클라우드 보안 국제표준과 개인정보

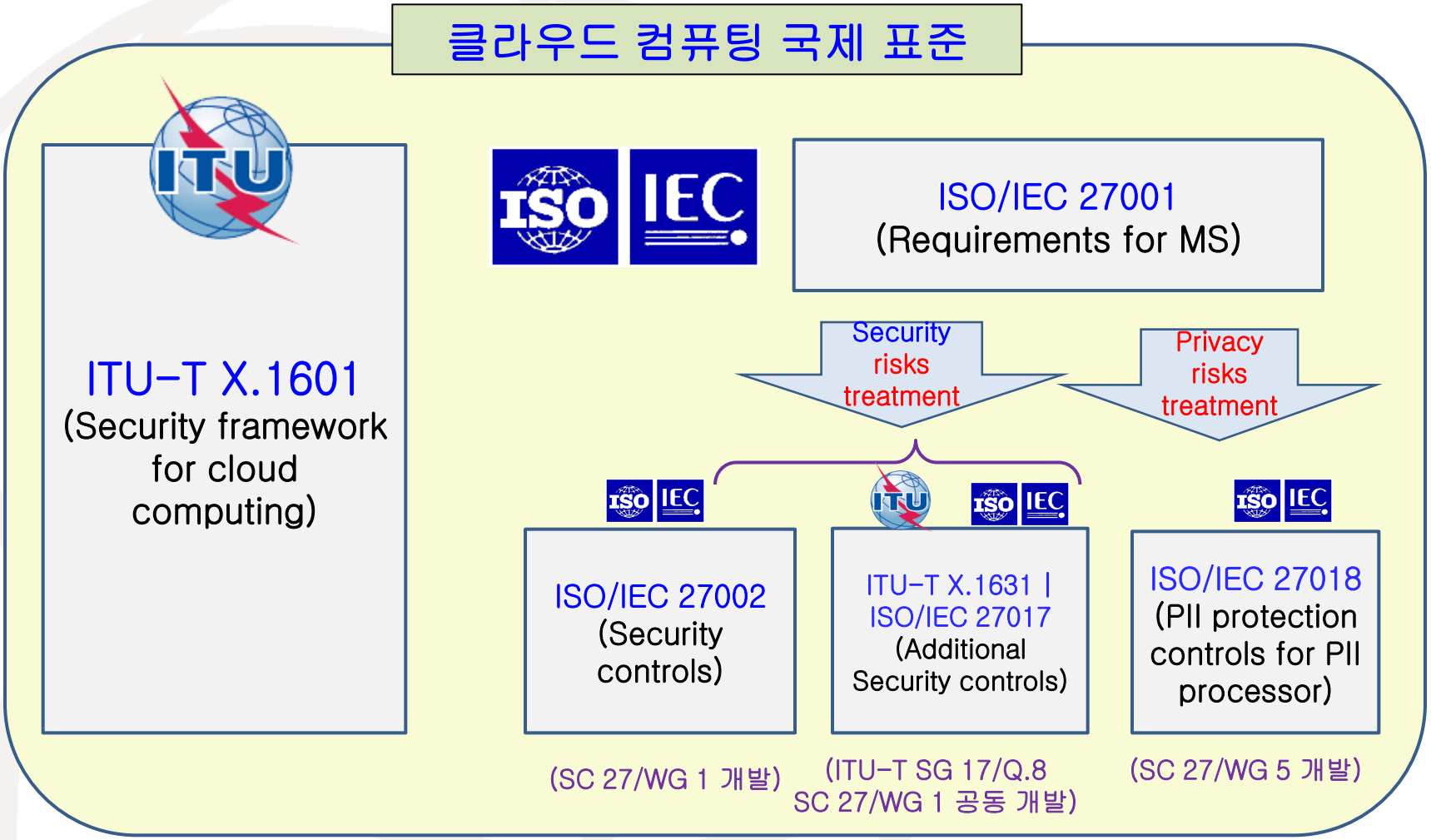
2016.09.28.

염흥열

순천향대학교 정보보호학과 교수

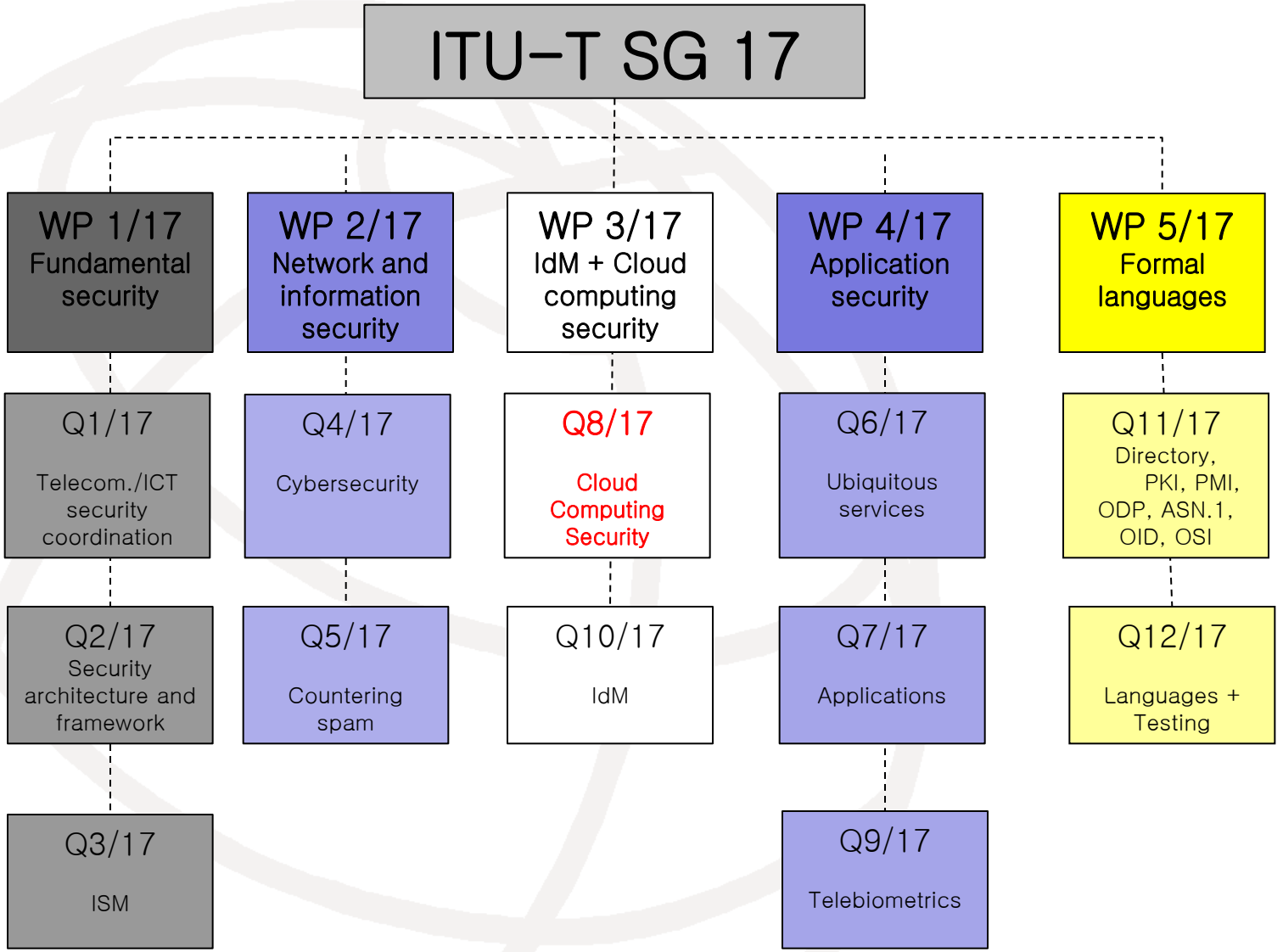
ITU-T SG17 부의장

클라우드 컴퓨팅 관련 대표 국제 표준



ITU-T SG17 국제표준화 현황

ITU-T SG17, 정보보호



연구과제 8/17 – 클라우드 보안

- 현재 4 국제 표준 채택
  - X.1601, X.1602, X.1631, X.1642
- 현재 개발중인 권고
  - X.1641(X.CSCDataSec), Guidelines for cloud service customer data security
  - X.dsms, Data security requirements for the monitoring service of cloud computing
  - X.SRIaaS, Security requirements of public infrastructure as a service (IaaS) in cloud computing – 2016.03 SG17 회의에서 신설된 워크아이템
- SG13, ISO/IEC JTC 1/SC 27, SC 38, Cloud Security Alliance 와 긴밀하게 협조하고 있음

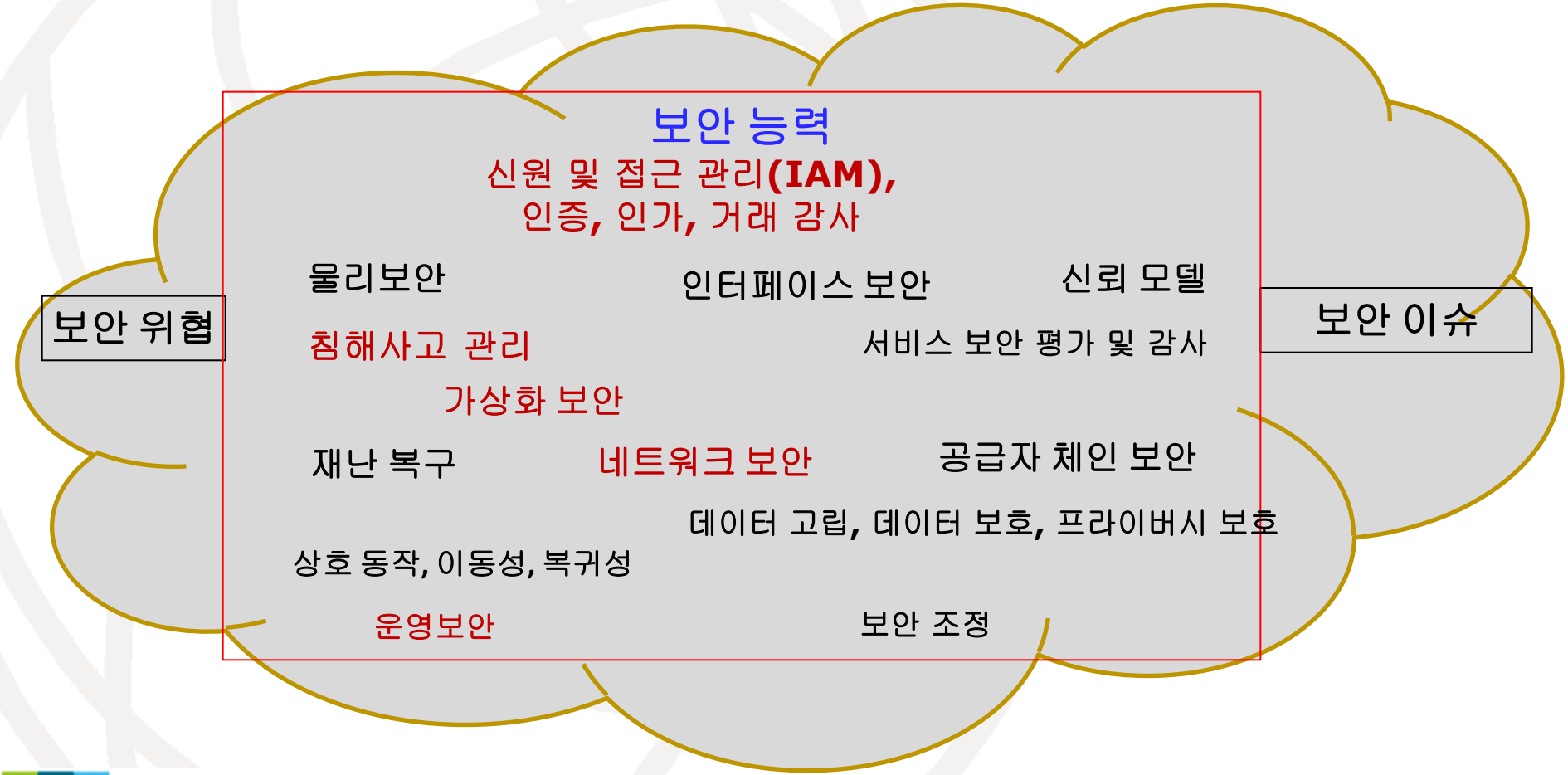
연구과제 8/17 – 채택된 국제 표준

- X.1601, Security framework for cloud computing, 2015.10.
- X.1602, Security requirements for software as a service application environments, 2016.03.
- X.1631|ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services, 2015.07.
- X.1642, Guidelines of operational security for cloud computing, 2016.03.

연구과제 8/17 표준화 구조

ITU-T X.1601 개요

- ITU-T X.1601: 클라우드 컴퓨팅 보안 프레임워크



ISO/IEC SC27 국제표준화 현황

ISO/IEC JTC 1/SC 27 작업반 역할

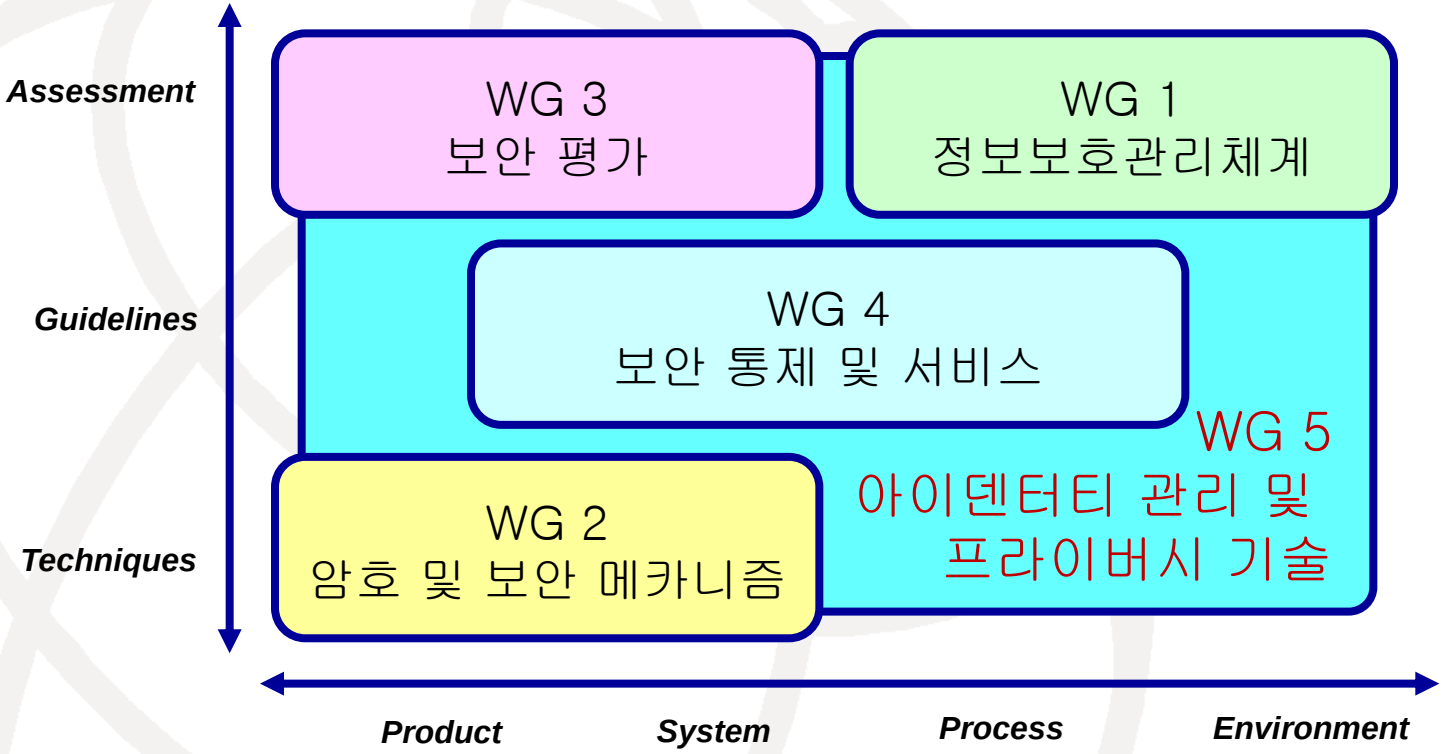
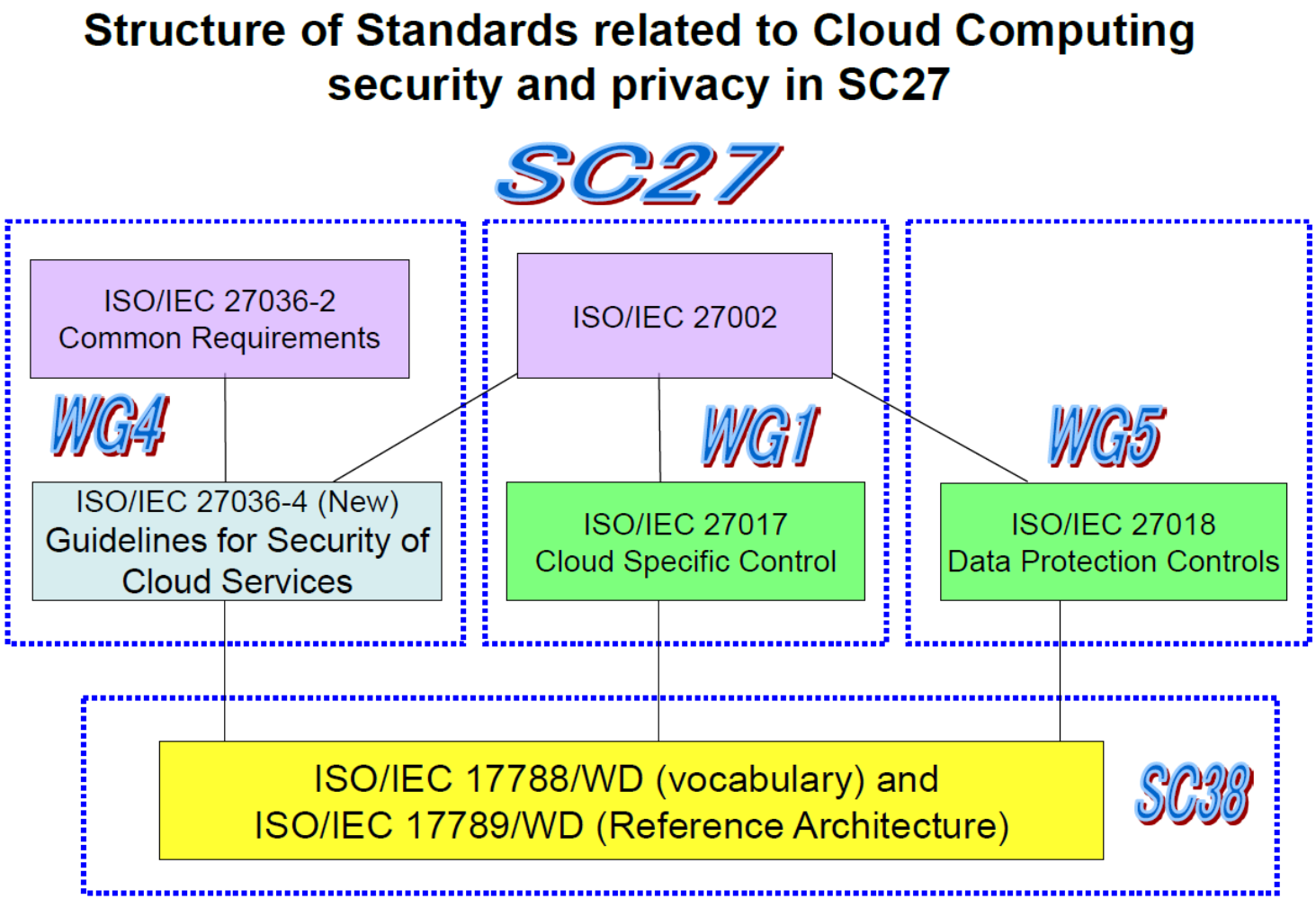


Figure by Jan Schallaböck, Vice-Convenor WG5

클라우드 컴퓨팅 보안 표준 현황 – ISO/IEC JTC 1/SC 27



ISO/IEC 27009 – 섹터 특화 ISMS

Sector-specific standard(s) using ISO/IEC 27009 requirements

e.g. privacy-specific standards

Sector-specific requirements standard (additional / refined / interpreted)

e.g. refined ISO/IEC 27001 requirement on the assessment of privacy impacts into the risk assessment process

And / Or

Sector-specific controls standard (additional / modified)

e.g. privacy controls on fundamental rights in addition to the ISO/IEC 27002 controls

Sector-specific ISMS

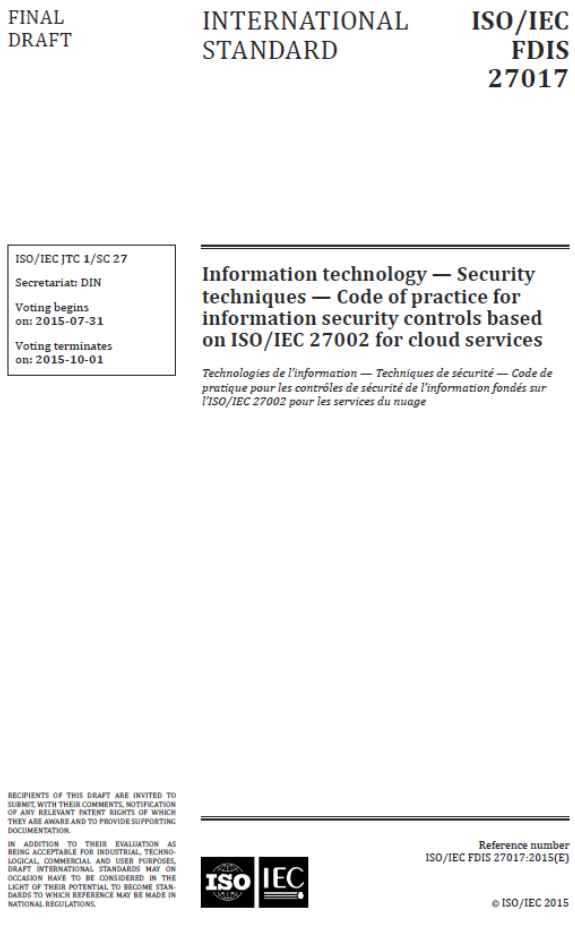
(based on the implementation of ISO/IEC 27001 and sector-specific standards)

e.g. privacy-specific ISMS

From ISO/IEC DIS 27009, IS 변경됨

ISO/IEC 27017 개요

- 표준 제목
  - 클라우드 서비스를 위한 ISO/IEC 27002 기반 정보보호 통제 지침 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services)
- 필요성
  - 클라우드 서비스 이용 증가
  - 클라우드 서비스 고객의 보안 우려 감소시킬 필요 있음
  - ISO/IEC 27002 이외 추가 보안 통제 개발 필요
- 개발 의도
  - 클라우드 서비스 사업자가 보안 통제의 적용을 통한 신뢰 부여 가능



FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 27017

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Voting begins on: 2015-07-31

Voting terminates on: 2015-10-01

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Technologies de l'information — Techniques de sécurité — Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number ISO/IEC FDIS 27017:2015(E)

© ISO/IEC 2015

published in 2015/11

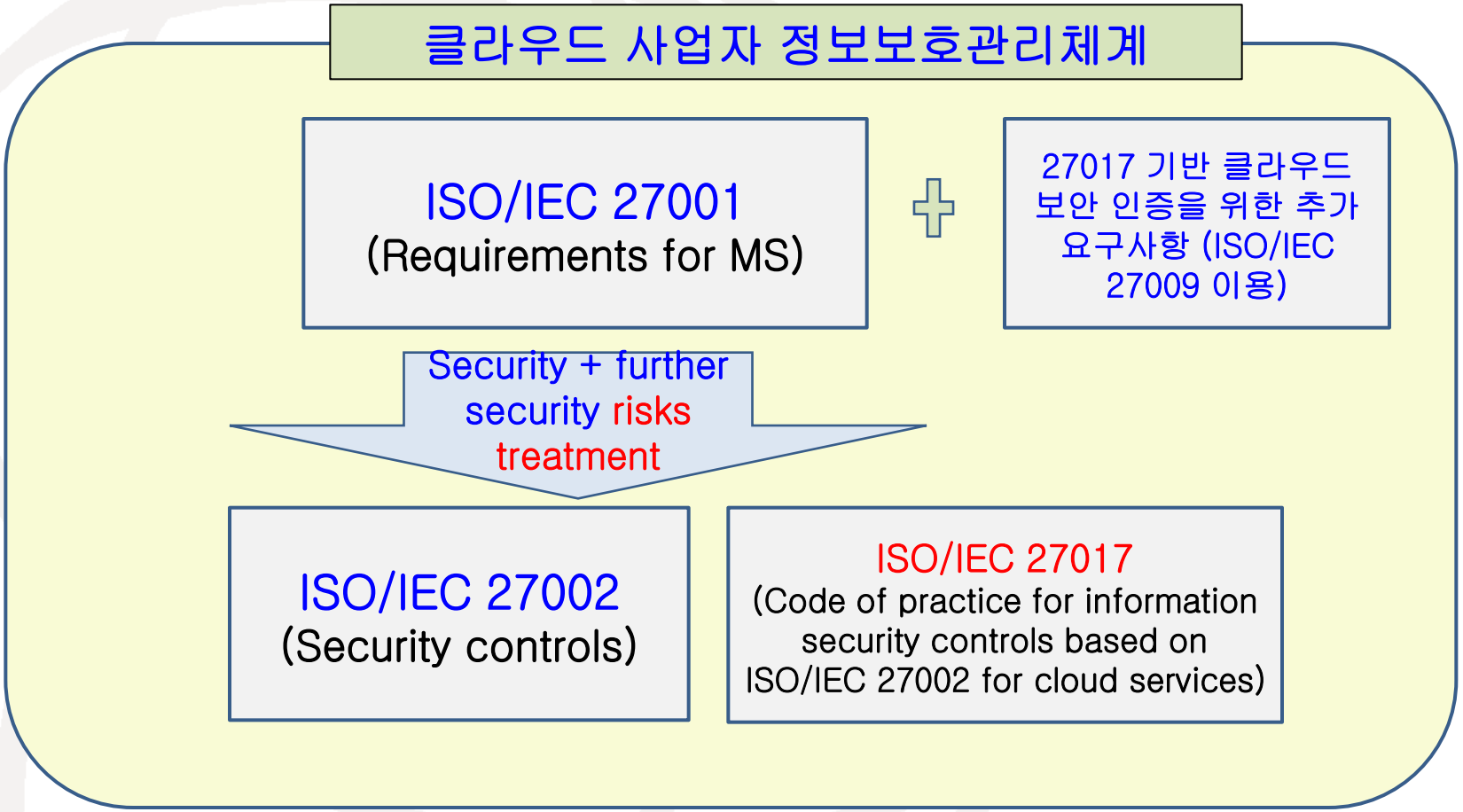
표준 범위

- 표준 개발 목적
  - 클라우드 서비스 제공과 이용을 위한 추가 보안 통제 제공
  - 클라우드 서비스 이용자와 클라우드 서비스 제공자를 위한 보안 통제 제공
- ISO/IEC 27002 에 주어진 보안 통제에 더해, 클라우드 서비스 고객을 위한 추가 구현 가이던스/추가 통제+ 클라우드 서비스 제공자를 위한 추가 구현 가이던스/추가 통제 제공
- 적용 대상
  - 모든 유형과 규모의 클라우드 서비스 제공자와 고객에 적용 가능함
  - 인증의 경우, 서비스 제공자와 고객에게 부여 가능함

ISO/IEC 27017 통제 – ISO/IEC 27002 추가

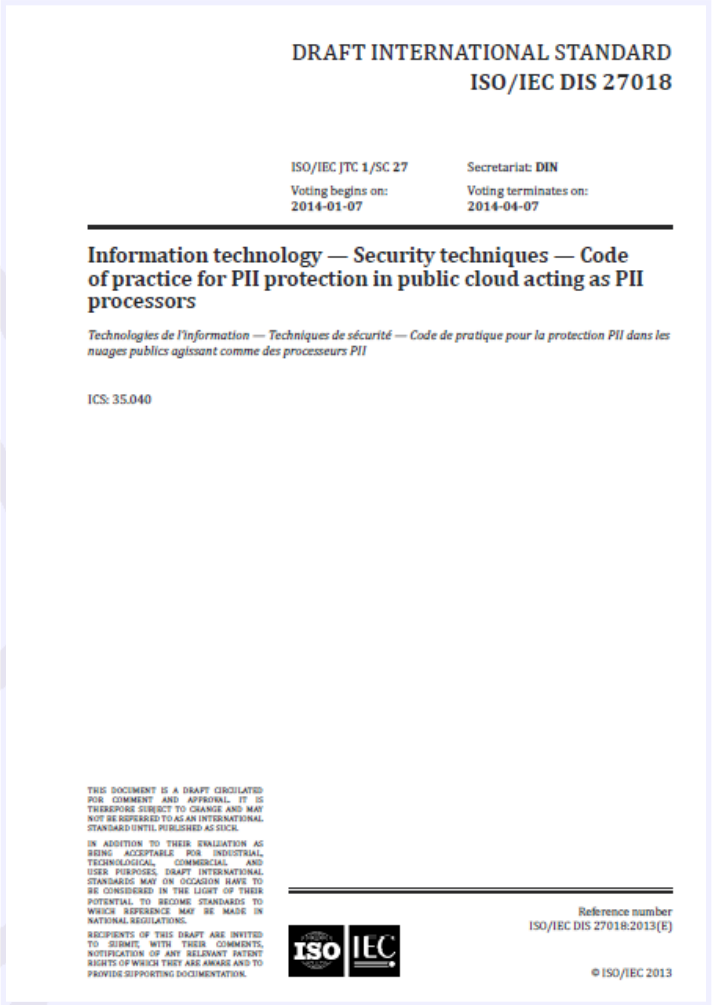
- 보안 정책 – 구현 가이던스 추가
- 정보보호 조직 –구현 가이던스 추가
- 인적 자원 보안 –구현 가이던스 추가
- 자산 관리 –구현 가이던스 추가
- 접근 통제 –구현 가이던스 추가
- 암호 –구현 가이던스 추가
- 물리 및 환경 보안 –구현 가이던스 추가
- 운영보안 –구현 가이던스 추가
- 통신 보안 –구현 가이던스 추가
- 시스템 구매, 개발 및 관리 – 구현 가이던스 추가
- 공급자 관계 –구현 가이던스 추가
- 정보보안 침해사고 관리 –구현 가이던스 추가
- 비즈니스 연속성을 위한 정보보안 측면 –구현 가이던스 추가
- 법 준수 –구현 가이던스 추가
- 부록 A (정규) – 클라우드 서비스 확장 통제 집합

클라우드 서비스 사업자 보안 보안 인증 개념
(ISO/IEC 27017 이용)



ISO/IEC 27018 개요

- 표준 제목
  - 클라우드 서비스 제공자를 위한 개인정보 보호 지침 (Code of practice for PII protection in public clouds acting as PII processors)
- 필요성
  - 클라우드 서비스 제공자에 대한 프라이버시 측면 신뢰 확보
  - 클라우드 서비스 사업자에 적용 가능한 프라이버시 기준 필요
  - ISO/IEC 27002 이외 추가 프라이버시 통제 개발 필요
- 개발 의도
  - 클라우드 서비스 사업자가 개인정보를 적절히 처리하고 있다는 확신을 주기 위한 기준



DRAFT INTERNATIONAL STANDARD
ISO/IEC DIS 27018

ISO/IEC JTC 1/SC 27 | Secretariat: DIN
Voting begins on: 2014-01-07 | Voting terminates on: 2014-04-07

Information technology — Security techniques — Code of practice for PII protection in public cloud acting as PII processors

Technologies de l'information — Techniques de sécurité — Code de pratique pour la protection PII dans les nuages publics agissant comme des processeurs PII

ICS: 35.040

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 27018:2013(E)

published in 2014/08

개인정보보호 관리체계 국제표준 개발 현황
(2012.10. 로마 SC27 회의 이후)

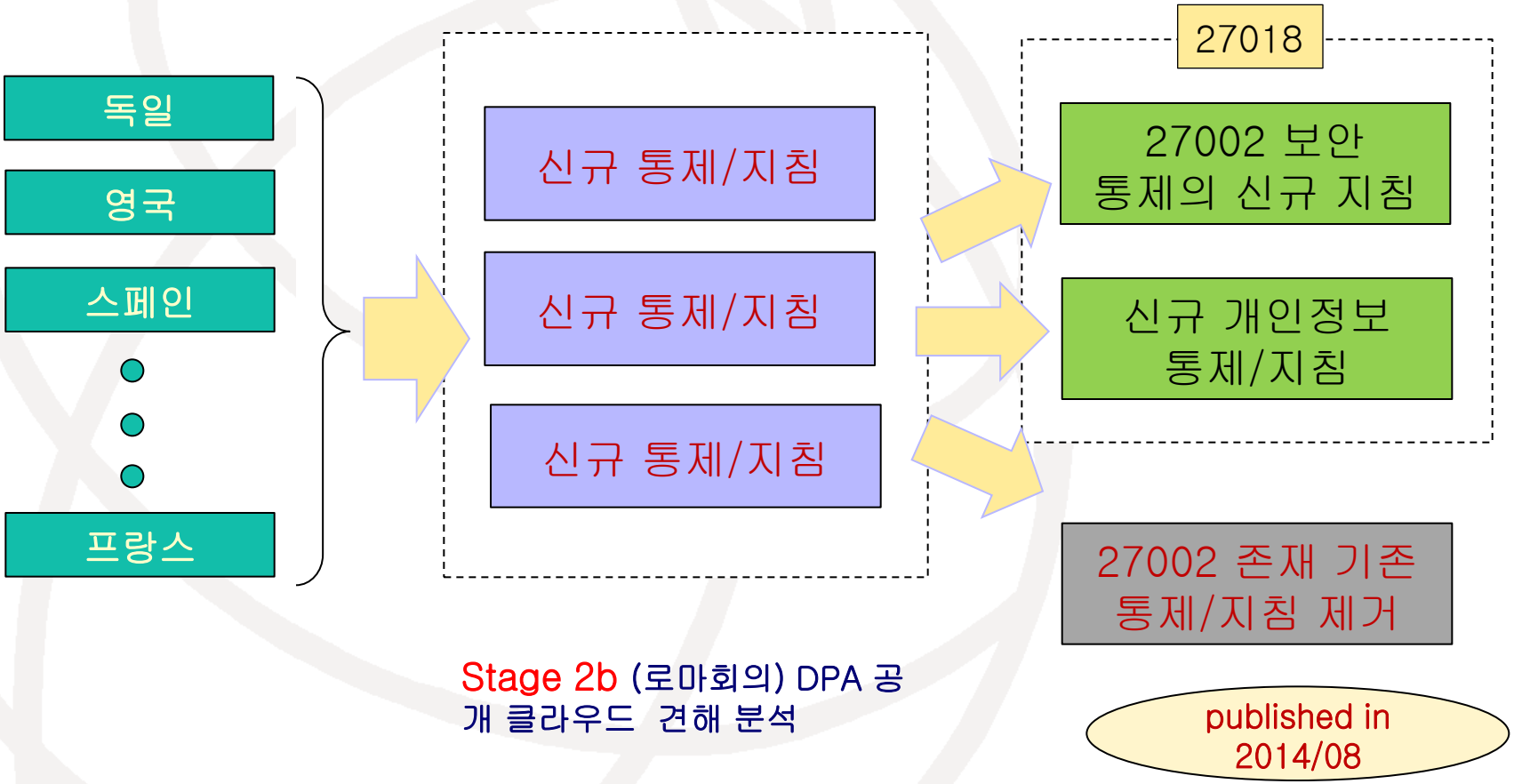
- 섹터 특화 관리체계에 대한 요구사항을 위한 별도 국제표준을 개발하지 않고 ISO/IEC 27001 이용
- ISO/IEC 27009
  - 작업반 1 개발, 섹터/응용 특화 정보보호 관리체계 – 요구사항, 섹터 ISMS 표준 생성 방법 기술
  - 현재 IS 발표됨
- ISO/IEC 29151
  - 작업반 5에서 개발 중, 개인정보보호 특화 통제
  - DIS 로 진행키로 함 (2016.4 탬퍼 SC27 회의)
- SD 5/ WG5
  - 작업반 5에서 개발 중
  - 개인정보보호관리체계를 위한 ISO/IEC 27001 이용 추가 요구사항 제시
  - PIMS 요구사항 문서 NWIP 추진 예정 (2016.04.)

ISO/IEC 27018 - 개발 과정

Stage 1. 클라우드 사업자에 적용되는 EU 법조항 분석

Stage 2a (나이로비 회의) EU 법 준수 위한 70 개 신규 통제 생성

Stage 3. 27002 존재 통제/지침 제거, 신규 통제/지침 ISO/IEC 27018에 배치

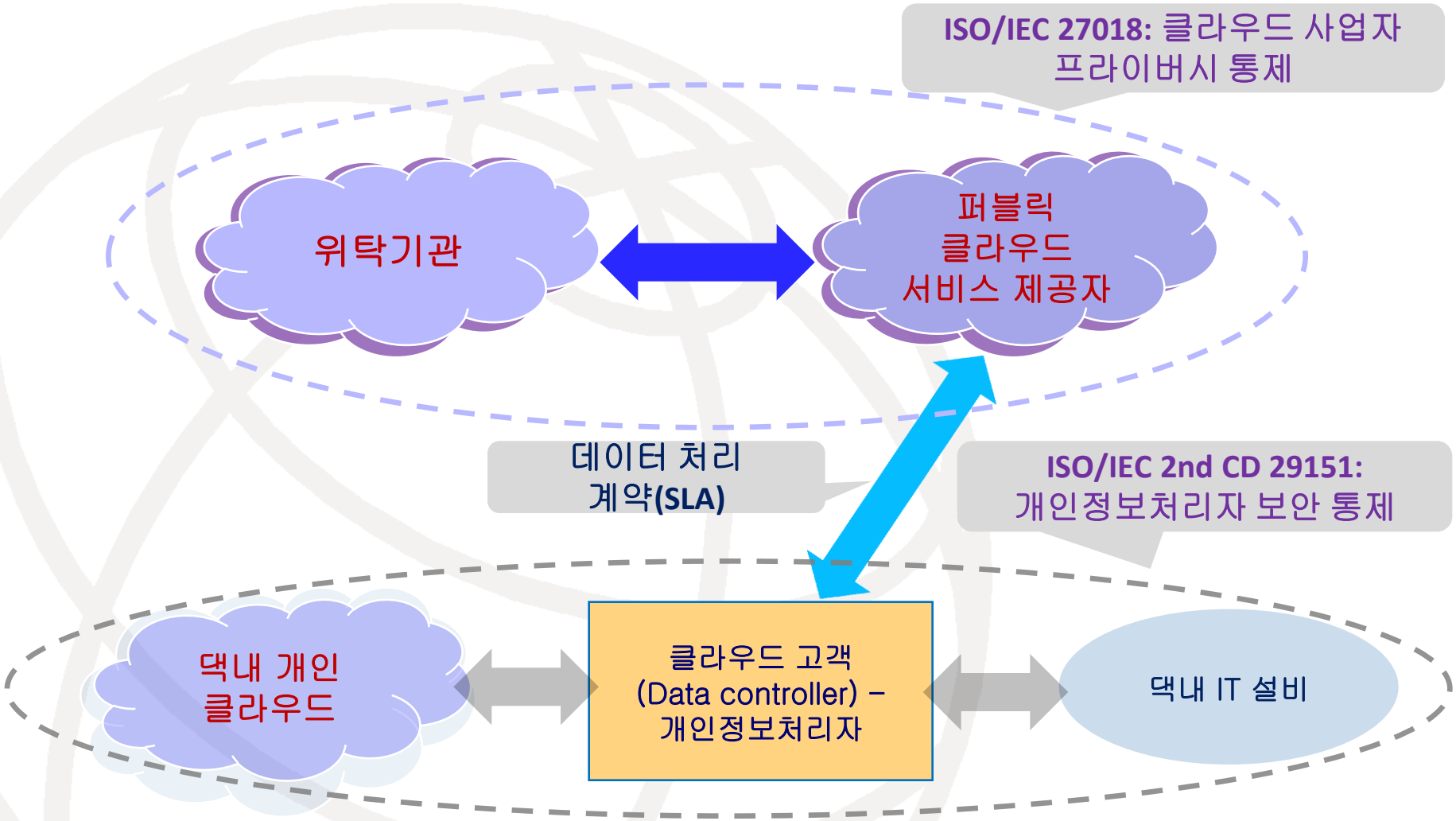


Stage 2b (로마회의) DPA 공개 클라우드 견해 분석

표준 범위

- 표준 개발 목적
  - 퍼블릭 클라우드 사업자 (PII processor) 에 적용 가능한 개인정보 통제 제공
  - 개인정보보호 요구사항(ISO/IEC 29100) 만족
- ISO/IEC 29100에서 제시한 개인정보보호 요구사항을 만족하는 통제 + ISO/IEC 27002 에 주어진 통제의 구현 지침
- 적용 대상
  - 모든 유형과 규모의 클라우드 서비스 제공자에 적용

ISO/IEC 27018 표준 적용

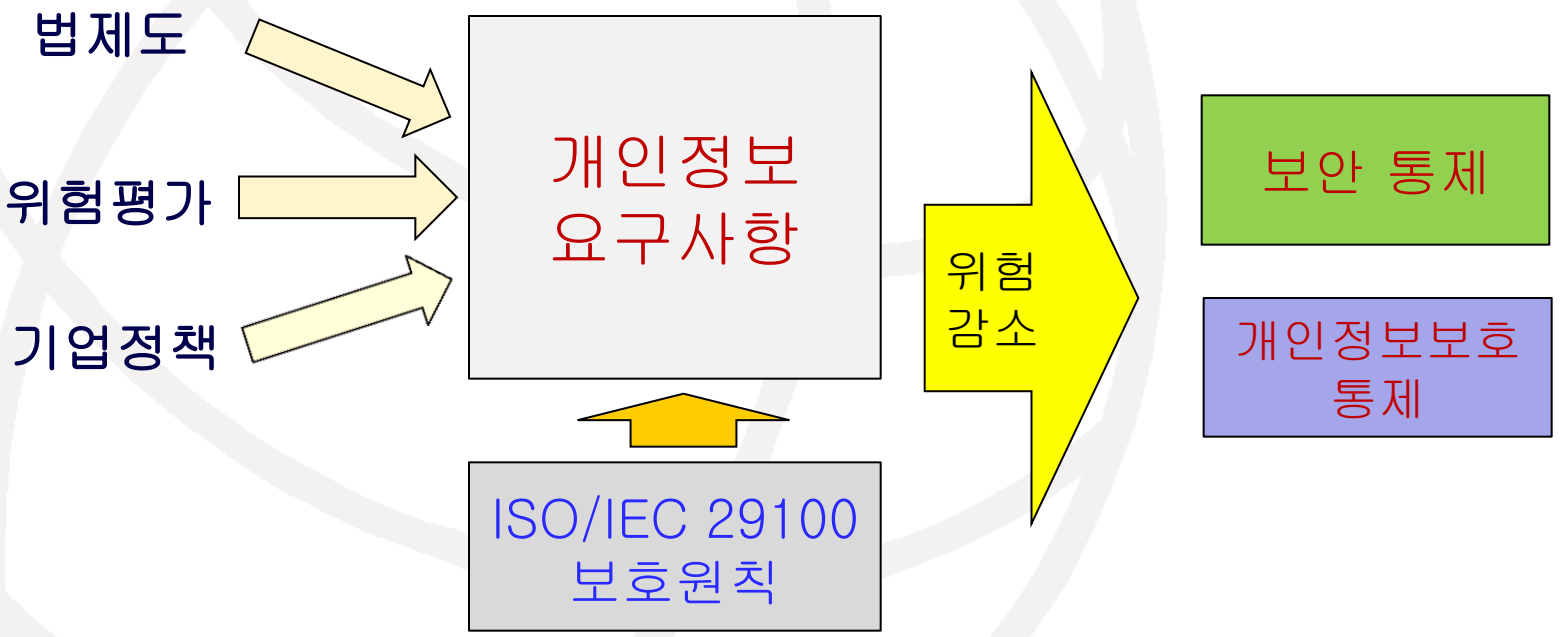


ISO/IEC 27018: 클라우드 사업자에 적용, ISO/IEC 29151 : 개인정보처리자에 적용

Figure by Allan Shipman, BS10012 Editor

개인정보보호 요구사항

- 세가지 소스
  - 법, 규제, 계약적 요구사항
  - 위험 평가 결과
  - 회사의 개인정보보호 정책



ISO/IEC 29100 개인정보보호 원칙 기반

- 동의 및 선택
- 목적 합법성 및 목적 명세
- 수집 제한
- 데이터 최소화
- 이용, 보유, 제공 제한
- 정확성 및 품질
- 공개, 투명성, 고지
- 정보주체 참여 및 접근
- 책임성
- 정보보안
- 프라이버시 법 준수

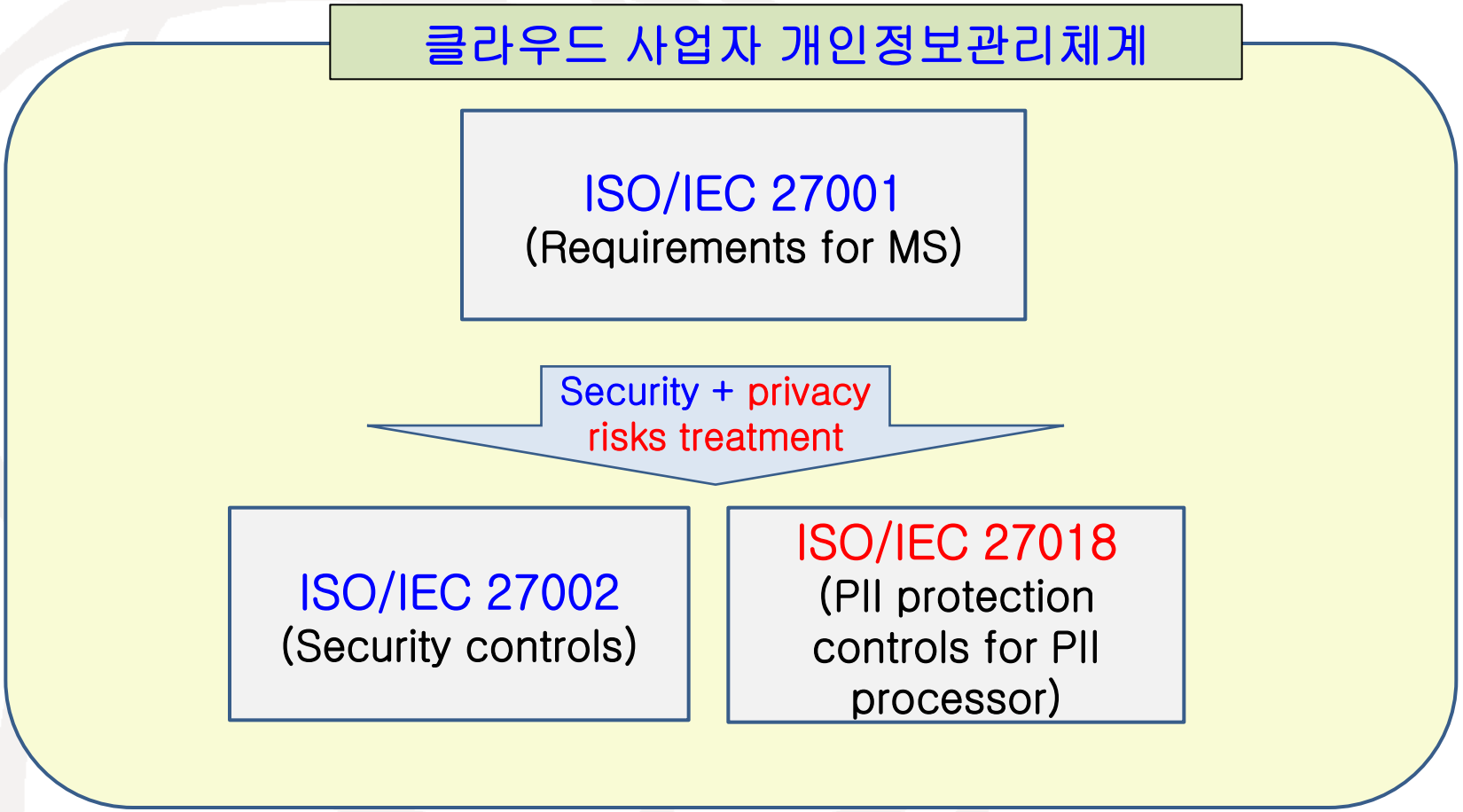
ISO/IEC 27018 통제 – ISO/IEC 27002 추가

- 보안 정책 – 개인정보보호 법 준수 등의 정책 추가
- 정보보호 조직 – 고객과의 연락책임자 임명
- 인적 자원 보안 – 사고로 인한 각 주체에 대한 부정적 영향 인식 필요
- 자산 관리
- 접근 통제
- 암호 – 민감 개인정보 암호화 요구
- 물리 및 환경 보안 – 저장 매체의 개인정보 삭제 필요
- 운영보안 – 시험 데이터 개인정보 포함시 보호 조치 강구
- 통신 보안 – 출입 물리적 매체 기록
- 시스템 구매, 개발 및 관리
- 공급자 관계
- 정보보안 침해사고 관리 – 고객과 제공자간 분리된 역할
- 비즈니스 연속성을 위한 정보보안 측면
- 법 준수 – 보안 정책 구현 증거 제시

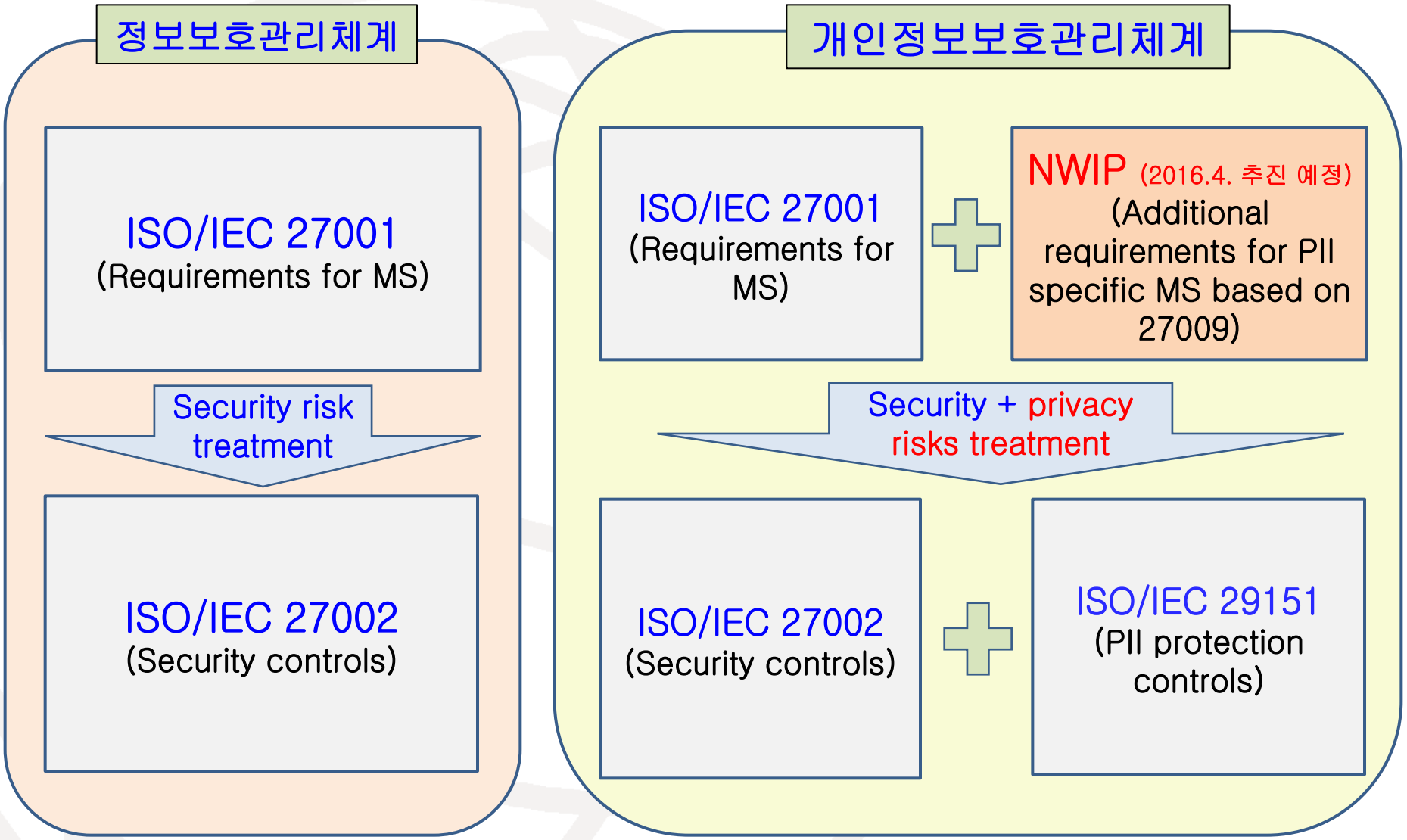
개인정보보호 특화 통제 사례 – 정규 부록

- 개인정보 주체의 권한을 행사 할 수 있는 수단 제공
- 목적 명세와 수집 제한 원칙 보장 – 고객의 요구한 목적으로만 개인정보 처리
- 별도 동의 없이 상업 및 홍보용 개인정보 이용 제한
- 개인정보 포함 임시 파일 삭제
- 클라우드 서비스 제공자의 위탁 기관 정보 사전 공개
- 주요 주체간의 보안 역할과 책임을 명확히 할당
- 데이터 유출, 비인가된 접근 등의 사건 발생시 통보
- 개인정보 저장시 지정학적 위치 규정 및 문서화
- 전송망 개인정보 암호화 조치

클라우드 서비스 사업자 개인정보보호 인증
(ISO/IEC 27018 이용)



개인정보보호관리체계 vs. 정보보호관리체계



ISO/IEC SC27/WG5 – 개인정보보호 및 신원확인 관리 국제표준 개발 현황

SC 27/WG 5 프로젝트 현황 (2016.09 현재)

- 프레임워크 및 구조
  - A framework for identity management – Part 3: Practice (ISO/IEC 24760-3, IS)
  - A framework for access management (ISO/IEC 29146, IS)
- 보호 개념
  - Telebiometric authentication framework using biometric hardware security module (ISO/IEC 17922, DIS/FDIS)
- 가이던스
  - Identity proofing (ISO/IEC 29003, 3rd CD)
  - Privacy impact assessment – guidelines (ISO/IEC 29134, DIS)
  - Code of practice for PII protection (ISO/IEC 29151, DIS)
  - Privacy enhancing data de-integration techniques (ISO/IEC 20889, 2nd WD)
  - User friendly online privacy notices and consent (ISO/IEC 29184, 1st WD)

NWIP and Study Periods (May 2015)

- Standing Documents
  - WG 5 SD1, WG 5 Roadmap
  - WG 5 SD2, Privacy references list
  - WG 5 SD3, Harmonized vocabulary effort
  - WG 5 SD4, Standards privacy assessment
  - WG 5 SD5, Guidelines for the application of ISMS in the area of privacy
- NWIP 투표 (진행 중)
  - Enhancement to ISO/IEC 27001 for privacy management – Requirements
  - Requirements for attribute-based unlinkable entity authentication
  - Privacy engineering
- Study Period
  - Editorial inconsistencies in ISO/IEC 29100 Information technology – Security techniques – Privacy framework
  - Guidelines for privacy in Internet of Things (IoT)
  - Entity Authentication Assurance Framework
  - PII Protection Considerations for Smartphone App providers
  - Privacy in Smart Cities

마치면서

- 공공 클라우드 사업자를 위한 보안 인증제도
  - 미래부, 2016.05년 발표
  - 국제 표준과 호환되는 통제 적용
  - 공공 서비스를 위한 고유 통제 적용
- 국제 클라우드 서비스 제공자를 위한 인증제도 가능
  - 27001 + 27002 + 27017 표준에 근거한 보안 인증체계 구축 가능
  - 27001 + 27002 + 27018 국제표준 인증 체계 구축 가능
  - 고객에 대한 보안 및 개인정보보호 측면의 신뢰 수준 제공

감사합니다.