SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**

M6 - Certification and Frameworks for Organizations and management systems

Contents

3. Cloud Security

- Cloud computing: benefits and risks
- ISO/IEC 27017 and ISO/IEC 27018.
  - Security and privacy in cloud;
  - Add-on structure
- Cloud Security Alliance (CSA) - STAR Certification
  - CCM
  - CAIQ

What is cloud computing?

DEFINED BY **IEC** (ELECTROPEDIA.ORG)

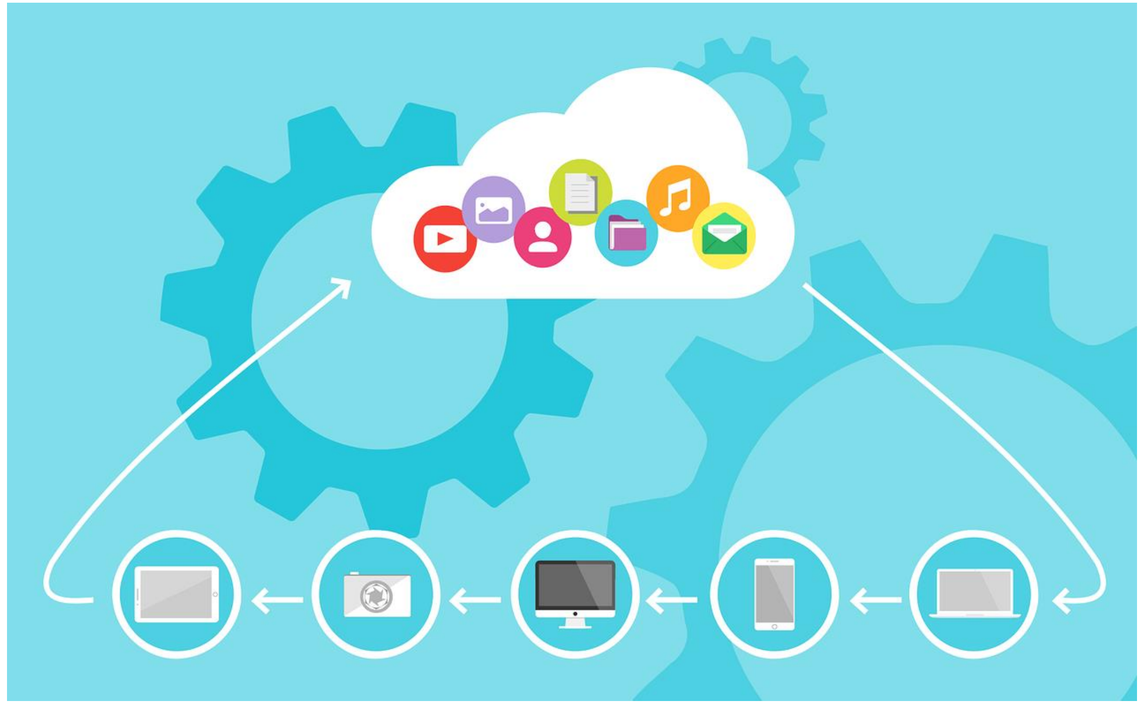
Cloud computing is

- data processing delivered as a service *over a network*, typically the Internet.

Cloud computing provides

- shared computer resources *on demand*.

[Source: IEV ref 171-09-12. “Digital technology – Fundamental concepts” (published on 2019-03-29)]

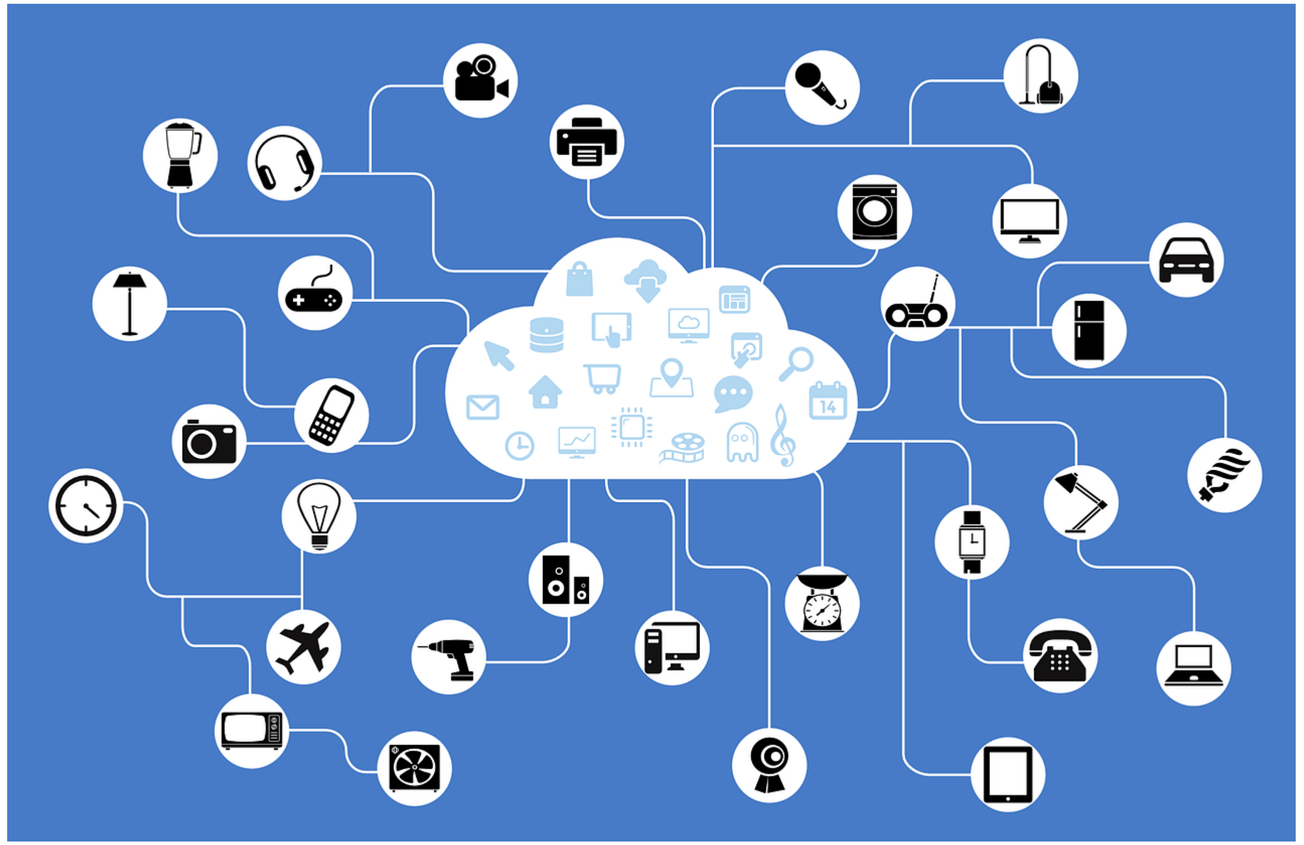


What is cloud computing?

DEFINED BY ISO/IEC 20924:2018

Cloud computing can be also defined as a "***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*"

[Source: ISO/IEC 20924:2018, 3.1.7]



What are the benefits of cloud computing?

The Cloud model introduces significant **advantages** over traditional hardware solutions, which allow you to:

- carry out **continuous updates** of the infrastructure and applications;
- use the applications from **any device** in any place via internet access;
- have greater **flexibility** in trying new services or making changes, with minimal costs;
- reduce the **risks** associated with the **management of the security** (physical and logical) of IT infrastructures;

What are the benefits of cloud computing?

But also:

- have important **savings** in the use of software, as it is possible to pay for resources as services on a consumption-based basis ("*pay per use*"), avoiding initial investments in the infrastructure and costs associated with licenses for use;
- reduce the overall costs associated with the **location** of the data centers (electricity consumption rents, non-ICT personnel).

What is a cloud service?

DEFINED BY **ISO/IEC 20924:2018**

A cloud service is one or more **capabilities** offered via cloud computing invoked using a defined interface.

[Source: ISO/IEC 20924:2018, 3.1.8]

Who is a cloud service provider?

«CSP» DEFINED BY **ISO/IEC 20924:2018**

Cloud service provider is the **party** which makes cloud services **available**

[Source: ISO/IEC 20924:2018, 3.1.9]

Public cloud service provider **is the** party which makes cloud services available according to the public cloud model

[Source: ISO/IEC 27018:2019, 3.7]

Who is a cloud service customer?

«CSC» DEFINED BY **NIST**

A cloud service **customer** (or consumer) "*is a person or organization that is a customer of a cloud.*" But

*"a cloud customer may itself be a cloud and that clouds may offer services to one **another**"*

[Source: NIST SP 800-146]

What are the main types of cloud services?

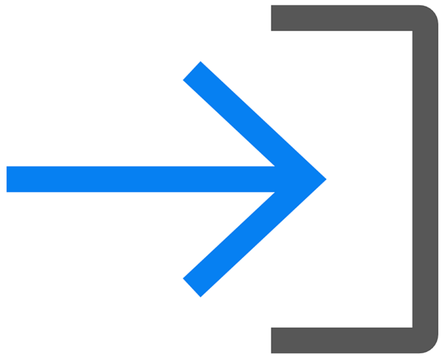
DEFINED BY **ISO/IEC 20924:2018**

There are **mainly three** different types of cloud service that a CSP can provide, which entail a different division of responsibilities among the actors:

- IaaS (Infrastructure as a Service);
- PaaS (Platform as a Service);
- SaaS (Software as a Service).

Infrastructure As A Service (IaaS)

CLOUD COMPUTING



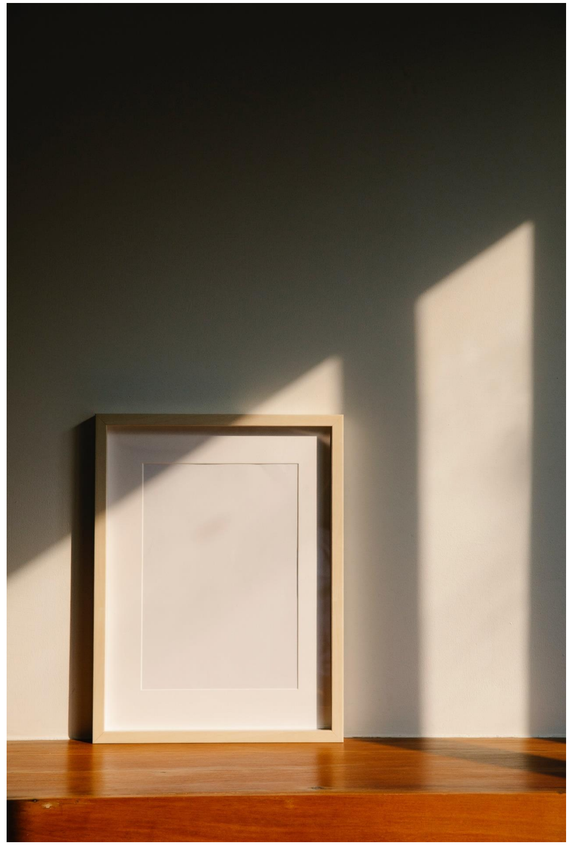
IaaS

The capability provided to the consumer is to *provision* **processing**, **storage**, **networks**, and other fundamental computing **resources** where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

[Source: NIST SP 800-145]

Platform As A Service (PaaS)

CLOUD COMPUTING



PaaS

The capability provided to the consumer is to *deploy* onto the **cloud infrastructure consumer-created** or **acquired** applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the **deployed applications** and **possibly configuration settings** for the application-hosting environment.

[Source: NIST SP 800-145]

Software As A Service (SaaS)

CLOUD COMPUTING

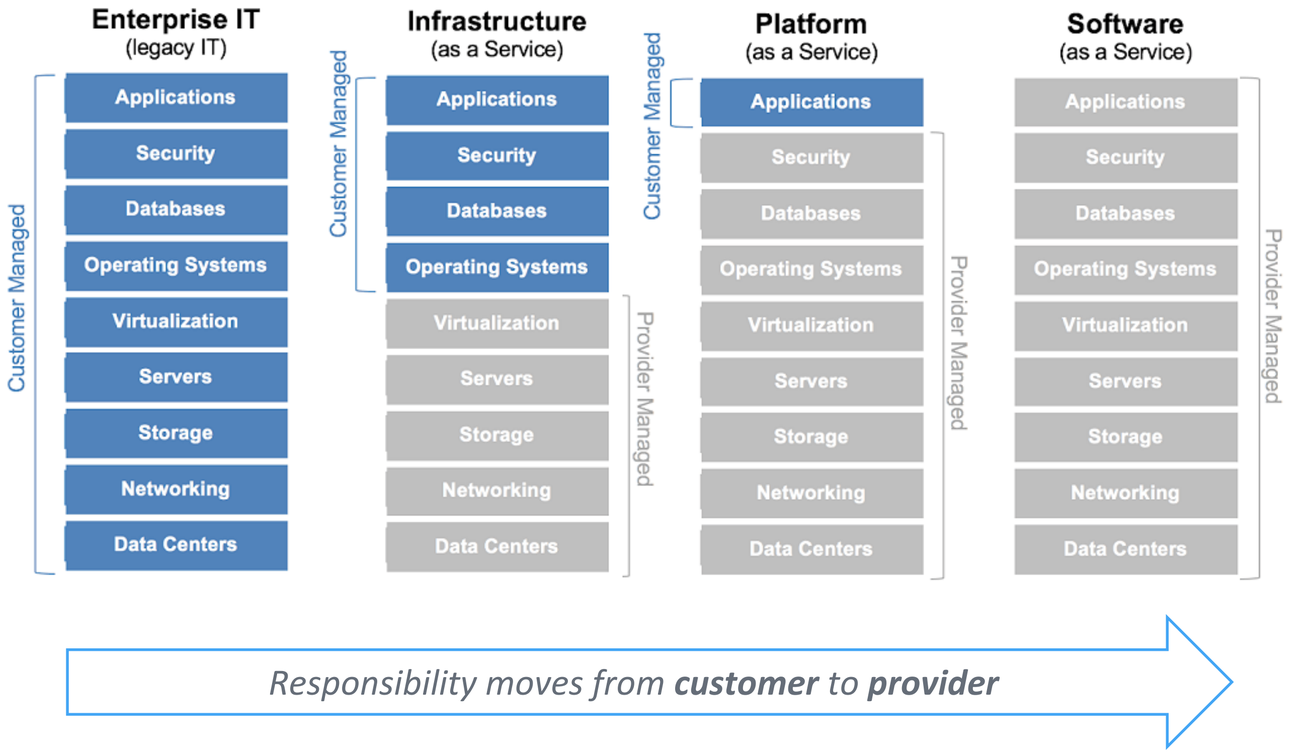
SaaS

The capability provided to the consumer is to *use* the provider's **applications running on a cloud infrastructure**. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

[Source: NIST SP 800-145]

CLOUD SECURITY - RESPONSIBILITY

AND CLOUD COMPUTING



From left to right the responsibilities of the provider increase

*"Consumers and Cloud Service Providers (CSPs) security responsibilities are dependent on the cloud service **model** procured. Understanding this shared security responsibility model is fundamental to ensuring the appropriate allocation of security compliance responsibilities (i.e., impact level, security controls)."*

[Source: https://cic.gsa.gov/basics/cloud-security]

In the SaaS, Customer is usually only responsible for information (data)

Securing the cloud

Specific standards, frameworks and certifications can represent a valid **tool**, even for cloud services.

ISO / IEC 27002:2022

AND CLOUD COMPUTING

Control 5.23, “Information security for use of cloud services”

There are several controls that **impact** cloud services. The one described by ISO/IEC 27002:2022 in particular, states that the processes for **acquiring**, **using**, **managing** and **terminating** cloud services must be established *in accordance* with the organization's information security requirements.

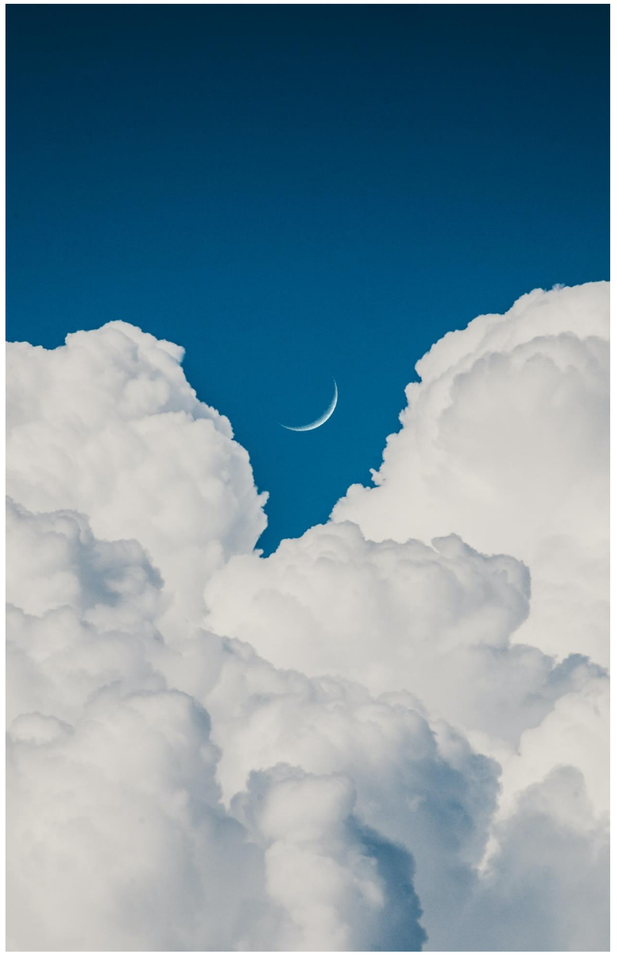
ISO/IEC 27017:2015 and ISO/IEC 27018:2019

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

How can these two standards be useful

- These two standards define a series of **additional** controls for information security, for management systems based on the **ISO/IEC 27001:2013** standard (which will be re-edited to *adapt* to the **new** ISO/IEC 27002:2022).

  They "*extend*" the ISMS, and by this mean they have no "standalone" value. They **expand** the control area of the management system already existing with **cloud services** specific controls.



ISO/IEC 27017:2015

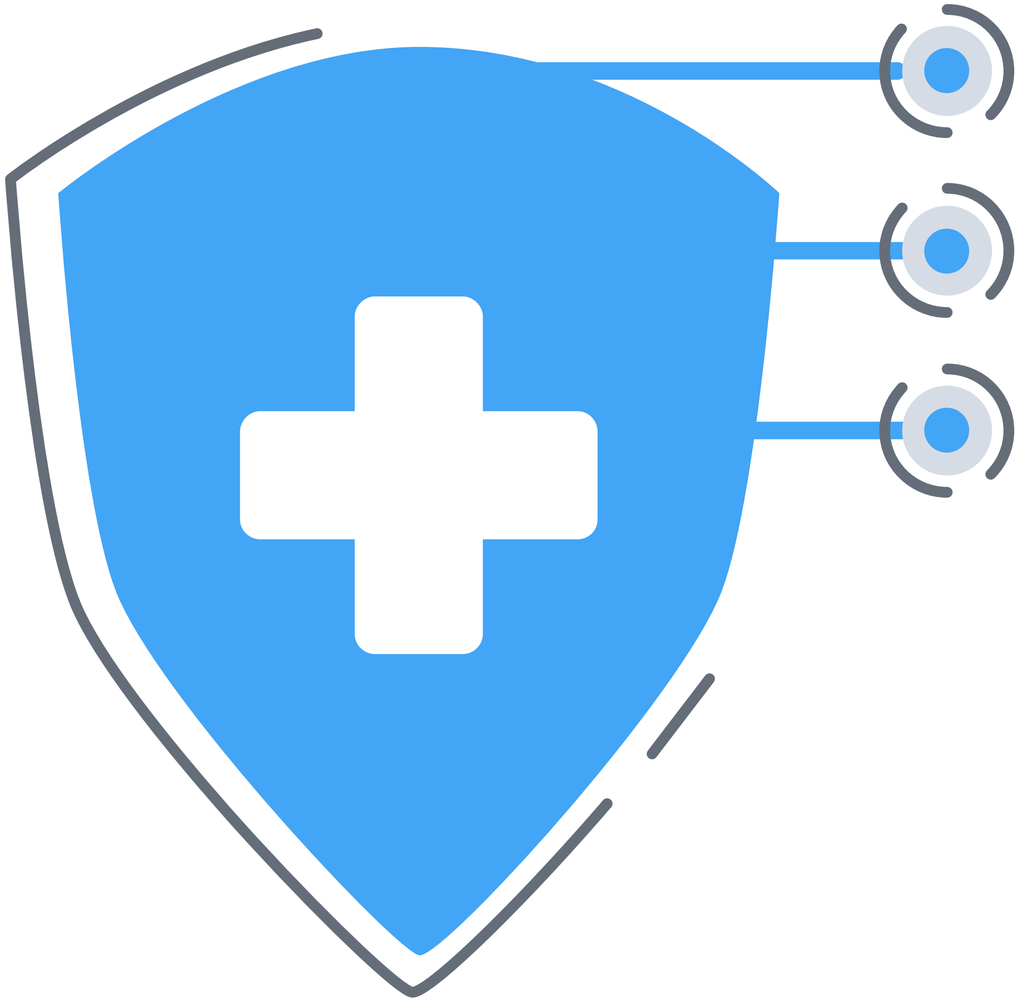
ISMS AND CLOUD COMPUTING

ISO/IEC 27017:2015

- 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 (which do not follow the scheme of annex “A” of ISO 27001).

- This Recommendation / International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.



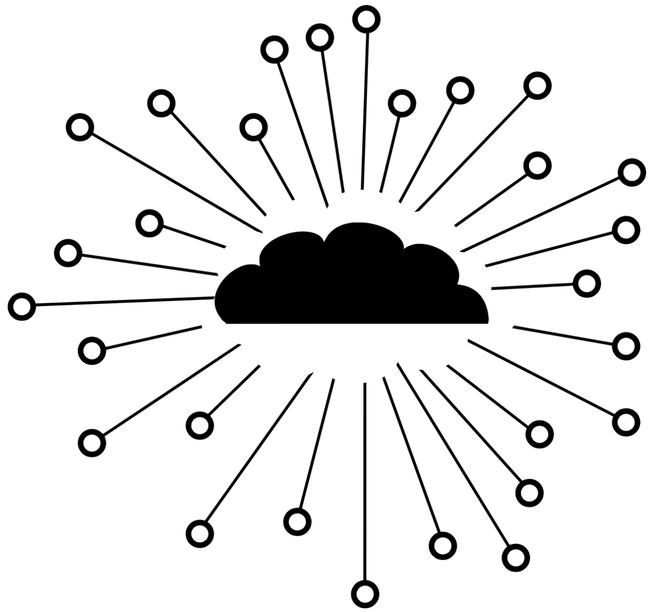
ISO/IEC 27017:2015

ISMS AND CLOUD COMPUTING

ISO/IEC 27017:2015

Some important areas of controls:

- **Shared responsibilities** and **roles** in the cloud computing environment
- Removal and return of cloud services customer **assets** upon **termination** of contract
- **Protection** and **separation** of a customer's virtual environment from that of **other customers**
- Virtual machine **hardening** requirements to meet business needs
- Procedures for **administrative** operations of a cloud computing environment
- **Monitoring** of relevant customer activity in a cloud computing environment
- Alignment of security management for **virtual** and **physical** networks



And more.

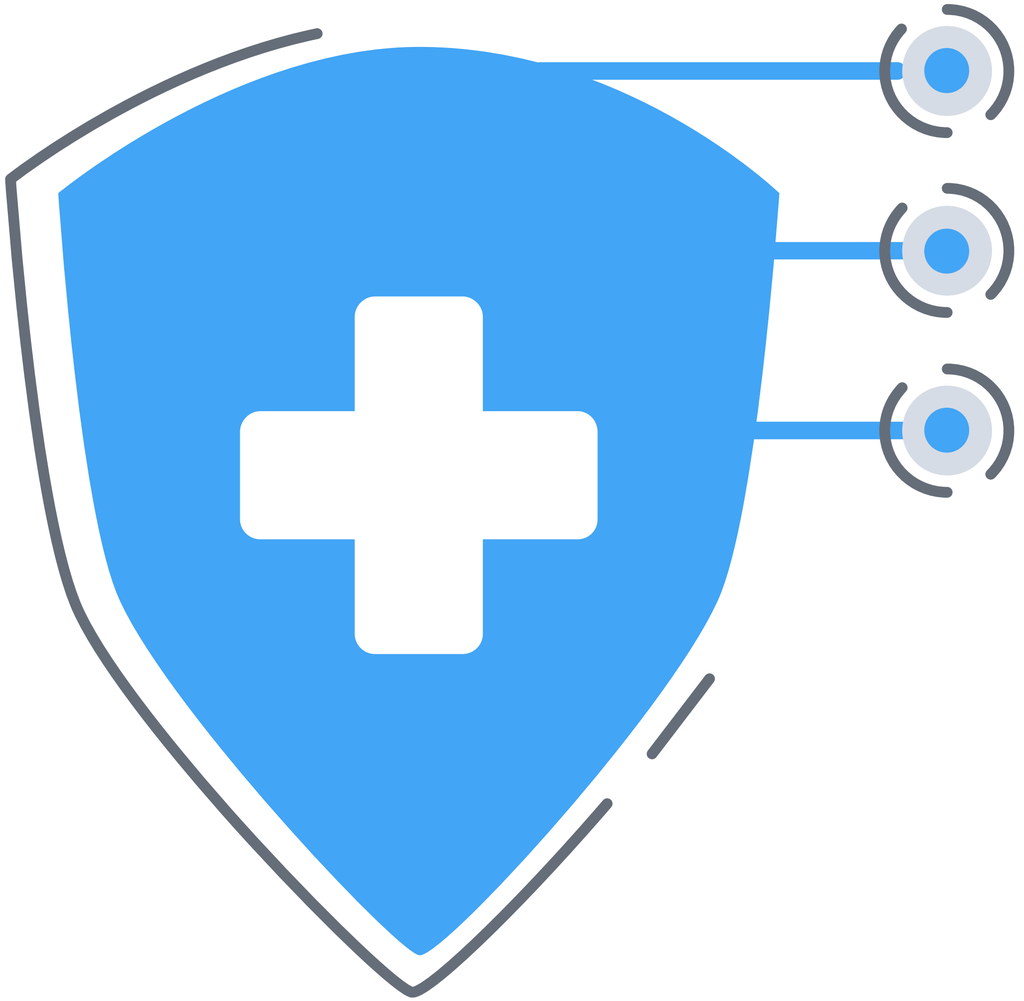
ISO/IEC 27018:2019

ISMS AND CLOUD COMPUTING

ISO/IEC 27018:2019

- 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.



ISO/IEC 27018:2019

ISMS AND CLOUD COMPUTING

ISO/IEC 27018:2019

- It is an international **Code of Practice** for privacy in the cloud.
- Substantially aligned with European Union data protection laws, it provides specific guidelines for cloud service providers (CSPs) processing personal information (PII) for risk assessment and implementation of state-of-the-art controls to protect such information.

ISO/IEC 27018:2019

ISMS AND CLOUD COMPUTING

ISO/IEC 27018:2019

Some important areas of control:

- Management of **data breach** involving PII;
- **Agreements** on the processing of personal data;
- definition of a **contact point** for the customer;
- **legitimate** use of personal data (e.g. commercial purposes must be declared and accepted);
- **Localization** of PII (where data centers are located);
- secure **deletion** and **return** of customer personal data;

And more.

Most common information security risks

IN CLOUD COMPUTING

- Multi-tenancy: creating multiple virtual environments logically distinct present on the same physical component, effectively allowing multiple customers (tenants) to work independently, increases the risk of attacks that can compromise this separation and therefore the **confidentiality** of the data;

- the increasingly international location of computational and storage systems makes the **place** of processing and storage of data often unidentifiable, giving the sensation of losing control. In particular on traceability, the non-homogeneity of laws and regulations between states in which the Datacenters of Cloud suppliers are present, in particular outside the EU, can cause problems of non-compliance and / or sanctions (even if mitigated by the entry into force of the new European regulation on data protection);

- the ways in which Cloud services and immaturity is scarce adoption of tools, standards and interoperable data formats often make it difficult to **migrate** from a provider to another, as well as the simple **recovery** of their data.

And more.

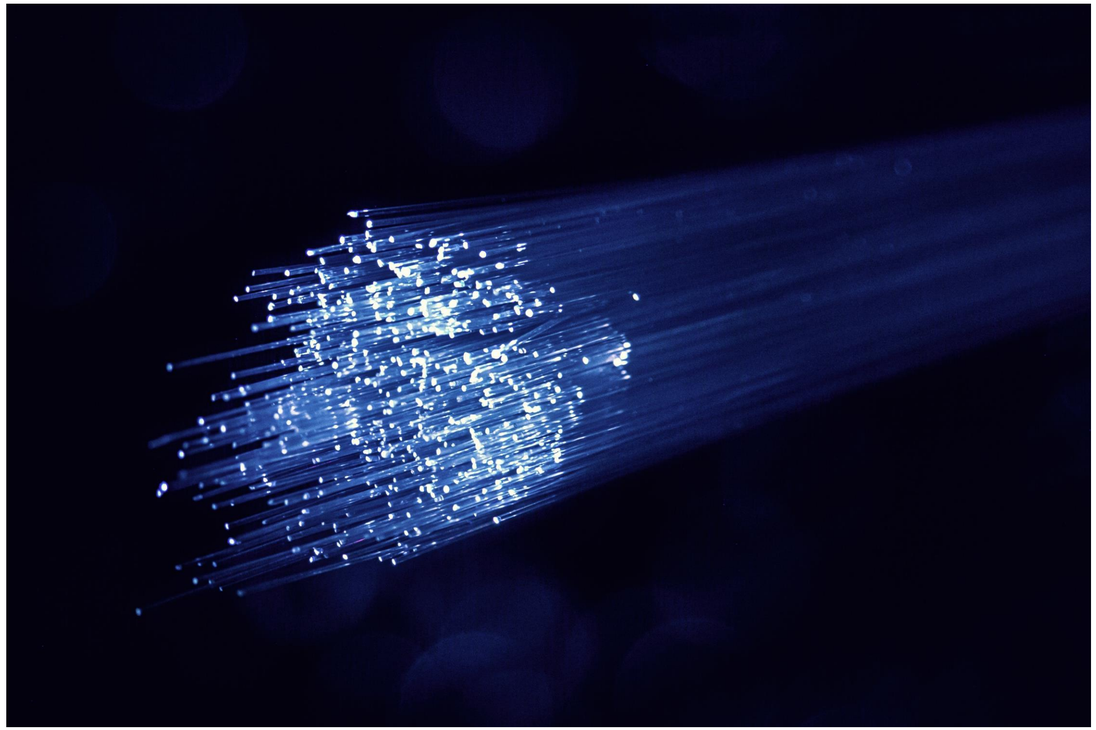
AGID (The Agency for Digital Italy)

CLOUD COMPUTING AND PUBLIC ADMINISTRATION

AGID Marketplace - How to join the Cloud model of the PA

- The Department for Digital Transformation, in collaboration with the Agency for Digital Italy (AgID), has developed a cloud enabling program that defines the set of activities and resources useful to administrations for the migration of digital services and infrastructures to the Cloud of the PA.

- For more info: **cloud.italia.it**

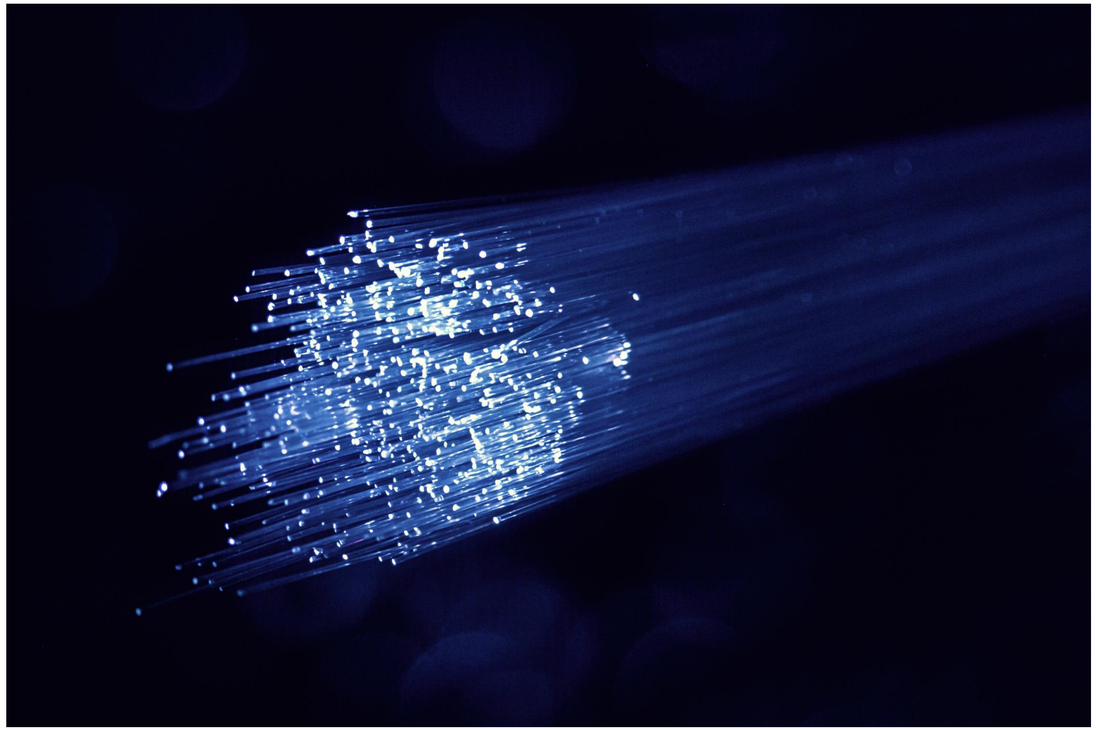


AGID (The Agency for Digital Italy)

CLOUD COMPUTING AND PUBLIC ADMINISTRATION

The Cloud Marketplace

- Since 1 April 2019, Public Administrations can only acquire IaaS, PaaS and SaaS services qualified by AgID and published in the Cloud **Marketplace**.
- To fully exploit the benefits of the cloud, public administrations should first evaluate the presence of SaaS services in the Cloud Marketplace that meet their **needs** and, only second, consider **PaaS** and finally **Iaas** solutions.



Cloud Security Alliance

CLOUD SECURITY ALLIANCE / CSA

The Cloud Security Alliance (CSA) is a world's leading organization dedicated to **defining** and **raising** awareness of *best practices* to help ensure a secure cloud computing environment.

The CSA "SECURITY GUIDANCE For Critical Areas of Focus In Cloud Computing" is an Official Study Guide for the CSSK certificate (cloud security knowledge)

The Cloud Control Matrix (CCM) is a powerful tool for improving cloud security.

Cloud Security Alliance

CLOUD SECURITY ALLIANCE / CSA

CSA Cloud security process:

Identify necessary security and compliance **requirements**, and any existing controls.

- Select your cloud provider, service, and deployment models.
- Define the architecture.
- Assess the security controls.
- Identify control gaps.
- Design and implement controls to fill the gaps.
- Manage changes over time.

[Source: Security Guidance v4.0 - Cloud Security Alliance]

CSA – Cloud Control Matrix

197 CONTROLS AND 17 DOMAINS

Controls

a. CCM Controls
This is the core of the CCM V4. It includes 197 controls structured in 17 domains.
Each control is described by a:
• Control Domain: the name of the domain to which the control pertains.
• Control Title: the title of the control.
• Control ID: the control identifier.
• Control Specification: the requirement(s) description of the control.
In addition, this tab includes the following sections (groups of columns)

How to read the matrix [SOURCE: CSA – CCM]

CSA – Cloud Control Matrix

APPLICABILITY AND OWNERSHIP

Controls

Typical Control Applicability and Ownership:
This group of columns describes the typical applicability of controls for the three main cloud delivery models: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Additionally, the section explores the typical SSRM-based (Shared Security Responsibility Model) allocation of responsibilities for the implementation of a given CCM control between a cloud service provider (CSP) and a cloud service customer (CSC). The matrix clarifies if a control's responsibility should be "CSP-Owned", "CSC-Owned", or "Shared".
IMPORTANT NOTE: Both the control applicability to IaaS, PaaS, and SaaS models—and the control ownership attributions—are meant to represent a high-level simplification. The CCM user should revise those attributions depending on the contractually agreed SSRM for the specific cloud environment.

How to read the matrix [SOURCE: CSA – CCM]

CSA – Cloud Control Matrix

SECURITY DOMAINS

Domains

Example 1

- Audit & Assurance
- Application & Interface Security
- Business Continuity Management and Operational Resilience
- Change Control and Configuration Management
- Cryptography, Encryption & Key Management
- Datacenter Security
- Data Security and Privacy Lifecycle Management
- Governance, Risk and Compliance
- Human Resources
- Identity & Access Management
- Interoperability & Portability
- Infrastructure & Virtualization Security
- Logging and Monitoring
- Security Incident Management, E-Discovery, & Cloud Forensics
- Supply Chain Management, Transparency, and Accountability
- Threat & Vulnerability Management
- Universal Endpoint Management

CSA – Cloud Control Matrix

CONTROLS

Example of control

Control Domain	Control Title	Control ID	Control Specification	Implementation Guidelines
Audit & Assurance - A&A				
Audit & Assurance	Audit and Assurance Policy and Procedures	**A&A-01**	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Both the cloud service provider (CSP) and cloud service customer (CSC) should develop a "customized integrated framework" of audit and assurance policies and procedures. This framework should incorporate/demonstrate compliance to leading industry standards and self-imposed business requirements while providing appropriate coverage of controls to assess the respective cloud environment and corresponding services. At a minimum, audit and assurance policies and procedures should include: a. Audit and assurance functions indicating purposes, responsibilities, authorities, and accountabilities to ensure organizational independence, professional care, audit objectivity, and proficiency, b. Audit and assurance plans, c. Audit development policies and procedures to determine criteria and assertions against which the subject matter will be assessed, quality assurance and supervision, sufficient and appropriate evidence, in accordance with commonly accepted frameworks and audit best practices, d. Audit reporting to communicate audit results and findings, e. Follow-up activities to monitor audit findings implementation progress

CAIQ

QUESTIONAIRE

From control to question

Control Domain	Control Title	Control ID	Control Specification	Question ID	Consensus Assessments Question
Audit & Assurance - A&A					
	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	**A&A-01.1**	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?
				A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?

CSA – Cloud Control Matrix

SECURITY DOMAINS

Domains

- Audit & Assurance
- Application & Interface Security
- Business Continuity Management and Operational Resilience
- Change Control and Configuration Management
- Cryptography, Encryption & Key Management
- Datacenter Security
- Data Security and Privacy Lifecycle Management
- Governance, Risk and Compliance
- Human Resources
- Identity & Access Management
- Interoperability & Portability
- Infrastructure & Virtualization Security
- Logging and Monitoring
- Security Incident Management, E-Discovery, & Cloud Forensics
- Supply Chain Management, Transparency, and Accountability
- Threat & Vulnerability Management
- Universal Endpoint Management

Example 2

CSA – Cloud Control Matrix

CONTROLS

Example of control

Control Domain	Control Title	Control ID	Control Specification
Governance, Risk and Compliance	Governance Program Policy and Procedures	**GRC-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.

CAIQ

QUESTIONAIRE

From control to question

Control Domain	Control Title	Control ID	Control Specification	Question ID	Consensus Assessments Question
	Governance Program Policy and Procedures	GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	**GRC-01.1**	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?
				GRC-01.2	Are the policies and procedures reviewed and updated at least annually?

CSA – Cloud Control Matrix

SECURITY DOMAINS

Domains

- Audit & Assurance
- Application & Interface Security
- Business Continuity Management and Operational Resilience
- Change Control and Configuration Management
- Cryptography, Encryption & Key Management
- Datacenter Security
- Data Security and Privacy Lifecycle Management
- Governance, Risk and Compliance

Example 3

- Human Resources
- Identity & Access Management
- Interoperability & Portability
- Infrastructure & Virtualization Security
- Logging and Monitoring
- Security Incident Management, E-Discovery, & Cloud Forensics
- Supply Chain Management, Transparency, and Accountability
- Threat & Vulnerability Management
- Universal Endpoint Management

CSA – Cloud Control Matrix

CONTROLS

Example of controls

Control Domain	Control Title	Control ID	Control Specification
Infrastructure & Virtualization Security	Infrastructure and Virtualization Security Policy and Procedures	**IVS-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.

CAIQ

QUESTIONAIRE

From control to question

Control Domain	Control Title	Control ID	Control Specification	Question ID	Consensus Assessments Question
Infrastructure & Virtualization Security - IVS					
	Infrastructure and Virtualization Security Policy and Procedures	IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	**IVS-01.1**	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?
				IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?

STAR CERTIFICATION

CSA STAR [SOURCE: CLOUDSECURITYALLIANCE.ORG/STAR/]

Level 1: Self-Assessment

At level one organizations can submit one or both of the security and privacy self-assessments. For the security assessment, organizations use the Cloud Controls Matrix to evaluate and document their security controls. The privacy assessment submissions are based on the GDPR Code of Conduct.

Who should pursue level one?

Organizations should pursue this level if they are...
- Operating in a low-risk environment
- Wanting to offer increased transparency around the security controls they have in place.
- Looking for a cost-effective way to improve **trust** and **transparency**

STAR CERTIFICATION

CSA STAR [SOURCE: CLOUDSECURITYALLIANCE.ORG/STAR/]

Level 2: Third-Party Audit

Level 2 of STAR allows organizations to build off of other industry certifications and standards to make them specific for the cloud.
Organizations looking for a **third-party audit** can choose from one or more of the security and privacy audits and certifications. An organization's location, along with the regulations and standards it is subject to will have the greatest factor in determining which ones are appropriate to pursue.

Which organizations should pursue level 2?

Organizations should pursue this level if they are...
•Operating in a medium to high risk environment
•Already hold or adhere to the following: ISO27001, SOC 2, GB/T 22080-2008, or GDPR
•Looking for a cost-effective way to increase assurance for **cloud security** and **privacy**.

Some more readings…

ABOUT CLOUD AND INFORMATION SECURITY

- NIST definitions:
  https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
- AGID tools for cloud enabling:
  https://cloud.italia.it/programma-abilitazione-cloud/#kit
- CSA “SECURITY GUIDANCE For Critical Areas of Focus In Cloud Computing”
  https://cloudsecurityalliance.org/group/security-guidance/#_overview

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**
Simone **Soderi**
antonio.belli@unipd.it
simone.soderi@unipd.it

Thanks for your attention!

M1 - Certification and Frameworks for Organizations and management systems