Security and privacy in Cloud Computing

The increasing demand of using Cloud Computing technology has introduced a range of privacy and security risks. Many standards and specifications related to privacy and security in Cloud Computing have been developed by standards developing organizations. These standards are developed within technical committees, with the aim to guide and propose solutions for all stakeholders involved in this technology.

Technical Committees working on standardization for security and privacy in Cloud Computing

- International level -

ISO/IEC JTC 1/SC 38 - Cloud computing and distributed platforms

- **Scope**:
  Standardization in the areas of Cloud Computing and Distributed Platforms including:
  - Foundational concepts and technologies,
  - Operational issues, and
  - Interactions among Cloud Computing systems and with other distributed systems

SC 38 serves as the focus, proponent, and systems integration entity on Cloud Computing, Distributed Platforms, and the application of these technologies. SC 38 provides guidance to JTC 1, IEC, ISO and other entities developing standards in these areas.

- 26 standards published
- 7 ongoing projects
- 2 working groups
- 6 national delegates registered for Luxembourg

ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection

- **Scope**:
  The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:
  - Security requirements capture methodology;
  - Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
  - Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
  - Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
  - Security aspects of identity management, biometrics and privacy;
  - Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
  - Security evaluation criteria and methodology.

- 230 standards published
- 67 ongoing projects
- 5 Working Groups and 2 Joint Working Groups
- 27 national delegates registered for Luxembourg

ITU-T/SG 17 - Security

- **Scope (extract):**

  ITU-T Study Group 17 is responsible for building confidence and security in the use of information and communication technologies. It includes Cloud Computing security.

  The SG 17 hosts a Working Party (WP) which develops standards related to security and privacy in Cloud Computing:

  WP4/17, Service and application security:

  - Question 7/17, Secure application services
  - Question 8/17, Cloud Computing and big data infrastructure security
  - Question 14/17, Distributed ledger technology (DLT) security

Standards for security and privacy in Cloud Computing

The following table lists the published standards for security and privacy in Cloud Computing at the international level. These standards are developed by ISO/IEC JTC 1/SC 27 and ITU-T/SG 17.

ISO/IEC TR 23186:2018
Information technology -- Cloud Computing -- Framework of trust for processing of multi-sourced data

Scope:
This document describes a framework of trust for the processing of multi-sourced data that includes data use obligations and controls, data provenance, chain of custody, security and immutable proof of compliance as elements of the framework.

Overview:
This document provides:

- Scenarios of using multi-sourced data
- Information about data access and processing rights
- Framework for trusted processing of multi-sourced data
- Elements of trust
- Generalized guidance for including the elements of trust in an agreement

ISO/IEC 23751:2022
Information technology -- Cloud Computing and distributed platforms -- Data sharing agreement (DSA) framework

Scope:
This document establishes a set of building blocks, i.e. concepts, terms, and definitions, including Data Level Objectives (DLOs) and Data Qualitative Objectives (DQOs), that can be used to create Data Sharing Agreements (DSAs). This document is applicable to DSAs where the data is intended to be processed using one or more Cloud services or other distributed platforms.

Overview:
This document provides:

- Overview of DSAs
- Dataset description
- Data use obligations and controls
- Data provenance records, quality, and integrity
- Chain of custody and transfer of custody
- Security and privacy
- Proof of compliance
- Examples of alternatives to bespoke data sharing agreements (DSAs)
- ISO/IEC standards for identity, privacy, chain of custody, forensics and security

ISO/IEC 19086-4:2019
Cloud Computing -- Service level agreement (SLA) framework -- Part 4: Components of security and of protection of PII

Scope:
This document specifies security and protection of personally identifiable information components, SLOs and SQOs for Cloud service level agreements (Cloud SLA) including requirements and guidance. This document is for the benefit and use of both CSPs and CSCs.

Overview:
This document explains the relationship with other parts of the Cloud Computing SLA framework, provides information security components and describes the protection of personally identifiable information component.

ISO/IEC 27017:2015

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

Scope:

This Recommendation | International Standard gives guidelines for information security controls applicable to the provision and use of Cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to Cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both Cloud service providers and Cloud service customers.

Overview:

The document provides:

- guidelines supporting the implementation of information security controls for Cloud service customers and Cloud service providers
- Cloud service extended control set
- References on information security risk related to Cloud Computing

ISO/IEC 27018:2019

Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public Clouds acting as PII processors

Scope:

This document establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public Cloud Computing environment.

In particular, this document specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public Cloud services.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via Cloud Computing under contract to other organizations.

The guidelines in this document can also be relevant to organizations acting as PII controllers. However, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. This document is not intended to cover such additional obligations.

Overview:

This document provides information and guidelines about:

- Security policies
- Organization of information security
- Human resource security
- Access control
- Cryptographic controls
- Physical and environmental security
- Operations security
- Communications security
- Information security incident management
- Information security aspects of business continuity management
- Compliance with legal and contractual requirements

ISO/IEC 27036-4:2016

Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of Cloud services

Scope:

This document provides Cloud service customers and Cloud service providers with guidance on

- gaining visibility into the information security risks associated with the use of Cloud services and managing those risks effectively, and
- responding to risks specific to the acquisition or provision of Cloud services that can have an information security impact on organizations using these services.

This document does not include business continuity management/resiliency issues involved with the Cloud service. ISO/IEC 27031 addresses business continuity.

This document does not provide guidance on how a Cloud service provider should implement, manage and operate information security. Guidance on those can be found in ISO/IEC 27002 and ISO/IEC 27017.

The scope of this document is to define guidelines supporting the implementation of information security management for the use of Cloud services.

Overview:
The document provides:

- Key Cloud concepts and security threats and risks
- Information security controls in Cloud service acquisition lifecycle
- Information security controls in Cloud service providers
- Information security standards for Cloud providers
- Mapping to ISO/IEC 27017 controls

ITU-T X.1641 (09/2016)
Guidelines for Cloud service customer data security

Scope:
Recommendation ITU-T X.1641 provides generic security guidelines for the Cloud service customer (CSC) data in Cloud Computing. It analyses the CSC data security lifecycle and proposes security requirements at each stage of the data lifecycle. Furthermore, the Recommendation provides guidelines on when each control should be used for best security practice.

Overview:
The document provides:

- Overview about Cloud service customer data security
- Guidelines for security controls related to data security
- Guidelines for using security controls

ITU-T X.1601 (10/2015)
Security framework for Cloud Computing

Scope:
Recommendation ITU-T X.1601 describes the security framework for Cloud Computing. The Recommendation analyses security threats and challenges in the Cloud Computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for Cloud Computing. Appendix I provides a mapping table on how a particular security threat or challenge is addressed by one or more corresponding security capabilities.

Overview:
The document provides:

- Security threats for Cloud Computing
- Security challenges for Cloud Computing
- Cloud Computing security capabilities
- Framework methodology
- Mapping of Cloud Computing security threats and challenges to security capabilities