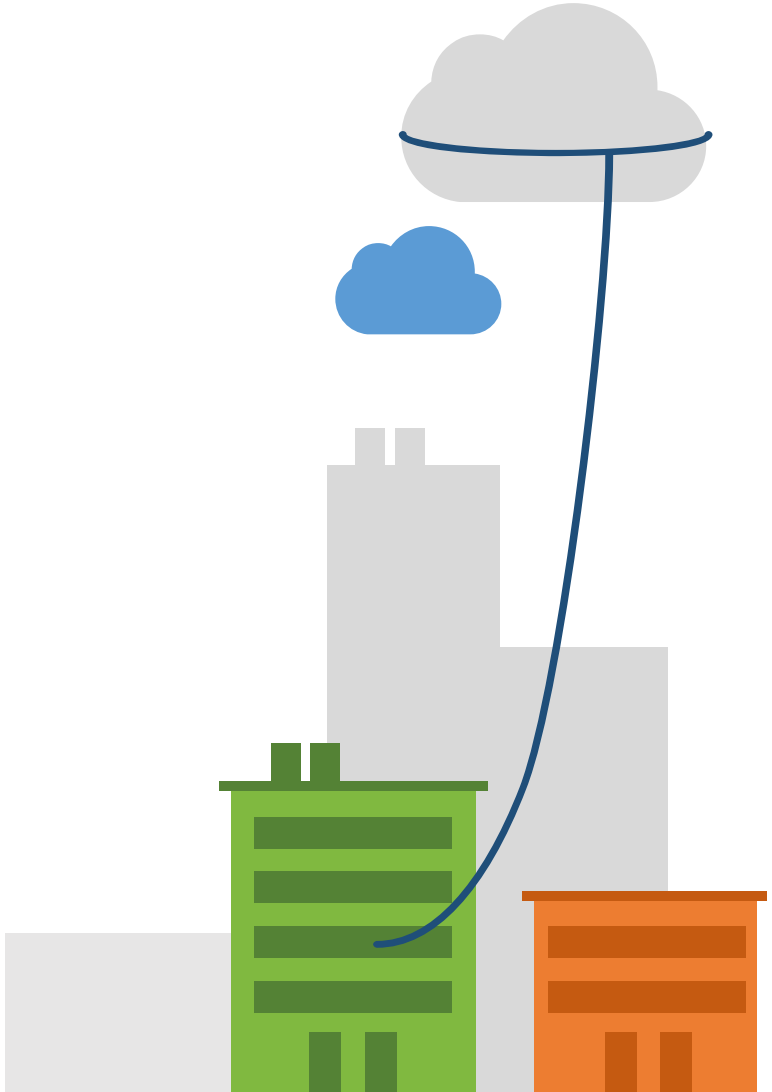
고객의 데이터의 공유의 차단



클라우드 보안 관련 인증

클라우드 보안 Compliance

정보보안 표준	보안 제어	정부 및 산업표준
ISO 27001 ISO 27002 ISO 27018	SOC 1 Type 2 SOC 2 Type 2	FedRAMP/FISMA PCI DSS Level 1 UK G-Cloud HIPAA/HITECH



클라우드관련 보안 인증 리스트

ISO / IEC 27001 / 27002 / 27018 Certification

SSAE 16/ISAE 3402 attestations
(SOC 1 Type 2, SOC 2 Type 2, and SOC 3)

CSA(Cloud Security Alliance) CCM(Cloud Control Matrix)
HIPAA BAA

PCI Data Security Standard Certification

FISMA Certification and Accreditation

Various State, Federal, and International Privacy Laws
(95/46/EC—aka EU Data Protection Directive; California SB1386; etc.)

CCCPPF (China Cloud Computing Promotion and Policy Forum)
UK G-Cloud OFFICIAL
Australia IRAP
Singapore MTCS

http://azure.microsoft.com/en-us/support/trust-center/compliance/

주요 IT 규제 인증의 의미

규제 항목	설명
ISO/IEC 27001	• 국제표준기구의 인증으로 미국뿐만 아니라 전세계에서 적용되는 클라우드 보안에 대한 산업표준. • 14개국 5개의 국제기구를 통하여 수립 • 정보보호, 통신, 운영, 접근통제, 정보 보호사고 대응에 대한 14개 영역 114개 항목 평가 • 매년 감사 및 표준준수 여부 시행
US-EU Safe Harbor Framework	• 미국-유럽연합 데이터 보호지침으로 개인정보 수집, 사용 및 보유기준에 부합하도록 미국 상무부에서 정한 프레임워크 • 미국 기업이 EU영역밖으로 게인정보를 수집 전송시 EU의 보호지침을 준수하도록 함.
HIPAA BAA	• 건강보험 양도 및 책임에 대한 법안 • 2003년 의료 및 프라이버시 보호를 대폭 강화하는 법안. 당사자의 허락없이 개인의 의료기록이나 건강상태등을 공표할 수 없다.
SOC (Service Organization Control)	• 미국공인회계사협회(AICPA)에서 발급하는 인증체계로 재무정보에 대한 규제 • SOC I (SSAE16) 기업의 재무 보고를 위한 정보 및 관리 시스템 등 종합적인 내부통제를 평가하는 인 증으로 감사 결과보고서는 기업 내부 및 감사 관련 조직 등 제한된 사람들에게만 공유 • SOC II 개인정보보호 시스템, 조직/관리시스템 등 기업의 종합적인 내부통제를 평가하는 인증 으로 클라우드 서비스, 데이터 센터 등의 출현으로 서비스 인증 체계가 마련됐다. 감사 결과보고서는 제한된 사람들에게만 공개
FISMA (Federal Information Security Management Act)	• 미국 연방정보 보안관리법 • 미국 연방 정부 정보시스템의 보안 강화를 위해 정부 정보보안개혁법과 이를 승계한 연방정보보안관리법을 통해 적정 보안조치를 취하지 않은 부처는 예산을 삭감토록 해 강력한 정책 집행의 기반을 마련했다

http://azure.microsoft.com/ko-kr/support/trust-center/services/

ISO/IEC 27018

- 2014년 7월에 발표
- 클라우드에 저장 된 민감한 고객정보(특히 개인식별정보, PII)의 보호, 보안 리스크 실행방안의 평가 및 가이드라인

• 고객의 명시적 동의를 얻지 못했다면, 고객 데이터를 광고 또는 마케팅 목적으로 사용해 서는 안 된다. 또한 고객이 사업자에게 광고 또는 마케팅 목적에 사용될 개인정보를 제공 하지 않아도 클라우드 서비스를 이용할 수 있어야 한다.

• 고객 데이터가 어디에 저장되고, 어떻게 활용되는지 투명하게 공개해야 한다.

• 고객 데이터가 어떻게 사용될지에 대한 통제권을 고객에게 부여해야 한다.

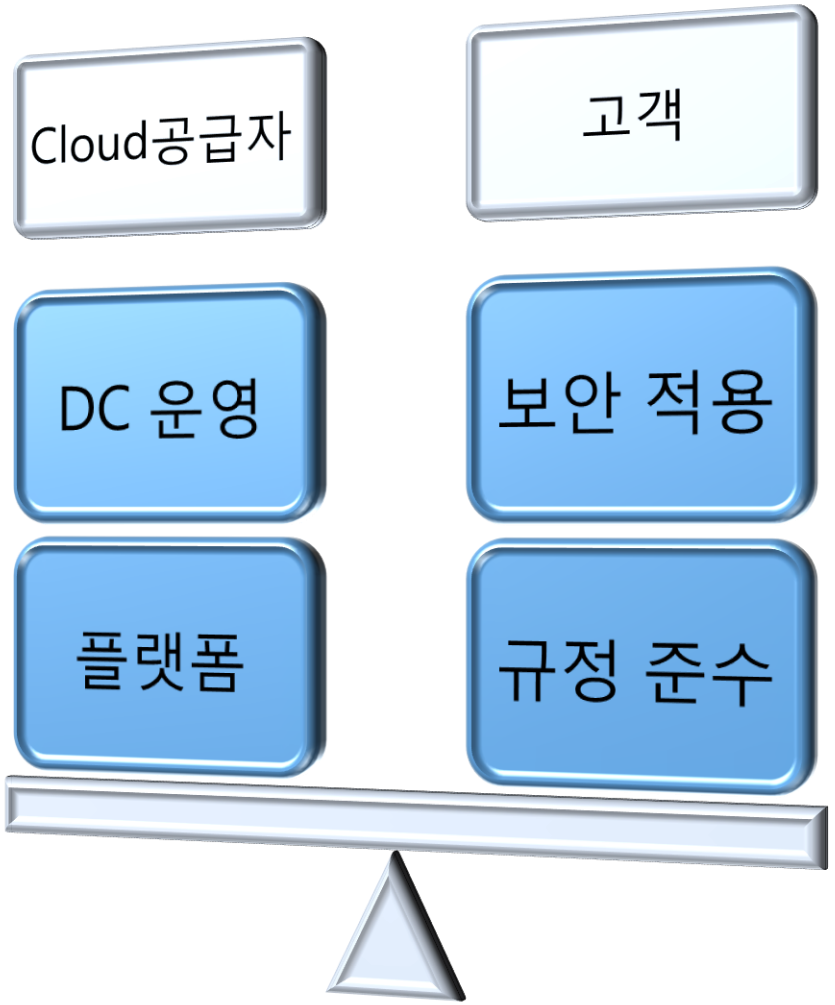
• 고객 데이터의 수집 및 삭제 관련 정책을 고객에게 고지해야 한다.

• 고객 데이터에 영향을 주는 위반 사항 또는 사고가 발생하면 반드시 고객에게 그 내용과 사후 조치내역을 알려줘야 한다.

• 서비스 제공자는 매년 법령 준수 여부에 대해 제3의 독립적 기관의 외부감사를 받아야 한다.

Public 클라우드의 책임구분

- 일반적인 운영 원칙
  - 국가별 법률 요건 및 산업의 법률 요건의 다양성
  - *공통적*으로 적용할 수 있는 일반 운영 원칙 하에 서비스 제공
- 클라우드 사업자의 책임
  - 고객의 보안, 개인 정보 및 규정 준수
- 고객 서비스의 보안 준수
  - 응용 프로그램, 데이터 콘텐츠, 가상 컴퓨터, 액세스 자격 증명등을 포함한 특정 환경에 대한 책임



공동책임(Shared Responsibility)의 사례