SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

Cloud Standards: What They Are, Why You Should Care

Live Webcast
February 13, 2020
10:00 am PT

Today's Presenters

SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

Alex McDonald
Vice Chair, SNIA CSTI
NetApp

Eric Hibbard
ISO Editor
Cloud Security Professional

About the Presenters

SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

- Alex McDonald
  - Member, NetApp Office of the CTO
  - Member, SNIA EMEA Board of Directors
  - Chair, SNA Cloud Storage Technologies Initiative
  - Co-Chair, SNIA Solid State Storage Initiative
  - Vice Chair, SNIA Networking Storage Forum
  - Advisor, SNIA Technical Council
- Eric Hibbard, CISSP-ISSAP, ISSMP, ISSEP, CIPT, CISA, CCSP, CCSK
  - Chair, SNA Security TWG
  - Co-Chairman, Cloud Security Alliance International Standardization Council
  - ISO Editor, ISO/IEC 17788, ISO/IEC 27040, ISO/IEC 20648, ISO/IEC 22123, ISO/IEC 27050
  - Chairman, INCITS TC CS1 Cyber Security
  - Chairman, IEEE Cybersecurity & Privacy Standards Committee
  - Member, ABA Cybersecurity Legal Task Force

SNIA Legal Notice

SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

- The material contained in this presentation is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

SNIA-At-A-Glance

SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

185
industry leading organizations

2,000
active contributing members

50,000
IT end users & storage pros worldwide

SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

What We Do

Educate vendors and users on cloud storage, data services and orchestration

Support & promote business models and architectures: OpenStack, Software Defined Storage, Kubernetes, Object Storage

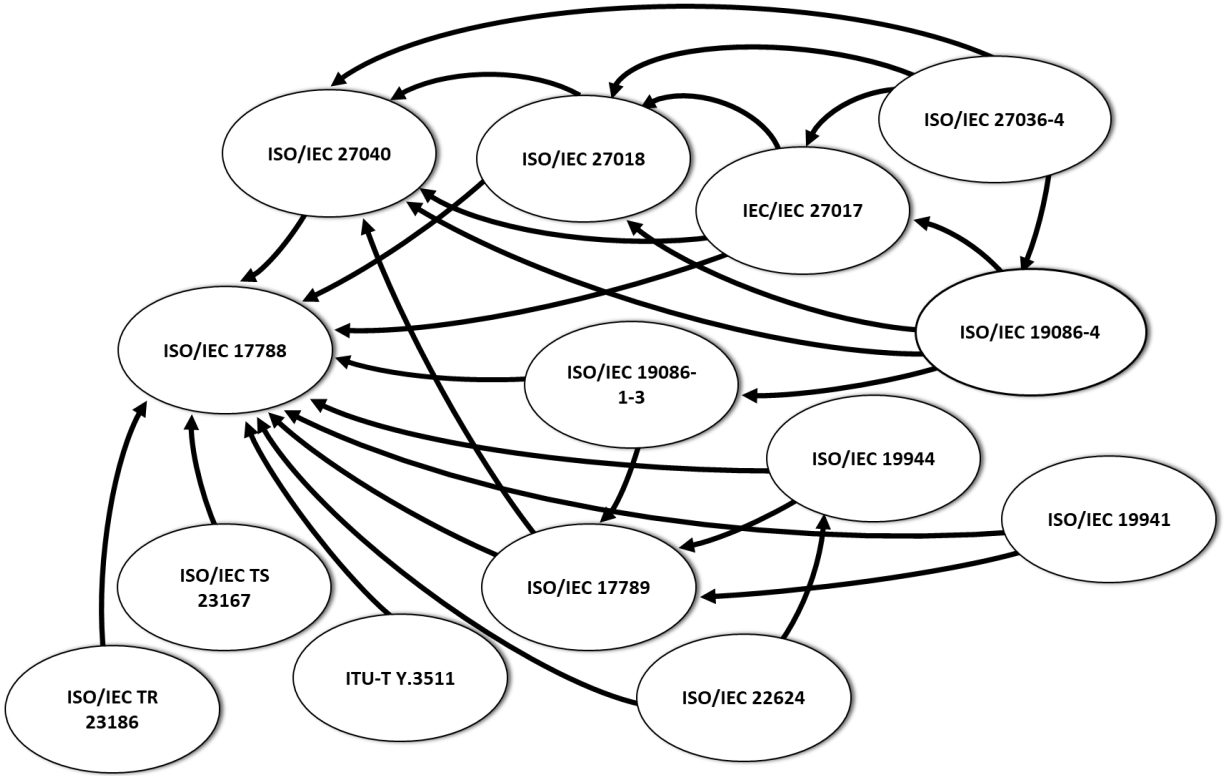
Understand Hyperscaler requirements Incorporate them into standards and programs

Collaborate with other industry associations

Does Cloud Standardization Have You Confused?

- Plethora of sources…
  - ISO/IEC, ITU, IETF, NIST, OASIS, IEEE, etc.
  - Industry Association: Cloud Security Alliance, Open Commons Consortium, Cloud Standards Customer Council, etc.
- What do they specify?
  - Foundations, technology, and interoperability
  - Best practices
  - Risk, security, privacy

Inter-relationship of Cloud Computing Standards



Why Should You Care?

- For cloud providers
  - Some standards represent table stakes
  - Help address the “Cloud Bogeyman”
- For cloud customer/users
  - Consistency in terminology and offerings
  - Set reasonable expectations
  - Compliance/verification

cloud computing: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.
NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

Review of Specific ISO Cloud and Related Standards

Key Cloud Topics

Terminology & Concepts

ISO/IEC 17788 | ITU-T Y.3500
ISO/IEC 17789 | ITU-T Y.3502

ISO/IEC 22123

Cloud SLA Framework

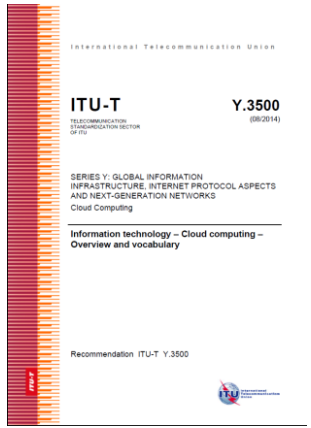
Outsourcing to the Cloud

Security & Privacy

ISO/IEC 17788 (ITU-T Y.3500)

- *Information technology – Cloud computing – Overview and vocabulary*

- Key Characteristics
  - Broad network access, measured service, multi-tenancy, on-demand self-service, rapid elasticity and scalability, resource pooling
- Cloud Roles and Activities
  - Customer (CSC), Provider (CSP), Partner (CSN)
- Cloud Service Categories
  - CaaS, CompaaS, DSaaS, **IaaS**, NaaS, **PaaS**, **SaaS**
- Cloud Deployment Models
  - Public, Private, Community, Hybrid



ISO/IEC 17788 (cont.)

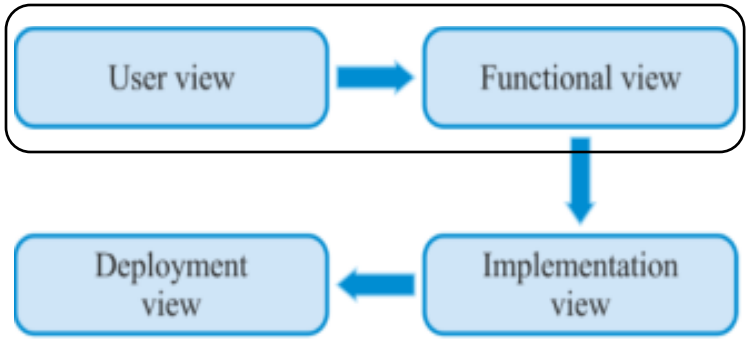
Cloud Cross-cutting Aspects

- Auditability
- Availability
- Governance
- Interoperability
- Maintenance & Versioning
- Performance
- Portability
- Protection of PII
- Regulatory
- Resiliency
- Reversibility
- Security
- Service Levels & SLAs

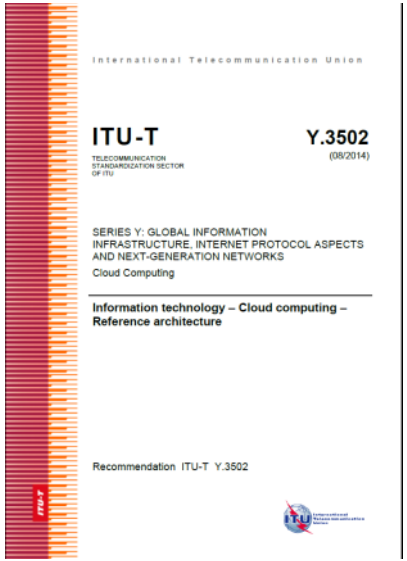
ISO/IEC 17789 (ITU-T Y.3502)

- *Information technology – Cloud computing – Reference architecture*

- Roles and sub-roles in cloud computing
- Expanded descriptions of cross-cutting aspects
- Layer Framework
  - User, access, service, resource
  - Multi-layer functions
- Functional components



ISO/IEC 17789 (cont.)


International Telecommunication Union

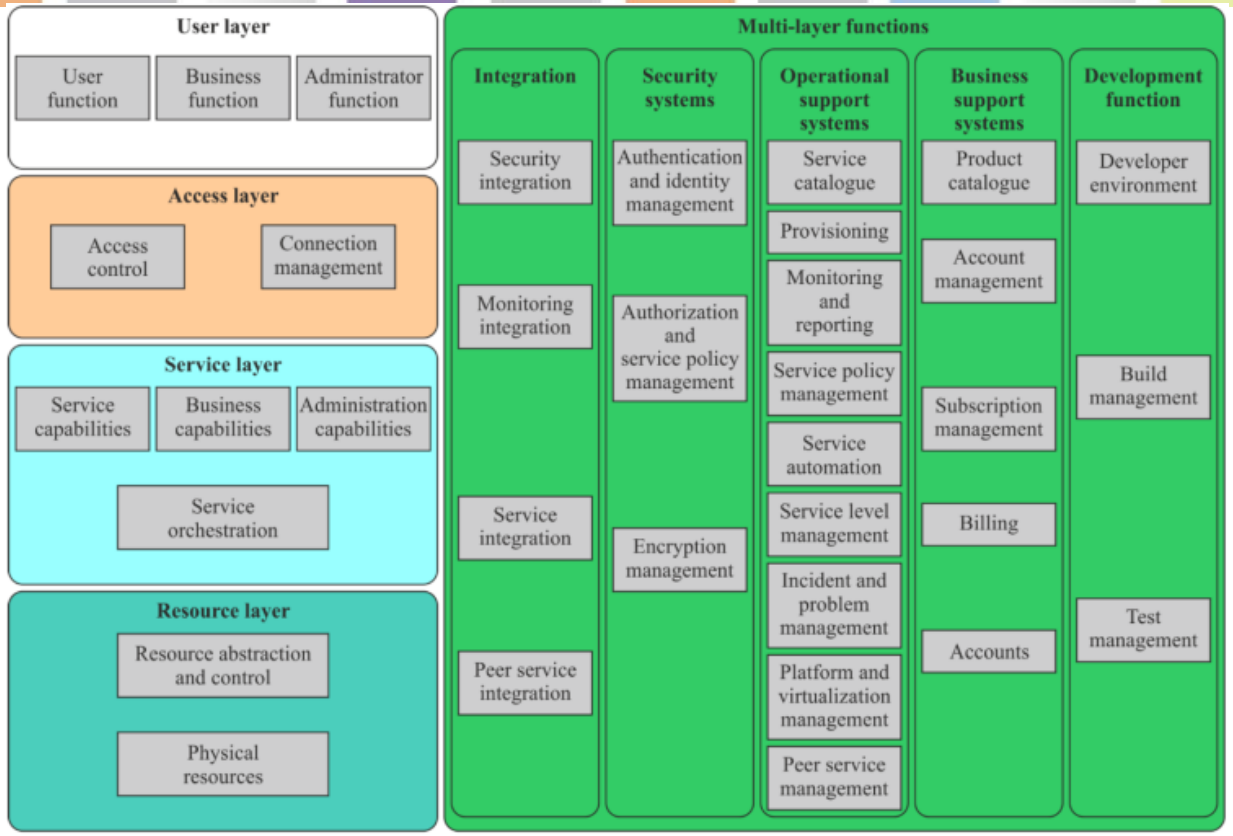
ITU-T Y.3502
(08/2014)

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS
Cloud Computing

Information technology – Cloud computing – Reference architecture

Recommendation ITU-T Y.3502



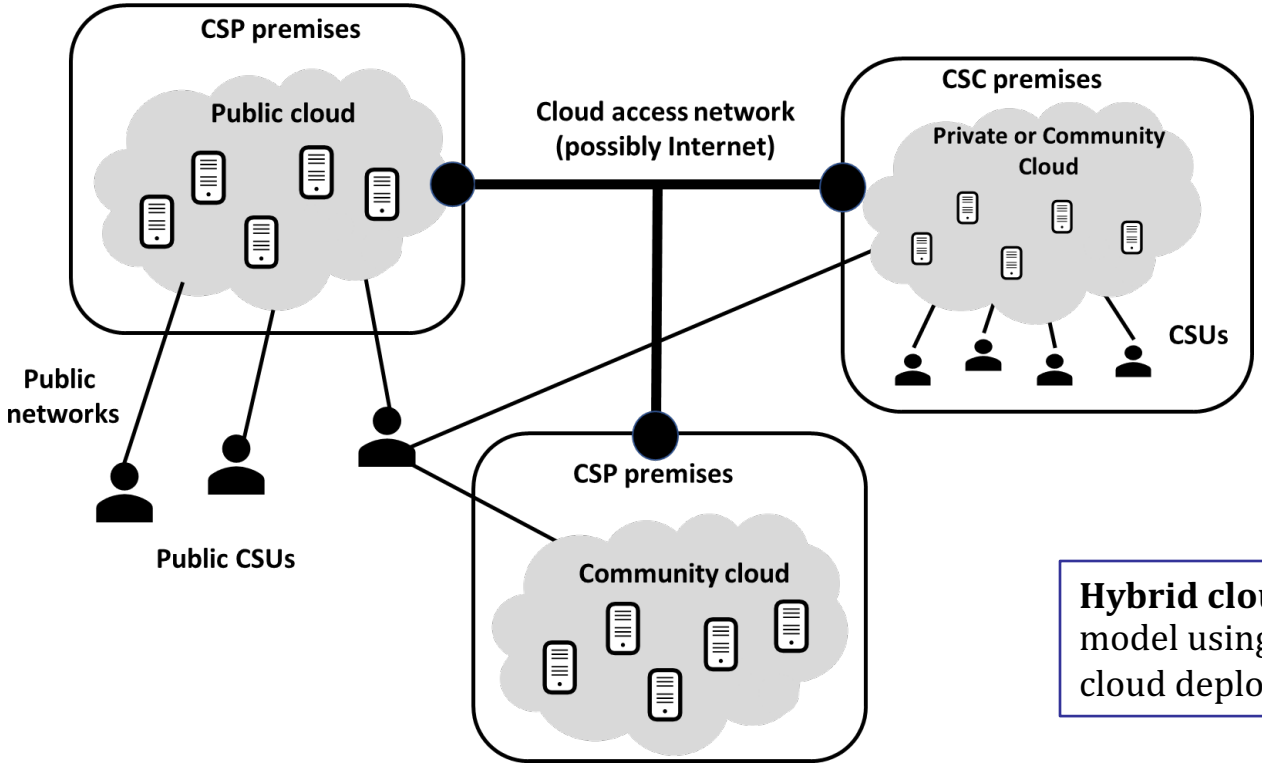
ISO/IEC 22123 (draft)

- Information technology – Cloud computing

Part 1: *Terminology*	Part 2: *Concepts*

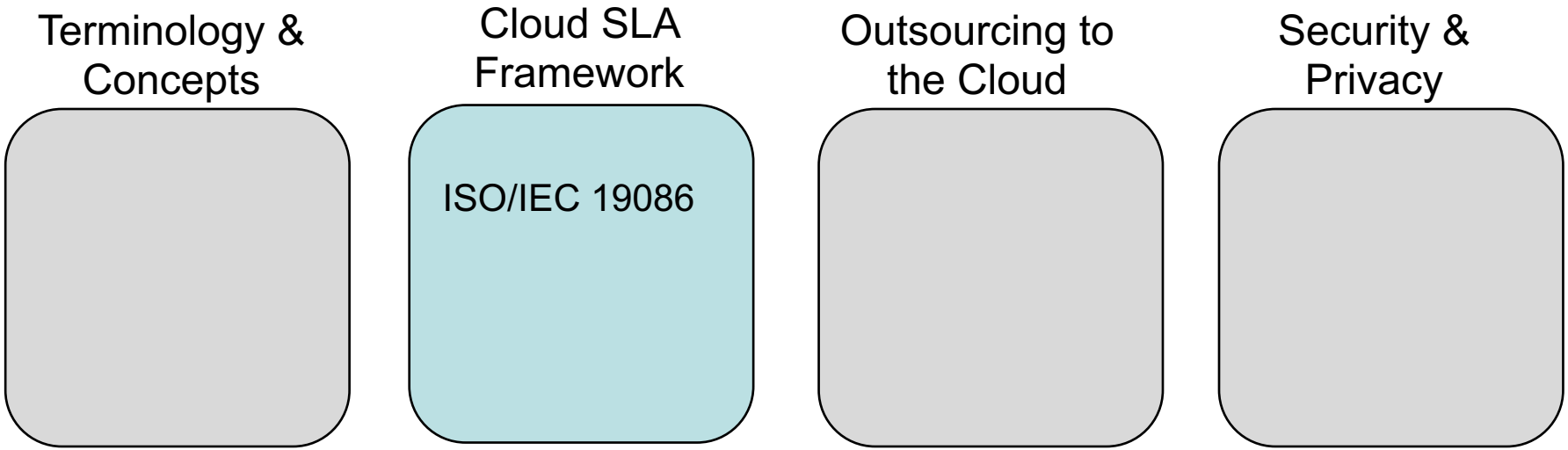
- Builds upon ISO/IEC 17788 & ISO/IEC 17789
- Introductory materials on cloud federation/multi-cloud
- Introductory materials on virtualization, which is a key technology that underpins cloud computing
- Trying to address hybrid cloud problems/issues

Clarifying Hybrid Cloud



Hybrid cloud. Cloud deployment model using at least two different cloud deployment models.

Key Cloud Topics



ISO/IEC 19086 [Multi-part]

- Information technology – Cloud computing – Service level agreement (SLA) framework

Part 1: ***Overview and concepts***	**Part 2:** ***Metric Model****
Part 3: ***Core Conformance Requirements***	**Part 4:** ***Components of Security and Protection of PII****

**Cloud computing – Service level agreement (SLA) framework

ISO/IEC 19086-1

- Applicable to CSC and CSP
- Identifies cloud service level objectives (SLOs)
- Cloud service qualitative objectives (SQOs)
- Cloud SLA components
  - Covered services
  - Cloud SLA definitions
  - Service monitoring
  - Roles and responsibilities


INTERNATIONAL STANDARD

ISO/IEC 19086-1

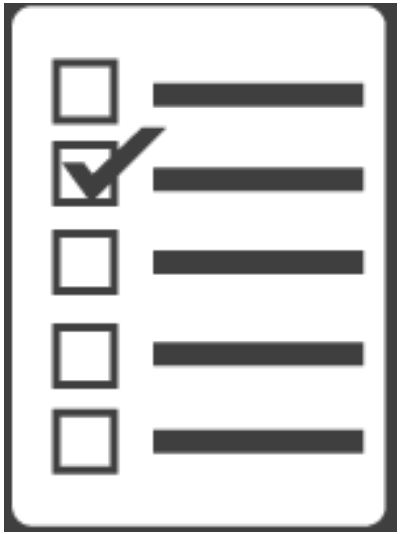
Information technology — Cloud computing — Service level agreement (SLA) framework —

Part 1:

Overview and concepts

ISO/IEC 19086-1 (cont.)

- Relationship between Cloud Service Agreements (CSAs) and Cloud SLAs
- Examples of common parts of CSAs:
  - Cloud Service Level Agreement (cloud SLA)
  - Acceptable Use Policy
  - Security Policy
  - Data Protection Policy
  - Business Continuity Policy
  - Upgrade Policy
  - Termination Policy



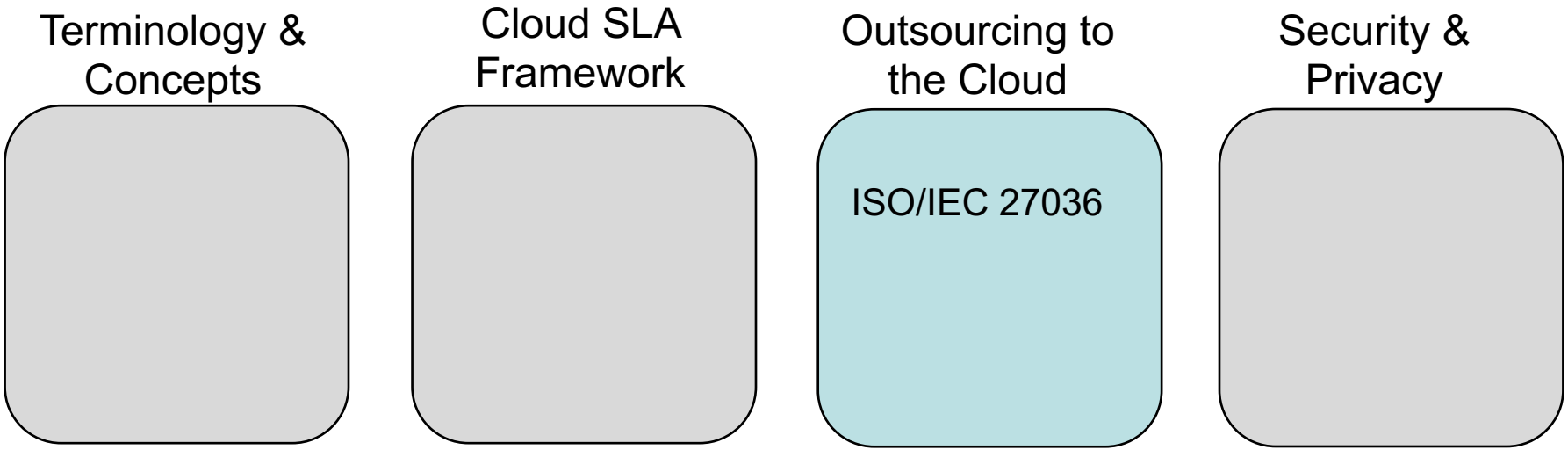
Cloud SLA Content Areas and their Components

- Accessibility
- Availability
- Cloud service performance
- Protection of PII
- Information security
- Termination of service
- Cloud service support
- Governance
- Changes to the cloud service features and functionality
- Service reliability
- Data management
- Attestations, certifications and audits

ISO/IEC 19086-3

- Specifies the core conformance requirements for SLAs for cloud services based on ISO/IEC 19086-1 and guidance on the core requirements
- SLA that conform must include: “Covered Services” and “Cloud SLA definitions”
- Sample language (termination of service):
  - A termination of service component shall specify one or more SLOs or SQOs for termination of service

Key Cloud Topics



ISO/IEC 19086 [Multi-part]

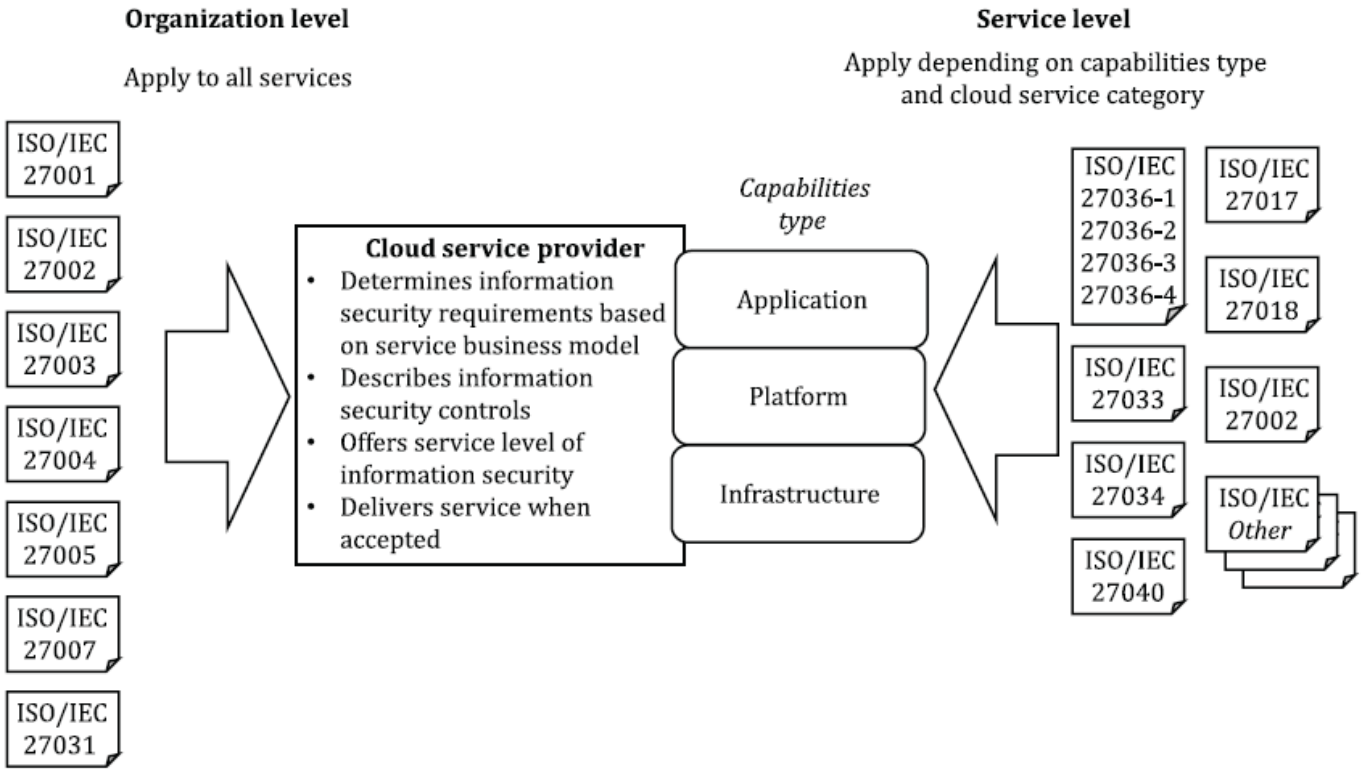
- *Information technology – Security techniques – Information security for supplier relationships*

Part 1: ***Overview and concepts***	**Part 2:** ***Requirements***
Part 3: ***Guidelines for ICT supply chain security***	**Part 4:** ***Guidelines for security of cloud services***

ISO/IEC 27036 [Part 4]

- Differences and similarities between ICT outsourcing and public cloud deployment models
- Cloud service threats and associated risks for public cloud
- Information security controls in cloud service acquisition lifecycle
- Information security controls in cloud service providers

Outsourcing to the Cloud
(ISO/IEC 27036)



Key Cloud Topics

Terminology & Concepts	Cloud SLA Framework	Outsourcing to the Cloud	Security & Privacy
			ISO/IEC 27017 | ITU-T X.1631 ISO/IEC 27018 ISO/IEC 27040 ISO/IEC 27701*

*Not a standard specific to cloud.

ISO/IEC 27017

- *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- Additional implementation guidance for relevant controls specified in ISO/IEC 27002
- Additional controls with implementation guidance that specifically relate to cloud services
- Provides an extended control set cloud service

ISO/IEC 27040

- *Storage security*

- Data/media sanitization
- Cloud storage security – General & CDMI
- Secure multitenancy
- Secure autonomous data movement
- Data retention

ISO/IEC 27018

- *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

- Focuses on protecting PII in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment
- Provides a Public cloud PII processor extended control set for PII protection

ISO/IEC 27701

- *Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management — Requirements and guidelines*

- Not specific to cloud, but likely to have an impact; ISO/IEC 27018 will probably be updated
- Similar to ISO/IEC 27001, organization could seek certification (e.g., GDPR)
- Covers both PII controllers and processors

Summary

Terminology & Concepts	Cloud SLA Framework	Outsourcing to the Cloud	Security & Privacy
ISO/IEC 17788 | ITU-T Y.3500 ISO/IEC 22123	ISO/IEC 19086	ISO/IEC 27036	ISO/IEC 27017 | ITU-T X.1631 ISO/IEC 27018 ISO/IEC 27040 ISO/IEC 27701

After This Webcast

SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

- Please rate this webcast and provide us with feedback
- This webcast and a PDF of the slides will be posted to the SNIA Cloud Storage Technologies Initiative website and available on-demand at https://www.snia.org/forum/csti/knowledge/webcasts
- A full Q&A from this webcast will be posted to the SNIA Cloud blog: www.sniacloud.com/
- Follow us on Twitter @SNIACloud

Thank You

Standards (1)

- ISO/IEC 17788 | ITU-T Rec. Y.3500, *Information technology — Cloud computing — Overview and vocabulary*
- ISO/IEC 17998 | ITU-T Rec. Y.3502, *Information technology — Cloud computing — Reference architecture*
- ISO/IEC 17826, *Information technology — Cloud Data Management Interface (CDMI)*
- ISO/IEC 19086-1,*Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1: Overview and concepts*
- ISO/IEC 19086-2,*Information technology — Cloud computing — Service level agreement (SLA) framework — Part 2: Metrics*
- ISO/IEC 19086-3,*Information technology — Cloud computing — Service level agreement (SLA) framework — Part 3: Core conformance requirements*
- ISO/IEC 19086-4,*Information technology — Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII*
- ISO/IEC 19941, *Information technology — Cloud computing — Interoperability and portability*
- ISO/IEC 19944, *Information technology — Cloud computing — Cloud services and devices: data flow, data categories and data use*

Standards (2)

- ISO/IEC AWI TR 3445, *Information technology — Cloud computing — Guidance and best practices for cloud audits*
- ISO/IEC 22123-1, *Information technology — Cloud computing — Part 1: Terminology*
- ISO/IEC 22123-2, *Information technology — Cloud computing — Part 2: Concepts*
- ISO/IEC 22624, *Information Technology — Cloud Computing — Taxonomy based data handling for cloud services*
- ISO/IEC TR 22678:2019, *Information Technology — Cloud Computing — Guidance for policy development*
- ISO/IEC TS 23167:2018, *Information Technology — Cloud Computing — Common technologies and techniques*
- ISO/IEC TR 23186:2018, *Information Technology — Cloud Computing — Framework of trust for processing of multi-sourced data*
- ISO/IEC TR 23187, *Information Technology — Cloud Computing — Interacting with cloud service partners (CSNs)*
- ISO/IEC TR 23188, *Information Technology — Cloud Computing — Edge computing landscape*
- ISO/IEC 23613, *Information Technology — Cloud Computing — Cloud service metering elements and billing modes*
- ISO/IEC 23751, *Information Technology — Cloud Computing and distributed platforms — Data sharing agreement (DSA) framework*
- ISO/IEC 23951, *Information Technology — Cloud Computing — Guidance for using the cloud SLA metric model*

Standards (3)

- ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*
- ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*
- ISO/IEC 27017 | ITU-T Rec. X.1631, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- ISO/IEC 27036-1, *Information technology — Security techniques — Information security in supplier relationships — Part 1: Overview and concepts*
- ISO/IEC 27036-2, *Information technology — Security techniques — Information security in supplier relationships — Part 2: Requirements*
- ISO/IEC 27036-3, *Information technology — Security techniques — Information security in supplier relationships — Part 3: Guidelines for information and communication technology supply chain security*
- ISO/IEC 27040, *Information technology — Security techniques — Storage security*