RED ALERT LABS
IoT Security

EUROPEAN CLOUD SERVICE SCHEME (EUCS SCHEME)

TRAINING

September 2021

A4CEF

Co-financed by the Connecting Europe Facility of the European Union

EUCS SCHEME TRAINING – TABLE OF CONTENTS

- INTRODUCTION TO CLOUD SECURITY(DAY 1)
- INTRODUCTION TO THE CANDIDATE EUCS SCHEME(DAY 1)
- OVERVIEW ON THE CERTIFICATION PROCESS– PART 1 (DAY 1)
- OVERVIEW ON THE CERTIFICATION PROCESS – PART 2 (DAY 2)
- FOCUS ON SECURITY CONTROL(DAY 2)
- OVERVIEW OF THE NEXT PHASES & ONGOING WORK (DAY 2)

A4CEF
Co-financed by the Connecting Europe
Facility of the European Union

01

INTRODUCTION TO CLOUD SECURITY

- ➢ Cloud Services Definition
- ➢ Typical Cloud infrastructure
- ➢ Cloud Services Examples
- ➢ Domains and Emerging Verticals
- ➢ Cloud Market Projection
- ➢ Risk analysis overview: Attack surface, assets, threats,

CLOUD SERVICES DEFINITION

CLOUD SERVICES DEFINITION

ISO / IEC 17788 : 2014

DEFINITION OF **STAKEHOLDER** IN THE CLOUD COMPUTING MARKET AND THE THREE **TYPES OF SERVICES** OFFERED

ISO / IEC 17789 : 2014

DEFINE THE **REFERENCE FUNCTIONAL ARCHITECTURE**, I.E. HOW TO BUILD A CLOUD COMPUTING SERVICES PLATFORM, FOR THE SAKE OF **INTEROPERABILITY**

ISO / IEC 27018 : 2014

SETS THE **SECURITY RULES** TO BE APPLIED FOR PUBLIC CLOUD PROVIDERS IN ORDER TO **ENSURE THE PROTECTION OF PERSONAL DATA**, GUARANTEE **TRANSPARENCY** AND COMPLY WITH THEIR **REGULATORY OBLIGATIONS**.

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

CLOUD SERVICES **DEFINITION** – ISO/IEC 17788

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.

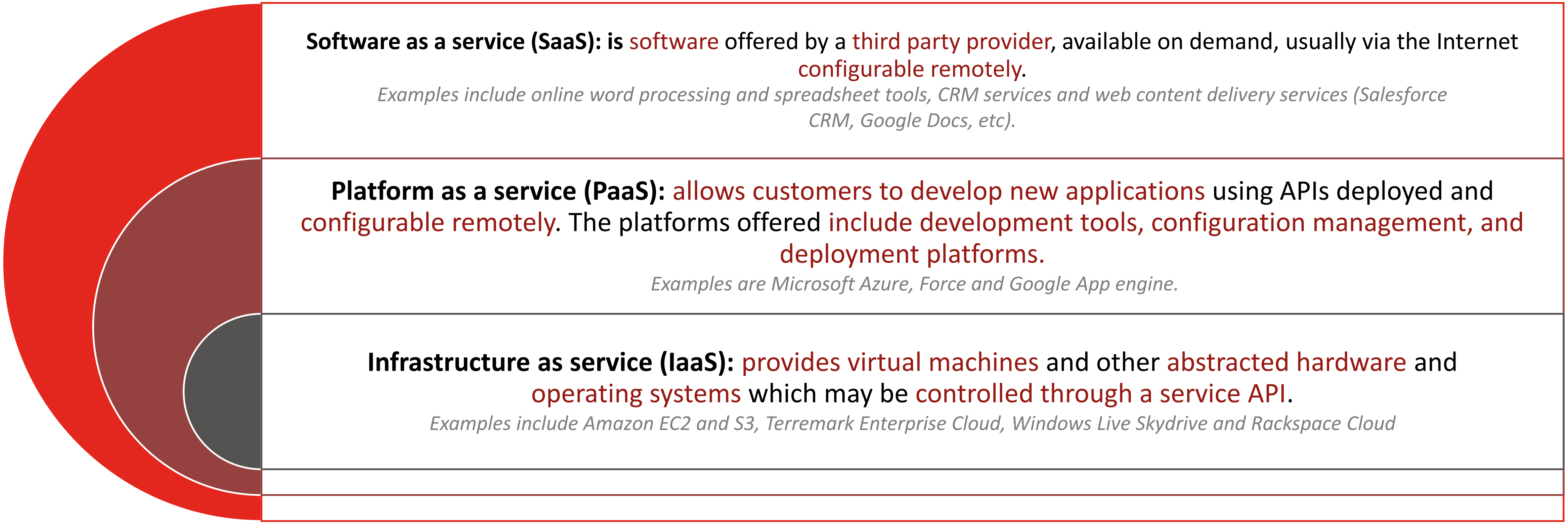
Cloud services: One or more capabilities offered via *cloud computing* invoked using a defined interface.

Cloud capabilities:

- Infrastructure (IaaS)
- Platform (PaaS)
- Application (SaaS)

CLOUD SERVICES DEFINITION – CLOUD COMPUTING RISK ASSESSMENT ENISA

There are three categories of cloud computing:



Software as a service (SaaS): is software offered by a third party provider, available on demand, usually via the Internet configurable remotely.

Examples include online word processing and spreadsheet tools, CRM services and web content delivery services (Salesforce CRM, Google Docs, etc).

Platform as a service (PaaS): allows customers to develop new applications using APIs deployed and configurable remotely. The platforms offered include development tools, configuration management, and deployment platforms.

Examples are Microsoft Azure, Force and Google App engine.

Infrastructure as service (IaaS): provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API.

Examples include Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live Skydrive and Rackspace Cloud

CLOUD SERVICES DEFINITION – CLOUD COMPUTING RISK ASSESSMENT ENISA

enisa

Clouds may also be divided into:

Public: available publicly - any organisation may subscribe

Private: services built according to cloud computing principles, but accessible only within a private network

Partner or Community: cloud services offered by a provider to a limited and well-defined number of parties.

A4CEF Co-financed by the Connecting Europe Facility of the European Union

CLOUD SERVICES DEFINITION - EUCS

In EUCS Scheme, ICT services matching the following criteria are referred to as “cloud services”.

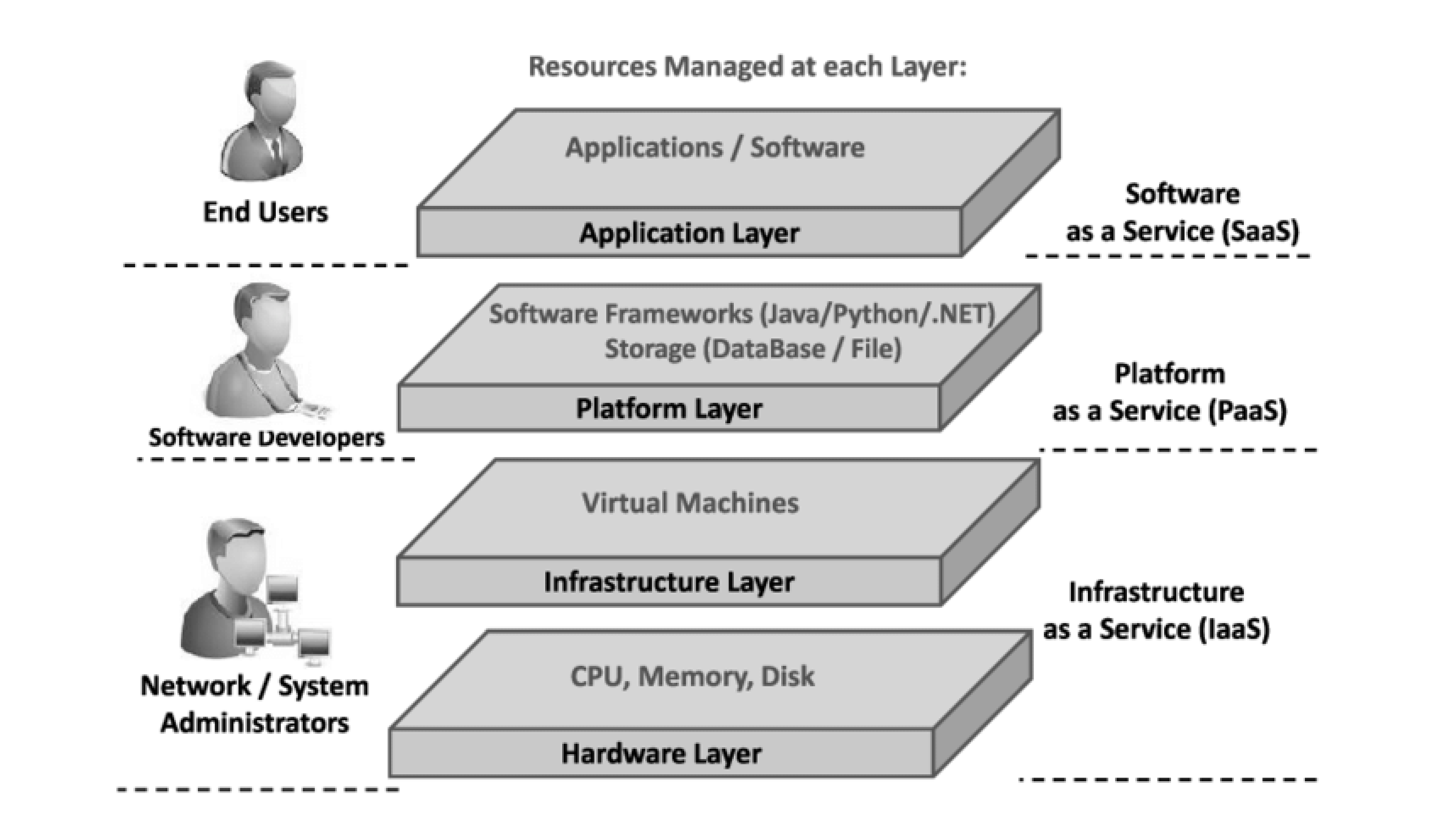
The ICT service implements one or more capabilities offered via cloud computing invoked using a defined interface [ISO17788].

The ICT service aims at reaching the assurance level corresponding to one of the three levels ‘basic’, ‘substantial’ and ‘high’ of the EUCSA as defined in the EUCS scheme

TYPICAL CLOUD INFRASTRUCTURE

Co-financed by the Connecting Europe
Facility of the European Union

TYPICAL CLOUD INFRASTRUCTURE



Resources Managed at each Layer:

End Users

Applications / Software

Application Layer

Software as a Service (SaaS)

Software Developers

Software Frameworks (Java/Python/.NET)
Storage (DataBase / File)

Platform Layer

Platform as a Service (PaaS)

Network / System Administrators

Virtual Machines

Infrastructure Layer

CPU, Memory, Disk

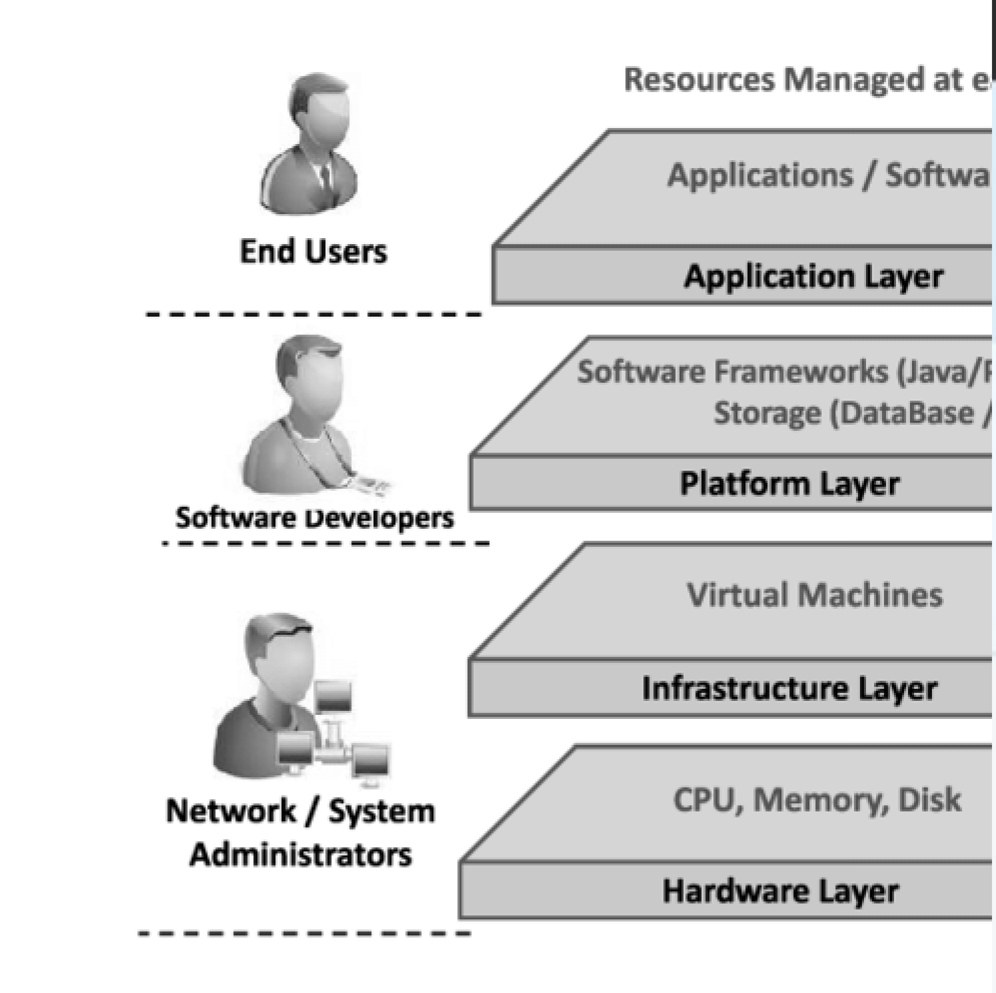
Hardware Layer

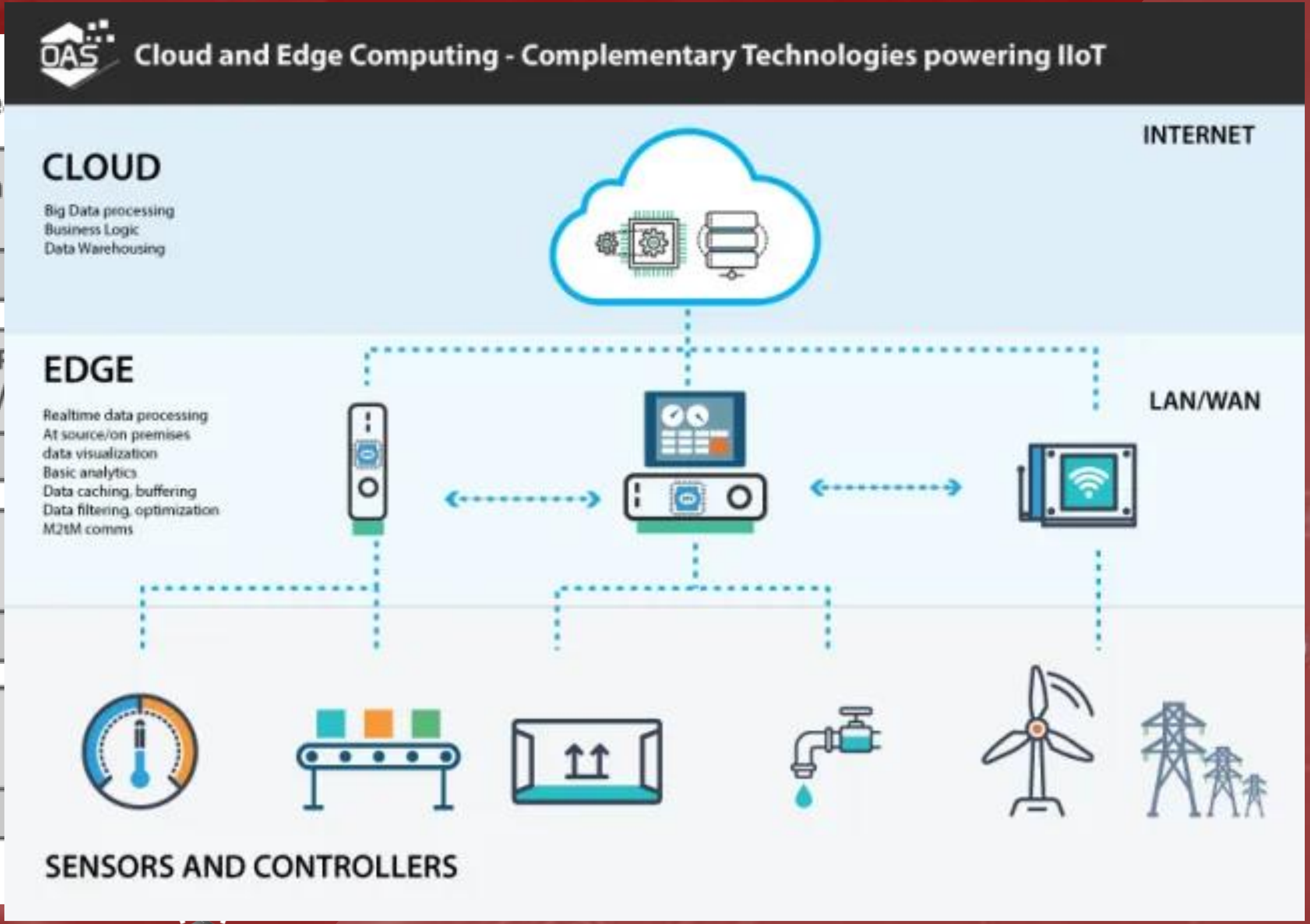
Infrastructure as a Service (IaaS)

https://www.researchgate.net/figure/Cloud-Computing-Architecture-39_fig4_257402

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

TYPICAL CLOUD INFRASTRUCTURE





https://softwareengineeringdaily.com/2018/09/14/edge-computing-and-the-future-of-the-cl

TYPICAL CLOUD INFRASTRUCTURE

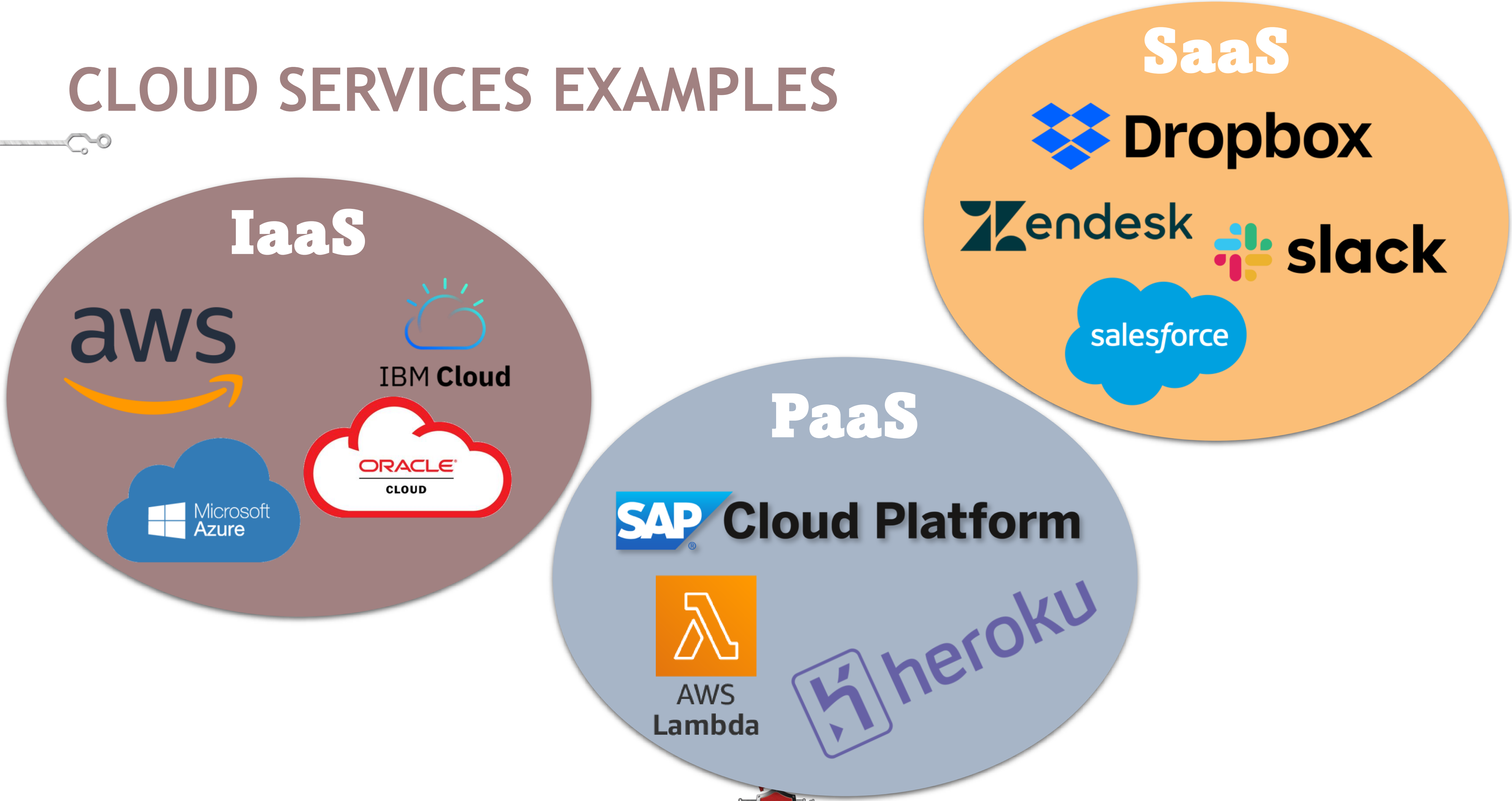
On-site	IaaS	PaaS	SaaS
🟦 Applications	🟦 Applications	🟦 Applications	🟥 Applications
🟦 Data	🟦 Data	🟦 Data	🟥 Data
🟦 Runtime	🟦 Runtime	🟥 Runtime	🟥 Runtime
🟦 Middleware	🟦 Middleware	🟥 Middleware	🟥 Middleware
🟦 O/S	🟦 O/S	🟥 O/S	🟥 O/S
🟦 Virtualization	🟥 Virtualization	🟥 Virtualization	🟥 Virtualization
🟦 Servers	🟥 Servers	🟥 Servers	🟥 Servers
🟦 Storage	🟥 Storage	🟥 Storage	🟥 Storage
🟦 Networking	🟥 Networking	🟥 Networking	🟥 Networking

🟦 You manage

🟥 Service provider manages

A4CEF
Co-financed by the Connecting Europe
Facility of the European Union

CLOUD SERVICES EXAMPLES



IaaS

aws

IBM Cloud

ORACLE CLOUD

Microsoft Azure

PaaS

SAP Cloud Platform

AWS Lambda

heroku

SaaS

Dropbox

zendesk

slack

salesforce

DOMAINS AND EMERGING VERTICALS

In this highly digitalized era, cloud computing offers immense benefits to a wide range of industries. It reduces storage costs while at the same time increasing storage capacity, and it is flexible enough to adapt to any business environment.

- Healthcare

- Banking

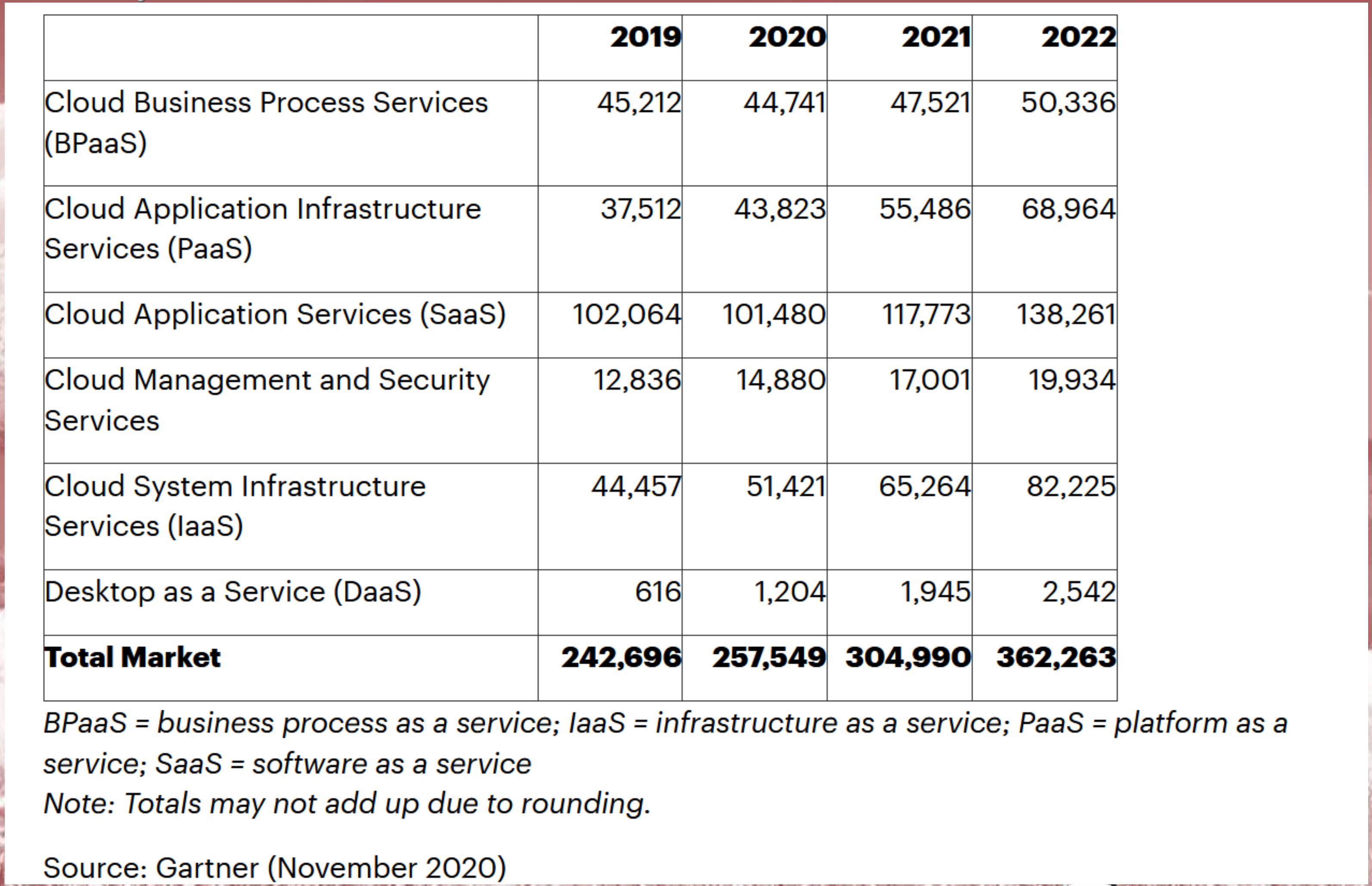
- IoT

- Manufacturing

- Self-driving vehicles

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

CLOUD MARKET PROJECTION



	2019	2020	2021	2022
Cloud Business Process Services (BPaaS)	45,212	44,741	47,521	50,336
Cloud Application Infrastructure Services (PaaS)	37,512	43,823	55,486	68,964
Cloud Application Services (SaaS)	102,064	101,480	117,773	138,261
Cloud Management and Security Services	12,836	14,880	17,001	19,934
Cloud System Infrastructure Services (IaaS)	44,457	51,421	65,264	82,225
Desktop as a Service (DaaS)	616	1,204	1,945	2,542
Total Market	**242,696**	**257,549**	**304,990**	**362,263**

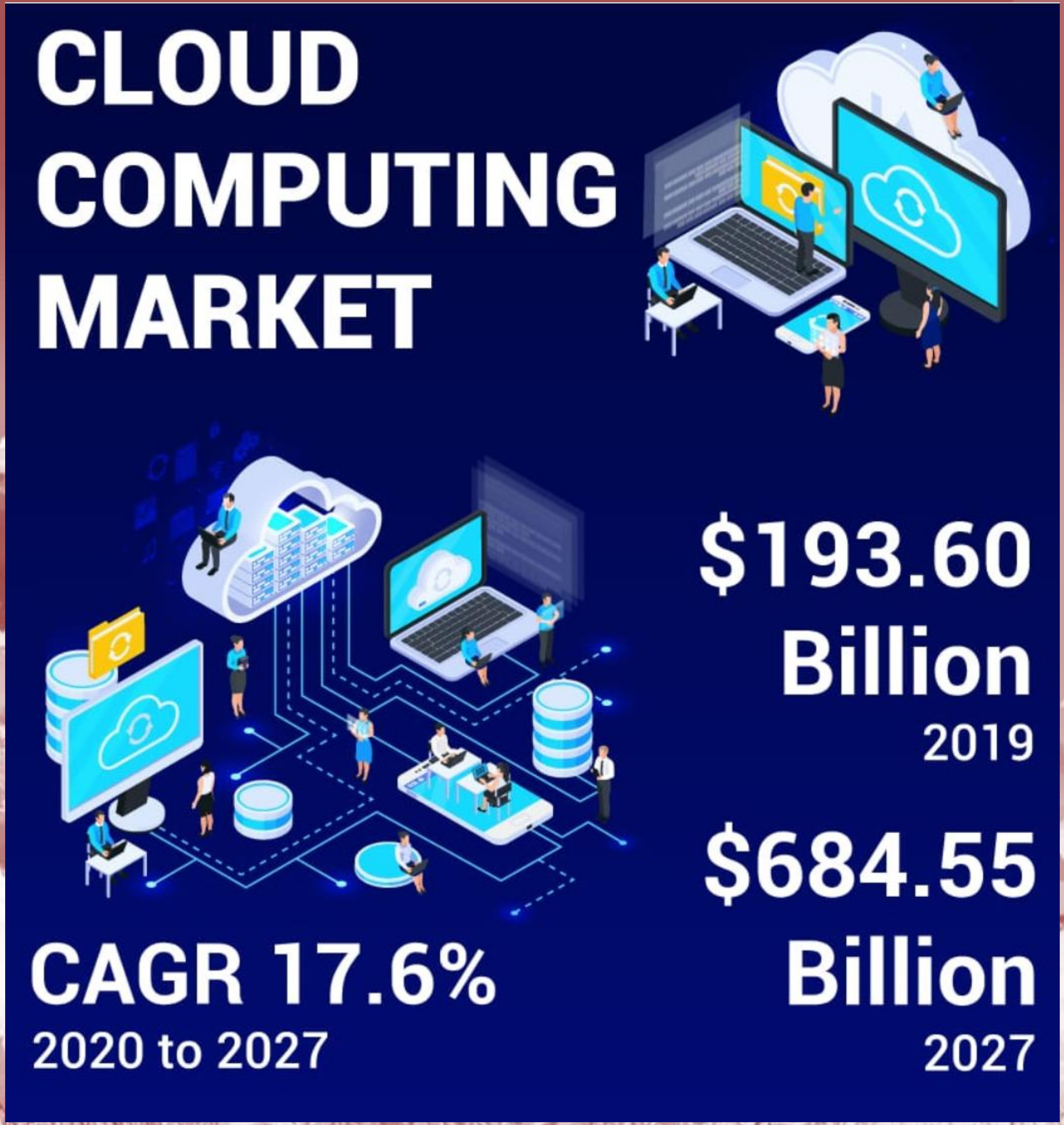
BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service
Note: Totals may not add up due to rounding.

Source: Gartner (November 2020)

Worldwide Public Cloud Services End-User Spending Forecast (Millions of U.S. Dollars)

A4CEF Co-financed by the Connecting Europe Facility of the European Union

CLOUD MARKET PROJECTION



CLOUD COMPUTING MARKET

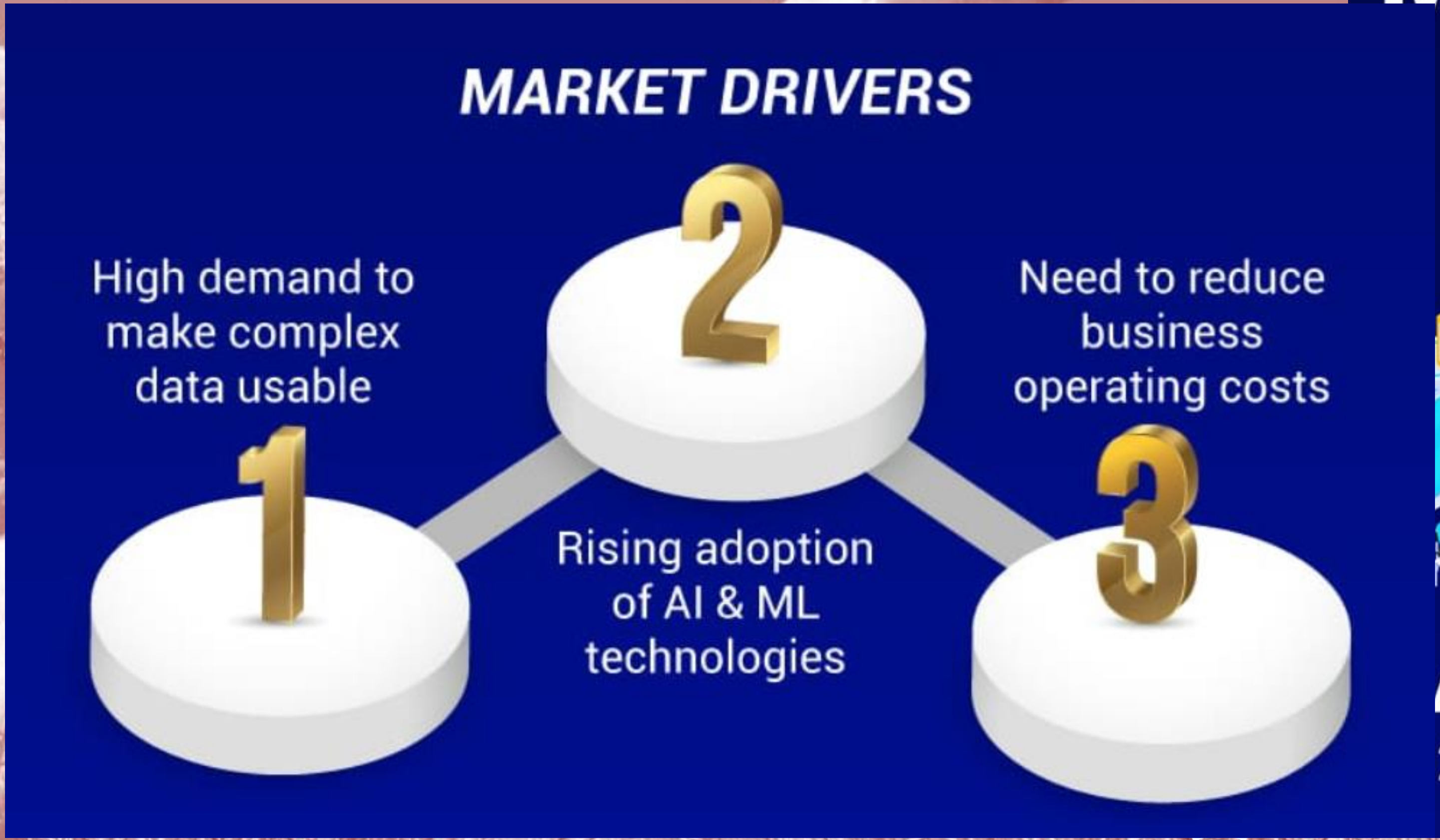
$193.60 Billion
2019

$684.55 Billion
2027

CAGR 17.6%
2020 to 2027

https://www.fortunebusinessinsights.com

CLOUD MARKET PROJECTION

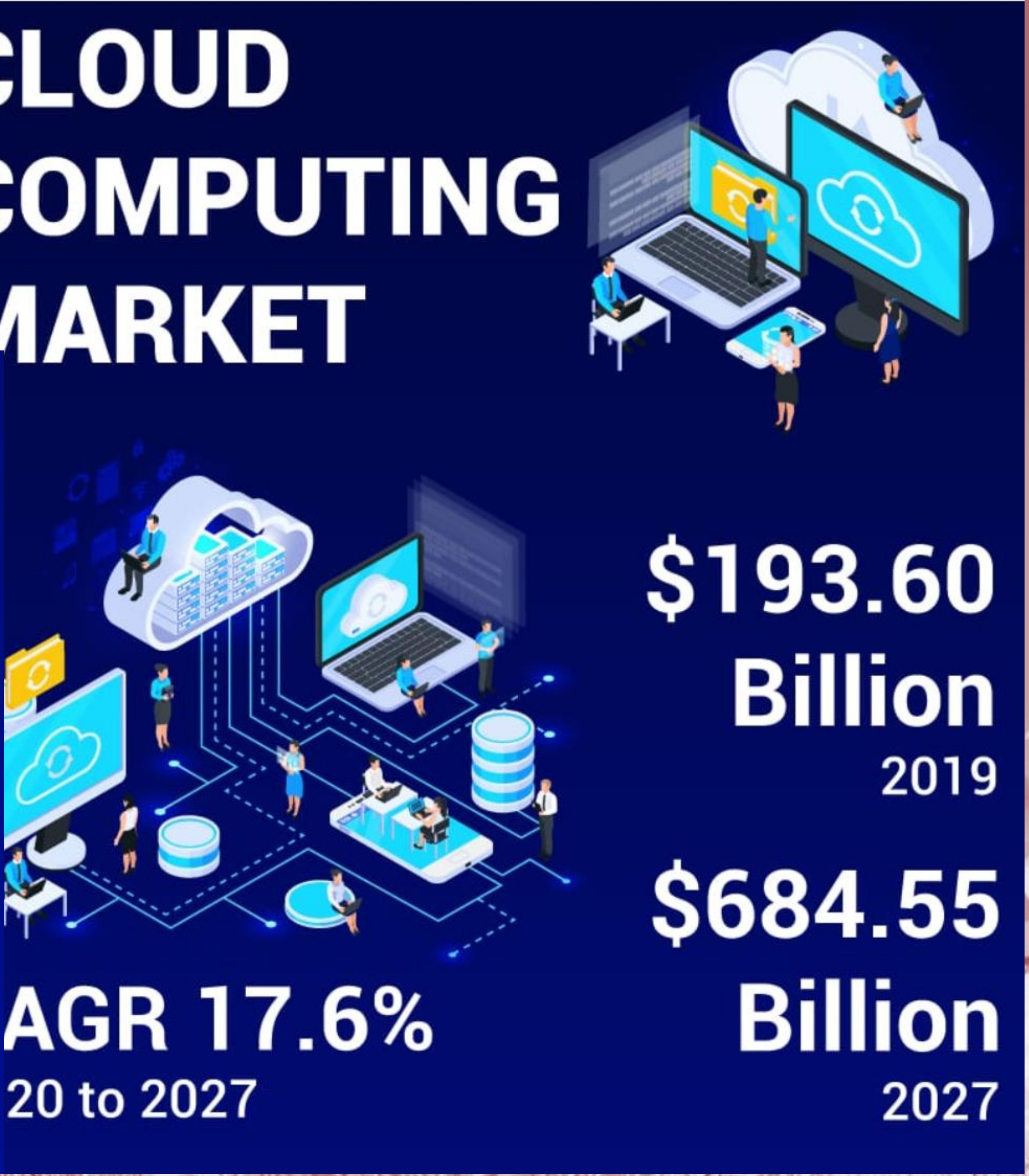


MARKET DRIVERS

1 High demand to make complex data usable

2 Rising adoption of AI & ML technologies

3 Need to reduce business operating costs



CLOUD COMPUTING MARKET

$193.60 Billion 2019

$684.55 Billion 2027

AGR 17.6%
20 to 2027

HOW ABOUT SECURITY?

Co-financed by the Connecting Europe Facility of the European Union

RISK ANALYSIS: THE CLOUD ATTACK SURFACE

EXTERNAL THREATS

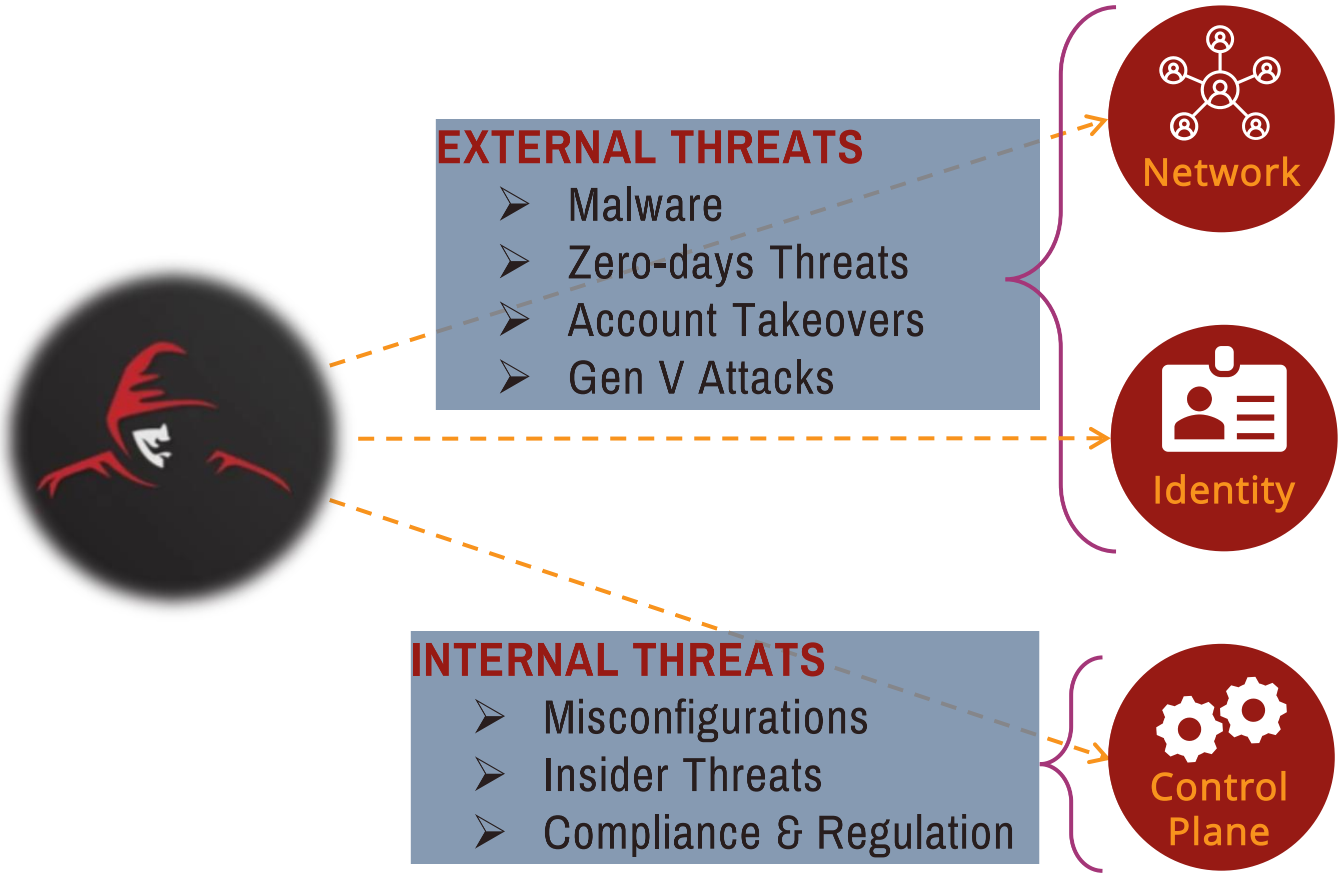
- Malware
- Zero-days Threats
- Account Takeovers
- Gen V Attacks

INTERNAL THREATS

- Misconfigurations
- Insider Threats
- Compliance & Regulation

RISK ANALYSIS: THE CLOUD ATTACK SURFACE

Surface of Attacks



EXTERNAL THREATS

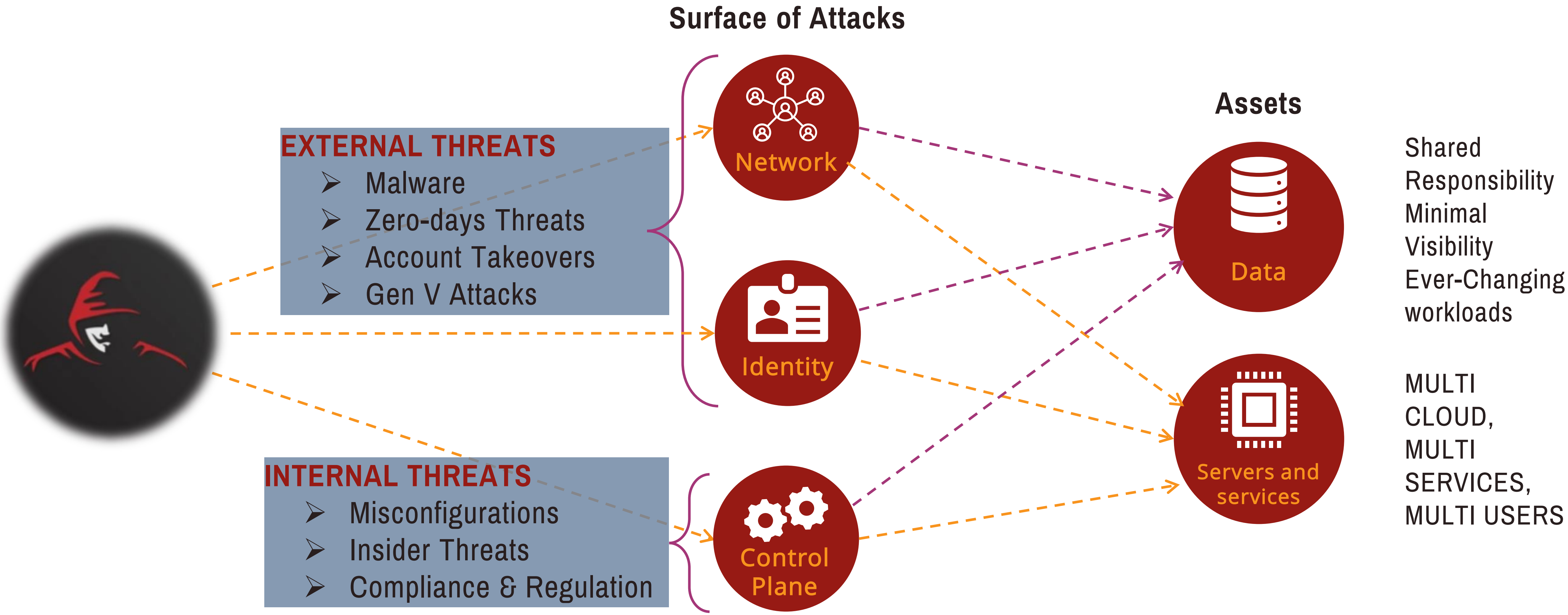
- Malware
- Zero-days Threats
- Account Takeovers
- Gen V Attacks

INTERNAL THREATS

- Misconfigurations
- Insider Threats
- Compliance & Regulation

Co-financed by the Connecting Europe Facility of the European Union

RISK ANALYSIS: THE CLOUD ATTACK SURFACE



Surface of Attacks

EXTERNAL THREATS

- ➤ Malware
- ➤ Zero-days Threats
- ➤ Account Takeovers
- ➤ Gen V Attacks

INTERNAL THREATS

- ➤ Misconfigurations
- ➤ Insider Threats
- ➤ Compliance & Regulation

Shared Responsibility
Minimal Visibility
Ever-Changing workloads

MULTI CLOUD, MULTI SERVICES, MULTI USERS

RISK ANALYSIS: EXAMPLES OF ASSETS (ENISA)

- Company reputation
- Customer trust
- Employee loyalty and experience
- Intellectual property
- Personal data
- Service delivery – real time services
- Access control/authentication/authorization (root/admin other)
- Credentials
- Management interface APIs
- Network (connections, etc.)
- Physical Hardware
- Operational logs
- Security logs
- Backup or archive data
- Others

RISK ANALYSIS: MAJOR THREATS (CLOUD SECURITY ALLIANCE)

CSA cloud security alliance®

- Data breaches
- Misconfiguration and Inadequate Change Control
- Lack of Cloud Security Architecture and Strategy
- Insufficient Identity, Credential, Access and Key Management
- Account hijacking
- Insider Threat
- Insecure Interfaces and APIs
- Weak Control Plane
- Metastructure and Applistructure Failures
- Limited Cloud Usage Visibility
- Abuse and Nefarious Use of Cloud Services

RISK ANALYSIS: CLOUD SCENARIOS/ VULNERABILITIES TO WATCH OUT IN 2021

Account Hijacking

- Phishing
- Keyloggers
- Buffer Overflow attacks
- Cross-site Scripting (XSS) attacks
- Brute force attacks

Data breaches

Insecure APIs

Malicious insiders

System vulnerabilities

https://www.alertlogic.com/blog/top-cloud-vulnerabilities/

QUIZ

- Could you name 2 Cloud capabilities?
- Could you name 2 emerging domains/verticals for Cloud?
- Could you name 1 market driver for Cloud use?
- Could you name 2 sensitive assets of the Cloud Infrastructure?

QUIZ

- Could you name 2 Cloud capabilities?

IaaS, PaaS, SaaS.

- Could you name 2 emerging domains/verticals for Cloud?

Healthcare, Banking, IoT, Manufacturing, Self-driving vehicle

- Could you name 1 market driver for Cloud use?

High demand to make complex data usable, Rising adoption of AI & ML technologies, Need to reduce business operating costs.

- Could you name 2 sensitive assets of the Cloud Infrastructure?

Credentials, security logs, operational logs, physical hardware, personal data, sensitive data, intellectual property, …

A4CEF
Co-financed by the Connecting Europe
Facility of the European Union

02

INTRODUCTION TO THE CANDIDATE EU CLOUD SERVICE SCHEME

- Introduction (EU CSA, EUCS history, terms and definitions, EUCS timing, …)
- Structure of the candidate scheme
- Key roles and actors
- Bringing trust to the Cloud: why a certification scheme is important?
- Consider security assurance levels
- Beneficiaries of Cloud Service certification scheme
- Scheme Stakeholders
- Used standards in the EUCS
- Subject matter and Scope – Target of Evaluation
- Certification
- Key benefits of the EUCS scheme

INTRODUCTION : REMINDER – EU CYBERSECURITY ACT

Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the EU Cybersecurity Agency) and on information and communications technology cybersecurity certification.

MAKING ENISA PERMANENT AND ADDING NEW MISSIONS

- From cybersecurity awareness to capacity building to CSIRTs network secretariat and the organization of EU-level exercises
- Also adding a mission related to certification, supporting policy making

ALSO DEFINING A CYBERSECURITY CERTIFICATION FRAMEWORK

- To increase the use of cybersecurity certification in Europe
- To go beyond national schemes and offer mutual recognition at European level
- Enabling customers to take informed decisions about cybersecurity
- Based on regulation 765/2008 and ISO/IEC 17065, and the existing accreditation network

A4CEF Co-financed by the Connecting Europe Facility of the European Union

INTRODUCTION: EUCS HISTORY

European Commission Request in accordance with **Article 48.2 of the Cybersecurity Act**.

> In duly justified cases, the Commission or the ECCG may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme which is not included in the Union rolling work programme. The Union rolling work programme shall be updated accordingly.
>
> *EU Cybersecurity Act – Article 48-2.*

➔ ENISA set up an Ad Hoc Working Group (AHWG) to support the preparation of a **candidate EU cybersecurity certification scheme on cloud services.**

➔ EUCS supports the three assurance levels in the EUCSA**: 'basic', 'substantial' and 'high'.**

- ➔ Requirements at level 'high' are demanding and close to the state-of-the-art
- ➔ whereas the requirements at level 'basic' define a minimum acceptable baseline for cloud cybersecurity

INTRODUCTION – TERMS AND DEFINITIONS

Reused from ISO 17788

Term	Abbreviations	Definition
Application capabilities type		Cloud capabilities type in which the cloud service customer can use the cloud service provider's applications
Cloud capabilities type		Classification of the functionality provided by a cloud service to the cloud service customer, based on resources used.
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.
Cloud service		One or more capabilities offered via cloud computing invoked using a defined interface.
Cloud service customer	CSC	Party which is in a business relationship for the purpose of using cloud services.
Cloud service customer data		*Class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service, or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer via the published interface of the cloud service.* *NOTE 1 – An example of legal controls is copyright.* *NOTE 2 – It may be that the cloud service contains or operates on data that is not cloud service customer data; this might be data made available by the cloud service providers, or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the cloud service customer using the capabilities of the cloud service on this data is likely to be cloud service customer data, following the general principles of copyright, unless there are specific provisions in the cloud service agreement to the contrary.*

INTRODUCTION – TERMS AND DEFINITIONS

Reused from ISO 17788

Term	Abbreviations	Definition
Cloud service derived data		*Class of data objects under cloud service provider control that are derived as a result of interaction with the cloud service by the cloud service customer.* *NOTE – Cloud service derived data includes log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorized users and their identities. It can also include any configuration or customization data, where the cloud service has such configuration and customization capabilities.*
Cloud service provider	CSP	Party which makes cloud services available
Cloud service provider data		*Class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider* *NOTE – Cloud service provider data includes but is not limited to resource configuration and utilization information, cloud service specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.*
Cloud service user	User	Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services. NOTE: Examples of such entities include devices and applications.
Infrastructure capabilities type		Cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources
multi-tenancy		Allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another.
on-demand self-service		Feature where a cloud service customer can provision computing capabilities, as needed, automatically or with minimal interaction with the cloud service provider.
Platform capabilities type		Cloud capabilities type in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider.
tenant		One or more cloud service users sharing access to a set of physical and virtual resources.

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

INTRODUCTION – SPECIFIC TERMINOLOGY

Term	Abbreviation	Definition
Ad hoc working group	AHWG	The working group that supports ENISA in the definition of the certification scheme on cloud services
Conformance Assessment Body	CAB	An entity in charge of the certification of products, services, and processes, typically according to ISO17065.
	CSP-CERT	The Working Group on Certification for Cloud Service Providers, who produced a report in 2019 that provides a starting point for the development of the certification schemes for cloud services.
European Cybersecurity Certification group	ECCG	A group composed of representatives of national cybersecurity certification authorities or other relevant national authorities (EUCSA, Article 62)
	EUCC	The candidate European cybersecurity certification scheme to serve as a successor to the existing SOG-IS
	EUCS	The present candidate European cybersecurity certification scheme for cloud services
Cybersecurity Act	EUCSA	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
National Cybersecurity Certification Authority	NCCA	A national authority in every EU Member State that is in charge of the oversight of the certification framework in its country, and also in charge of issuing certificates at 'high' level in its own country.
Stakeholder Cybersecurity Certification Group	SCCG	Advisory group composed of members selected from among recognised experts representing the relevant stakeholders

A4CEF Co-financed by the Connecting Europe Facility of the European Union

INTRODUCTION: WHAT ELSE I SHOULD KNOW ABOUT THE SCHEME?

CABs

Based on the ISO/IEC 17065 standard in terms of applicable requirements to CABs performing certification

Basic simplified methodology

The candidate scheme also defines a simplified assessment methodology for the EUCSA assurance level ‘basic’.

The methodology is based on a self-assessment performed by the cloud service provider

Whose results are then audited by a conformity assessment body.

Inspiration from

the German C5 scheme,

the French SecNumCloud scheme,

the proposals in the CSP-CERT report,

principles in other schemes used in Europe.

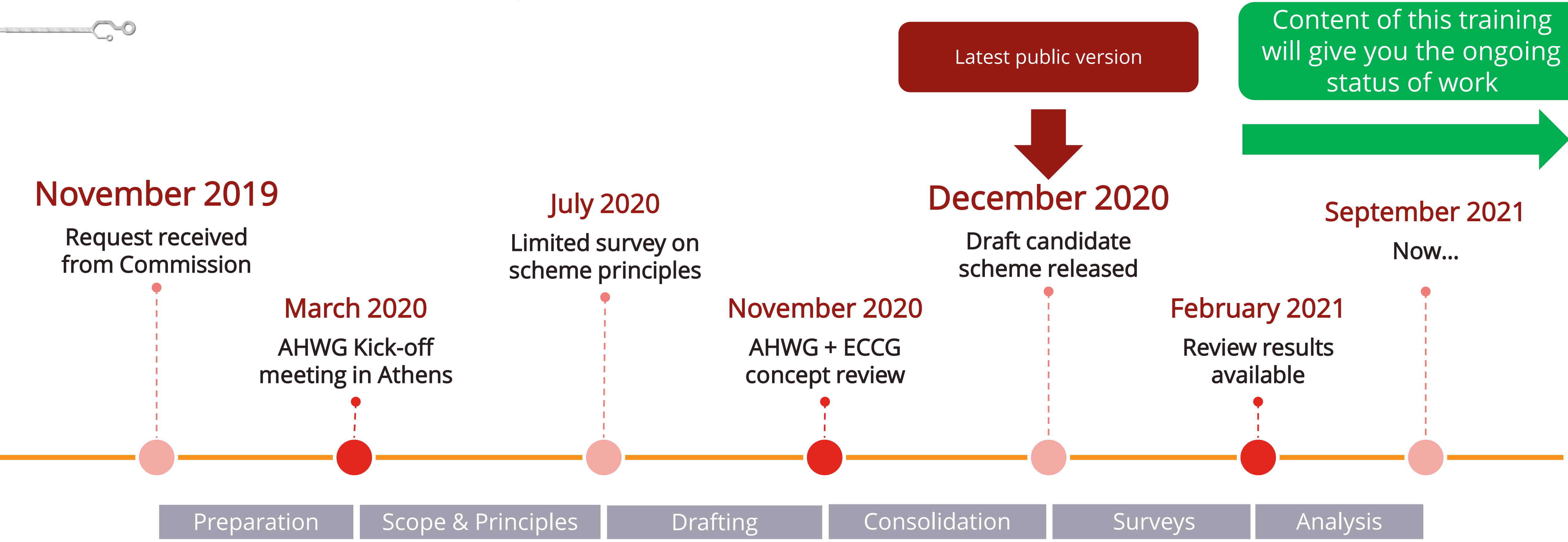
Not standalone

Finally, the EUCS scheme is not a standalone scheme; it is part of the European cybersecurity certification framework.

A4CEF Co-financed by the Connecting Europe Facility of the European Union

EUCS Timing

INTRODUCTION: WHERE ARE WE NOW?



Latest public version

Content of this training will give you the ongoing status of work

November 2019
Request received from Commission

March 2020
AHWG Kick-off meeting in Athens

July 2020
Limited survey on scheme principles

November 2020
AHWG + ECCG concept review

December 2020
Draft candidate scheme released

February 2021
Review results available

September 2021
Now…

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

INTRODUCTION – RELATIONSHIP WITH OTHER SCHEMES

This scheme will be a regulation, similar to National schemes

- If national schemes in europe are deemed equivalent, then they shall stop emitting certificates and be replaced by the european scheme
- In that case, a transition will be organized between the scheme, in particular regarding the recognition of certificates and of objective evidence obtained previously
- There may be official mutual recognition with third countries, but none is foreseen at this stage

There is no formal relationship with private schemes

- There will be neither transition nor recognition
- We are aware that these schemes will co-exist
- A key objective is to enable optimized certification strategies, with significant reuse of objective evidence

A4CEF Co-financed by the Connecting Europe Facility of the European Union

INTRODUCTION – SUMMARY OF THE CANDIDATE SCHEME

A scheme implementing a regulation

Following the EU Cybersecurity Act

Defined itself as a regulation

Implemented by EU Member States

Part of a larger framework

Part of the EU CSA Certification Framework

Following rules of openness and standards use

Possibly reused and refined in vertical schemes

A horizontal scheme

Catering to a wide array of cloud services

Defining 3 assurance levels, based on risk levels

Providing baselines applicable to all services

Done + available soon

Principles fixed by the end of June 2020 **(Done)**

Candidate scheme by the end of the year **(Done)**

Implementing Act around mid-2021 **(available soon)**

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

STRUCTURE OF THE CANDIDATE SCHEME

Chapters 2 to 23 follow the same structure. Each one of them provides content related to one of the points raised in Article 54(1). There are 22 such points, numbered (a) to (v), so there are 22 chapters.

Every chapter contains the following sections:

- An excerpt from Article 54 defining the topic to be addressed in the chapter.
- A proposed text, which is the proposed content for the scheme. This content defines scheme rules and requirements and makes extensive use of “shall” to express a requirement, and “may” to express an option.
- A rationale, starting when available by relevant excerpts from the EU Cybersecurity Act, and providing additional information, reasons for making the choices in the proposed text, and any other additional information deemed necessary.

A4CEF Co-financed by the Connecting Europe Facility of the European Union

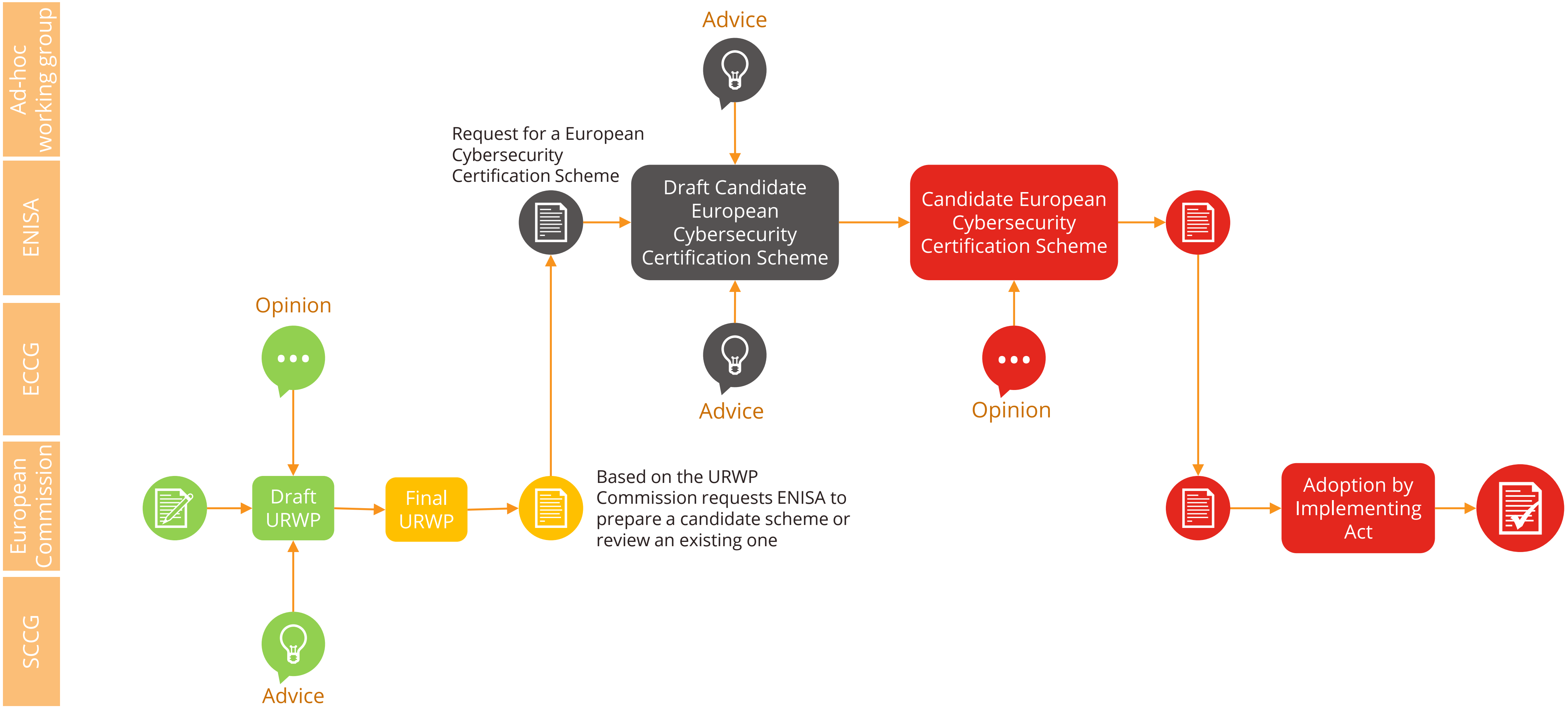
INTRODUCTION: WHERE CAN I FIND THE LATEST VERSION?

https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

STRUCTURE OF THE SCHEME – EUCSA ART 54.1

a. **Subject matter and scope**
b. Clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme
c. References to the international, European or national standards applied in the evaluation, and if not available to technical specifications
d. **One or more assurance levels**
e. An indication whether conformity self-assessment is authorized
f. **Specific requirements for the CABs**
g. **Specific evaluation criteria and methods to be used**
h. The information necessary for the evaluation or otherwise to be made available by the applicant
i. If applicable, conditions of use of marks and labels
j. **Rules for monitoring compliance of certified and self-assessed products**
k. **Conditions for issuing, maintaining, continuing certificates, and for extending/reducing scope**
l. Rules concerning the consequences for products that have been certified or self-assessed and do not comply
m. Rules concerning how previously undetected vulnerabilities should be reported and handled
n. Rules concerning the retention of records by CABs
o. Identification of national and international schemes with the same scope
p. Content and format of the certificates and EU statements of conformity
q. The period of the availability of EU statements of conformity and related documentation
r. **Maximum period of validity of certificates**
s. Disclosure policy for certificate issuance, withdrawal, amendment
t. **Conditions for mutual recognition with third countries**
u. Where applicable, rules for peer assessment
v. Formats and procedures to be followed by suppliers to provide supplementary cybersecurity information

STAKEHOLDERS – PREPARATION PROCESS



Ad-hoc working group
ENISA
ECCG
European Commission
SCCG
Advice
Request for a European Cybersecurity Certification Scheme
Draft Candidate European Cybersecurity Certification Scheme
Candidate European Cybersecurity Certification Scheme
Opinion
Advice
Opinion
Draft URWP
Final URWP
Based on the URWP Commission requests ENISA to prepare a candidate scheme or review an existing one
Adoption by Implementing Act
Advice

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

what are the key roles and actors?

STAKEHOLDERS - THE CLOUD SERVICE PROVIDER

Single person or group

Top management
CxO, board, …

Authorized body
Delegation from top management

Single person

Employee
Subject to HR policies

Internal employee
Employed by the CSP

External employee
Employed by subcontractor

Owner
Person responsible for something

Risk owner
In charge of managing a risk

Asset owner
With custody of an asset

Subject matter expert
In charge of a topic

what are the key roles and actors?

STAKEHOLDERS - OTHER

Legal entity

Subcontractor
Company under contract

Service provider
Subcontractor for services

Subservice provider
Provides part of cloud service

Cloud customer
The CSP's customer

Supplier
Subcontractor for products

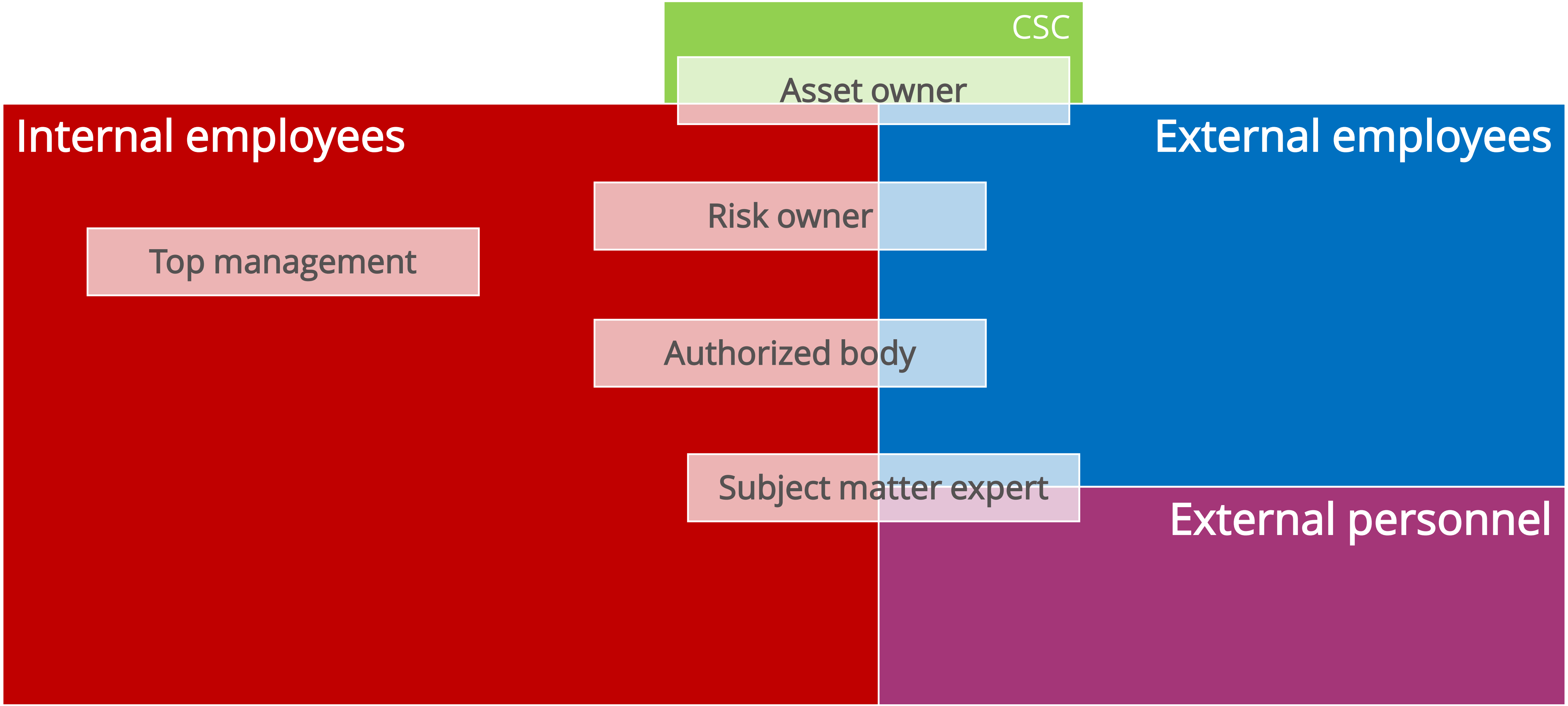
Single person

External personnel
Not subject to HR policies

A4CEF Co-financed by the Connecting Europe Facility of the European Union

what are the key roles and actors?

STAKEHOLDERS – MAPPING OF CSP ROLES



QUIZ

- “Level ‘basic’ define a maximum acceptable baseline for cloud cybersecurity”. True or False?
- What these acronyms stand for: CSP & CSC?
- What 2 major European schemes the EUCS is inspired from?
- The EUCS is a vertical scheme. True or false?
- Please tell which sentence is wrong when it comes to Private schemes:
  - There will be **a transition and a recognition**
  - We are aware that these schemes **will co-exist**
  - A **key objective** is to enable **optimized certification strategies**, with **significant reuse** of objective **evidence**

A4CEF Co-financed by the Connecting Europe Facility of the European Union

QUIZ

- “Level ‘basic’ define a maximum acceptable baseline for cloud cybersecurity”. True or False?

False. “Level ‘basic’ define a minimum acceptable baseline for cloud cybersecurity”.

- What these acronyms stand for: CSP & CSC?

CSP: Cloud Service Provider, CSC: Cloud Service Customer

- What 2 major European schemes the EUCS is inspired from?

German C5 scheme and French secnumCloud

- The EUCS is a vertical scheme. True or false?

False. It is a horizontal scheme providing baselines applicable to all services

- Please tell which sentence is wrong when it comes to Private schemes:
  - ~~There will be a transition and a recognition~~
  - We are aware that these schemes will co-exist
  - A key objective is to enable optimized certification strategies, with significant reuse of objective evidence

A4CEF Co-financed by the Connecting Europe Facility of the European Union

WHY A CERTIFICATION SCHEME IS IMPORTANT?

A4CEF

Co-financed by the Connecting Europe
Facility of the European Union

BRINGING TRUST TO CLOUD: WHY A CERTIFICATION SCHEME IS IMPORTANT

http://www.flickr.com/photos/lwr/

"TRUST should be further strengthened by offering information in a transparent manner on the level of security of ICT products, ICT services and ICT processes …"

"An increase in trust can be facilitated by Union-wide CERTIFICATION providing for common cybersecurity requirements and evaluation criteria across national markets and sectors."

Cybersecurity Act – Section (7)

CERTIFICATION ➔ TRUST

FRAGMENTATION OF THE CLOUD COMPUTING INDUSTRY

Currently, cloud computing products and services in France and Germany

- Have to obtain two specific certifications to be accepted across the entirety of the EU: the secnumcloud and the compliance controls catalogue (C5).
  ➔ *A problem arises because these two certification processes seem to be at odds with each other.*

A widely accepted solution

- That would bring forth a host of other benefits and lower the fragmentation of the cloud computing industry is a unified certification under the EU cybersecurity act prepared by ENISA and certification stakeholders.
  ➔ *All EU Member States would accept this single certification and would greatly aid the cloud computing market as it stands today.*

BENEFITS OF A SINGLE CERTIFICATION SCHEME

Cost reduction

Reduce cost for compliance

Save around 1.1 € billion per year

Shorter certification time

audit and testing processes required for certification last around 7-9 months

This time should be shortened to only 4 to 6 months

Improved Client Trust

Currently, end-users cannot effectively compare and decide which standard is best suited for their needs.

As a result, the end-users' (clients') trust in cloud computing services and products is greatly diminished.

Increased Market Competition

Bigger competition among suppliers leads to a broader choice of products and services.

opportunity to choose between different options until they find one that works best for them.

Lower R&D Expenses

Cloud system providers waste a lot of money on research

Participating in standardization lowers the economic risk, but it also reduces R&D costs.

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

WHAT ABOUT ASSURANCE LEVELS?

Co-financed by the Connecting Europe
Facility of the European Union

ASSURANCE LEVELS - WHAT IS ASSURANCE?

Reminder

Assurance is a very loaded word, used in many different contexts, so having a shared understanding is really necessary.

WEBSTER'S, 1913 (FROM WIKIPEDIA)

- The **act** of assuring; a **declaration** tending to inspire full confidence; that which is designed to give **confidence**.

SOC2, ONE CENTURY LATER

- An objective examination of evidence for the purpose of providing the reader or user of the report with a **level** of comfort that security **goals** have been adequately **met** through the organization's risk management and governance processes

COMMON CRITERIA, CIRCA 2000

- *assurance level:* **grounds** for **confidence** that a TOE **meets** the **SFRs**

A set of **actions** to bring some **level** of **confidence** that some **requirements** are **met**

ASSURANCE LEVELS - GENERATING ASSURANCE

Reminder

So, assurance is what we do with a scheme…

DEFINITIONS IN ISAE 3000

- *Assurance engagement:* An engagement in which a practitioner aims to **obtain sufficient appropriate evidence** in order to express a conclusion designed to **enhance the degree of confidence** of the intended users other than the responsible party about the subject matter information…
- *Reasonable assurance engagement:* An assurance engagement in which the practitioner **reduces engagement risk** to an acceptably **low level in the circumstances** of the engagement as the basis for the practitioner's conclusion…

DEFINITION IN SOC2

- *Reasonable assurance:* A **high**, but not absolute, **level** of assurance

A4CEF Co-financed by the Connecting Europe Facility of the European Union

ASSURANCE LEVELS - GENERATING ASSURANCE

Reminder

Every framework defines how assurance is generated.

IN NIST SP 800-53R5 (DRAFT)

- “Assurance is the measure of confidence that the system functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system—thus possessing the capability to accurately mediate and enforce established security and privacy policies.”
- Assurance-related controls “narrow the analysis for instance by increasing the discipline applied to the system architecture, software design, specifications, code style, and configuration management”

IN ISO/IEC 15408-3 (COMMON CRITERIA)

- CC defines Security Assurance Requirements (SARs) that look a lot like assurance-related controls
- These SARs are combined in sets that define Evaluation Assurance Levels (EALs)

A4CEF Co-financed by the Connecting Europe Facility of the European Union

ASSURANCE LEVELS - DEFINITION

Let's talk about this

What is an assurance level? This is a central question in the definition of a scheme.

DEFINITION FROM EC 881/2019 (EU CYBERSECURITY ACT):

- *assurance level:* a basis for confidence that an [ICT service] meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an [ICT service] has been evaluated but as such does not measure the security of the [ICT service] concerned

IN THE CLOUD SCHEME:

- Assurance is about building confidence that a cloud service meets the scheme's requirements
- An assurance level reflects the level of scrutiny to which the cloud service is submitted
- Higher assurance levels will include more assurance-related controls
- Higher assurance levels will have increased assessment requirements to match the circumstances of the audit
- Higher assurance levels may have higher functional requirements if they help to build confidence

A4CEF Co-financed by the Connecting Europe Facility of the European Union

WHO ARE THE BENEFICIARIES OF CLOUD SERVICE CERTIFICATION SCHEME

BENEFICIARIES OF CLOUD SERVICE CERTIFICATION SCHEME: WHO?

Cloud service providers (CSPs)

- who wish to assess the security of their cloud services through third-party certification

Cloud service customers (CSCs)

- who wish to benefit from the evidence provided with certified cloud services to make informed decisions related to the security of these cloud services

Regulatory authorities

- who wish to include security and assurance requirements on cloud services within their regulations and directives

BENEFICIARIES OF CLOUD SERVICE CERTIFICATION SCHEME : HOW?

CSP

- to **assess how a cloud service**, as described by the CSP, **meets the requirements** of a predefined **set of security control objectives** and a related **set of measures**, when used **according to security recommendations** provided by the CSP

CSC

- to **provide CSCs the information** required **to make informed choices** about the procurement and operation of cloud services, and to **allow CSCs to use certified cloud services** in their own development activities, and to **meet their own security compliance requirements**;

Regulatory authorities

- to **allow regulatory authorities** to **refer to the scheme** in **European and national regulations**, including criteria based on information defined in the scheme, and to check compliance by verifying the information provided in the certificates stored in the site managed by ENISA.

SCHEME STAKEHOLDERS?

STAKEHOLDERS : INVOLVED IN THE PRODUCTION OF CERTIFICATES

- Development
- Operations
- Compliance

Cloud Service Provider

- Evaluation
- Review and Certification

CAB

- As a CAB
- Compliance monitoring

NCCA

- CAB Accreditation

NAB

- Publicity

ENISA

STAKEHOLDERS : INVOLVED IN THE PRODUCTION OF CERTIFICATES

- Development
- Operations
- Compliance

Cloud Service Provider

- Evaluation
- Review and Certification

CAB

- As a CAB
- Compliance monitoring

NCCA

- CAB Accreditation

NAB

NCCA CAB

For **level 'high'**, the NCCA is involved and may perform the tasks of a CAB. This would include at least the Review and Certification role, and it may also include the Evaluation role.

- Publicity

ENISA

NCCA: Compliance monitoring

NCCAs have a Compliance Monitoring role, to ensure that certified cloud services remain Compliant to the requirements of the scheme

A4CEF Co-financed by the Connecting Europe Facility of the European Union

STAKEHOLDERS : CONSUMING CERTIFICATES

- Procurement
- Customer Development
- Customer Operations
- Customer Compliance

Cloud Service Customer

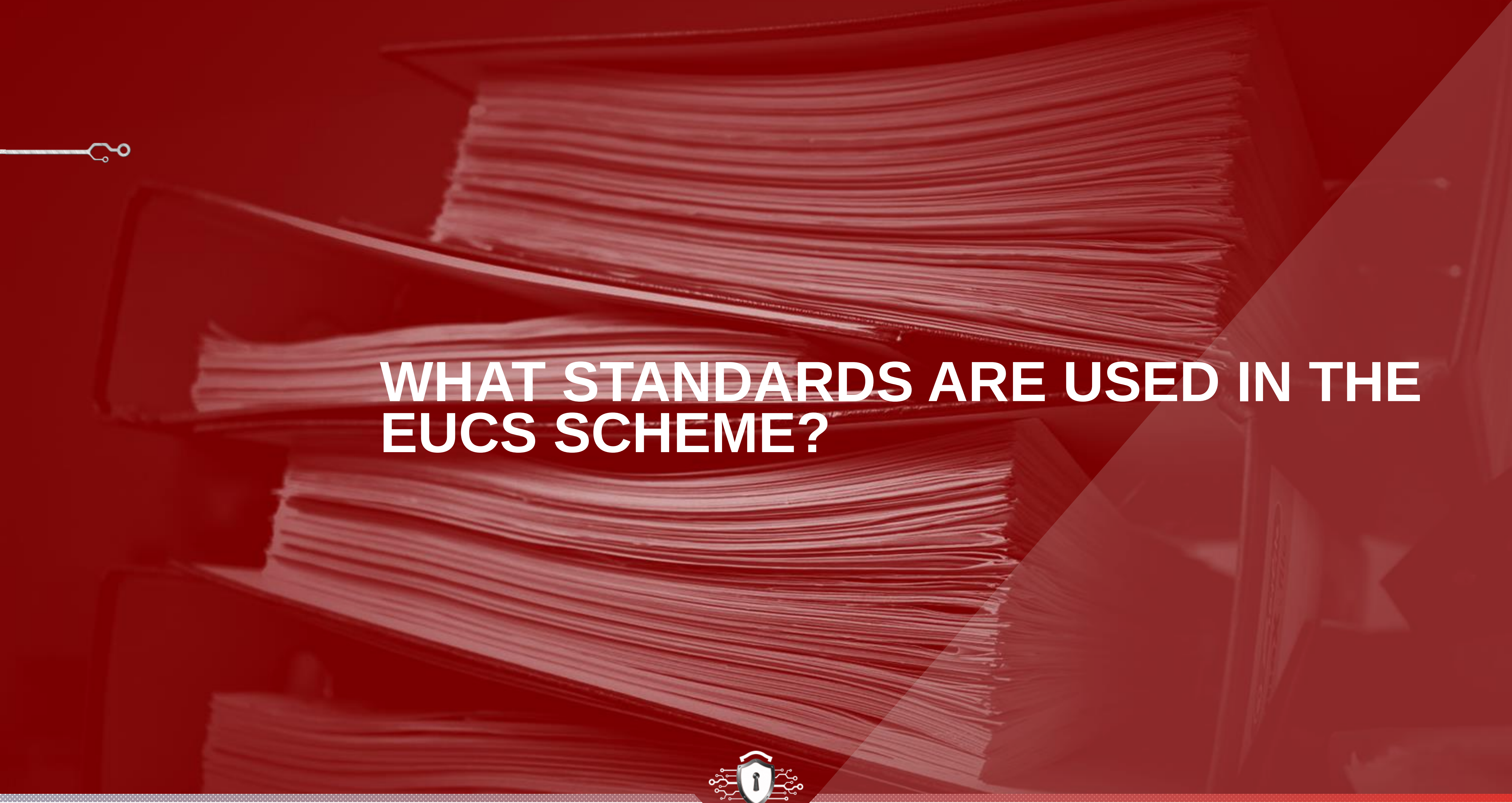
- User

Cloud Service User

- Regulation
- Enforcement

Regulatory Authority

A4CEF
Co-financed by the Connecting Europe Facility of the European Union



WHAT STANDARDS ARE USED IN THE EUCS SCHEME?

USE OF STANDARDS : GLOBAL STANDARDS AND TECHNICAL SPECIFICATIONS

ISO/IEC 17788 and ISO/IEC 17000, and to a lesser extent ISO/IEC 9000 and ISO/IEC 27000

➔ are being used as references for the **terminology** used through the scheme, with input from all the schemes listed below when required.

ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017, and on documents previously issued by Member States to define the security controls in their respective National Schemes [C5, SecNumCloud].

➔ are being used for the **security controls** of the scheme, together with the associated **security requirements**

Defined in Annex A of the scheme

ISO/IEC 15408-3 standard

➔ the definition of **the assurance levels** reuses some concepts

ISO/IEC 17065 international standard

➔ are used as a base for the **conformity assessment methodology** defined in the scheme

USE OF STANDARDS : SECURITY ASSESSMENT STANDARDS

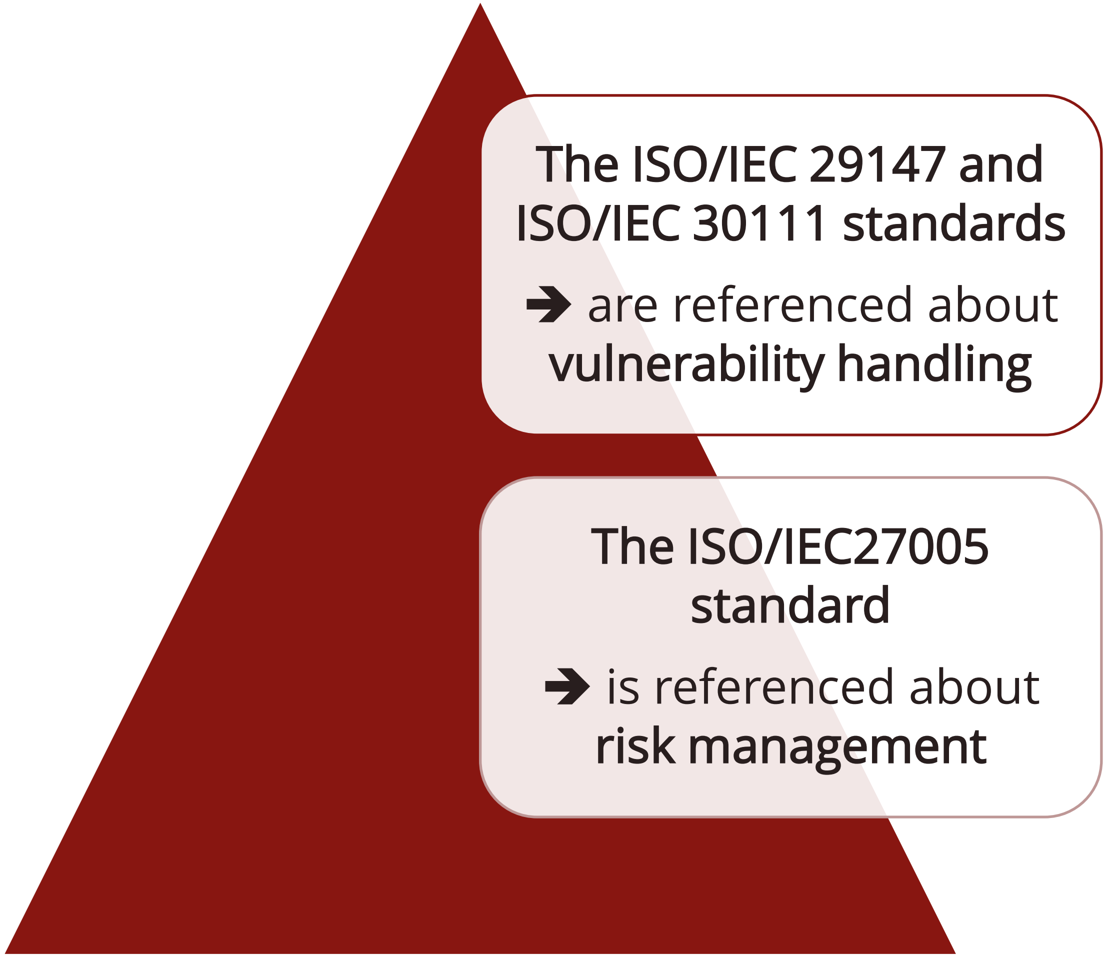
International standards **ISO/IEC 17021** and **ISO/IEC 27006.**

International auditing standards **ISAE3402** and **ISAE3000.**

One method defined in an Annex to the present scheme **(see Annex D: Assessment for level Basic).**

A4CEF Co-financed by the Connecting Europe Facility of the European Union

USE OF STANDARDS : SECURITY CONTROLS AND OTHER ANNEXES



The ISO/IEC 29147 and ISO/IEC 30111 standards

➔ are referenced about **vulnerability handling**

The ISO/IEC27005 standard

➔ is referenced about **risk management**

A4CEF

Co-financed by the Connecting Europe Facility of the European Union

SUBJECT MATTER AND SCOPE ?
TARGET OF EVALUATION?

Co-financed by the Connecting Europe
Facility of the European Union

SUBJECT MATTER AND SCOPE

The European cybersecurity certification scheme for cloud services, referred to as the EUCS scheme, shall allow for the cybersecurity certification of cloud services according to the criteria and methods defined in the scheme (Chapter 8: Evaluation Methods and Criteria).

The EUCS scheme may cover any type of ICT service, provided that:

- The ICT service implements one or more capabilities offered via cloud computing invoked using a defined interface [ISO17788].
- The ICT service aims at reaching the assurance level corresponding to one of the three levels 'basic', 'substantial' and 'high' of the EUCSA as defined in the EUCS scheme

A4CEF Co-financed by the Connecting Europe Facility of the European Union

SUBJECT MATTER AND SCOPE

ICT services matching criteria are referred to as “cloud services” in the scheme. The EUCS scheme may apply to all cloud services, following some principles that are listed below. The EUCS scheme:

distinguishes between different categories of cloud services by relying on the cloud capabilities types (infrastructure, platform, application)

aims at establishing the conformity of cloud services to a set of requirements corresponding to one of the assurance levels defined in the EUCS scheme

aims at making geographical and legal information about the cloud services available and understandable to all users of the scheme to allow to use them as needed.

acknowledges that the responsibility for the security of a cloud service is split between the Cloud Service Provider (CSP) and the Cloud Service Customer (CSC)

aims at providing sufficient information for making informed security decisions on cloud services to prospects and customers with adequate cybersecurity knowledge

SUBJECT MATTER AND SCOPE

In the evaluation of a cloud service, the EUCS scheme shall support and encourage the reuse of conclusions and evidence from already audited or certified ICT products, ICT processes, and ICT services, in particular those cloud services that have been **certified with the EUCS scheme.**

The scheme includes an assessment of the dependencies, in which the assurance information available from subservice organizations is considered and compared to the requirements of the scheme, in particular regarding the required level of assurance (Annex B: Meta-approach for the assessment of cloud services)

When a certified composite cloud service relies on a base cloud service certified with the EUCS scheme, the EUCS scheme shall aim at verifying that the recommendations defined in the base cloud service are adequately applied by the composite cloud service, and included into the recommendations defined for that composite cloud service (Section 24.4 Composition).

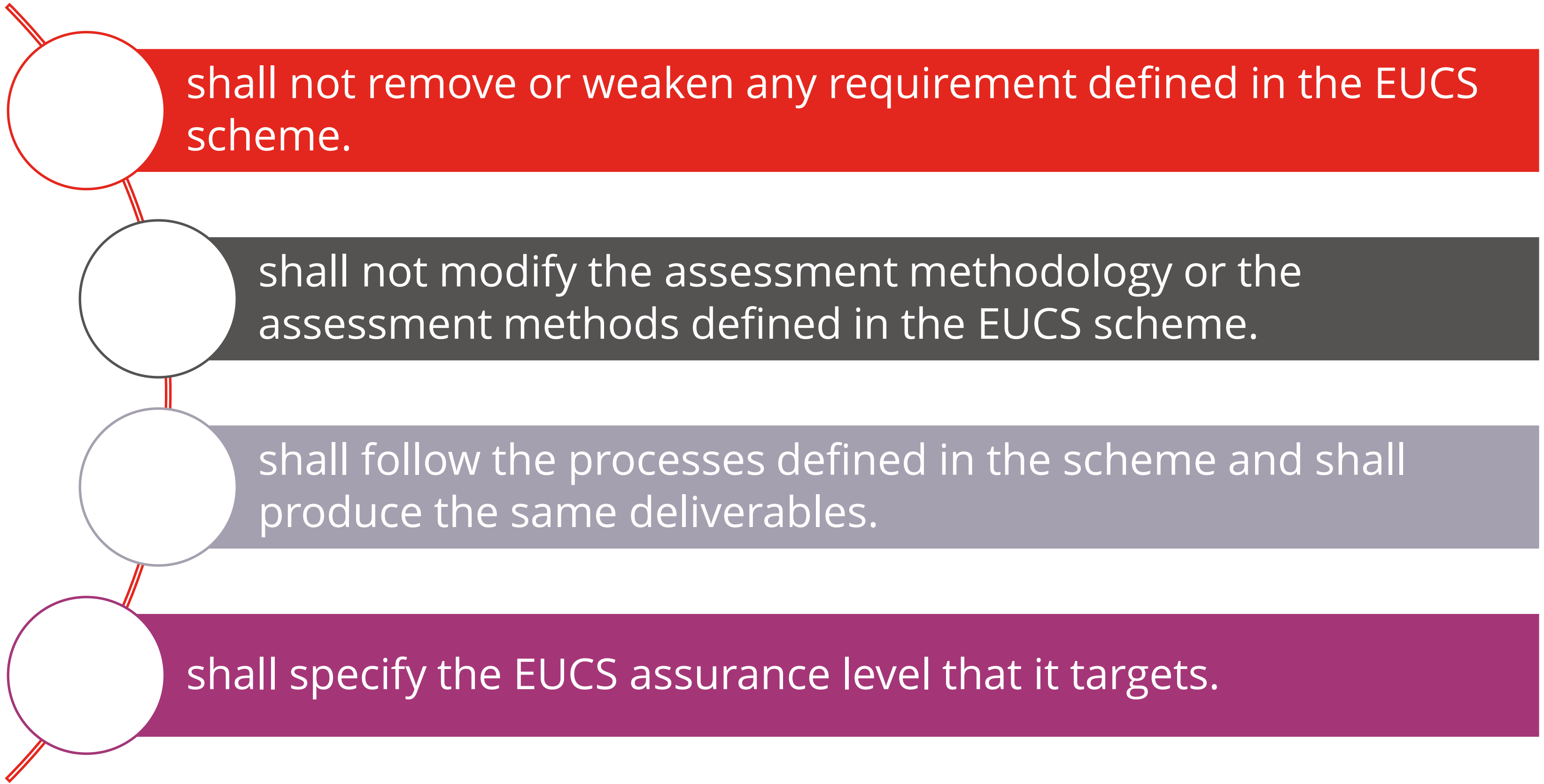
SUBJECT MATTER AND SCOPE: SECURITY PROFILES

Cloud services are likely to be used in ICT products, ICT services and ICT processes that will themselves be subject to certification in the context of another conformity assessment scheme, and in particular of another European cybersecurity certification scheme. Some of these conformity assessment schemes may have specific requirements, for instance related to an industry vertical.

In order to simplify the use of certificates issued in the EUCS scheme in other schemes, it is therefore important to support the definition of such specific vertical requirements, and to allow cloud services to take these requirements into consideration in their certification.

SUBJECT MATTER AND SCOPE: SECURITY PROFILES

Such specific requirements shall be defined in a Security Profile, following some principles. A security Profile:



- shall not remove or weaken any requirement defined in the EUCS scheme.
- shall not modify the assessment methodology or the assessment methods defined in the EUCS scheme.
- shall follow the processes defined in the scheme and shall produce the same deliverables.
- shall specify the EUCS assurance level that it targets.

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

SUBJECT MATTER AND SCOPE: SECURITY PROFILES

Such specific requirements shall be defined in a Security Profile, following some principles. A security Profile:

- may define new security controls or may add new requirements to an existing security control, as long as these requirements do not weaken existing EUCS requirements.
- may mandate a higher frequency of periodic assessments.
- may define a dedicated section in the document templates defined in the EUCS scheme.

WHAT SHOULD I KNOW ABOUT THE CERTIFICATION?

Co-financed by the Connecting Europe Facility of the European Union

OVERVIEW OF CERTIFICATION PROCEDURE

When a CSP wishes to get a cloud service certified in the EUCS scheme, or to maintain the certification of an already certified cloud service

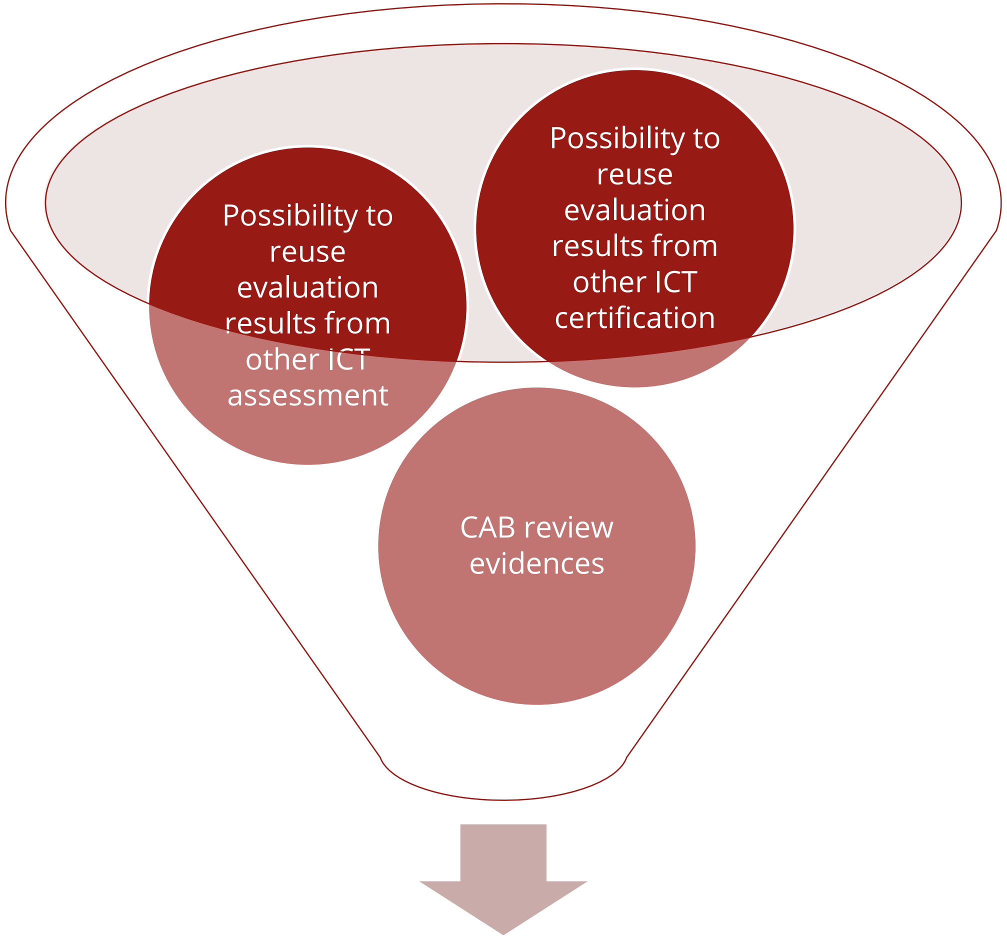
- the CSP shall submit an application document, following the template defined in Annex F: (Scheme Document Content requirements),
- During the evaluation, the CSP shall submit all the information needed to demonstrate that the implementation of their cloud service meets the security requirements defined in Annex A: (Security Objectives and requirements for Cloud Services) for the targeted assurance level, including but not limited to:

Policies & procedures

If required, records to be used as evidence

If subservice organisations, records and document of compliance

OVERVIEW OF CERTIFICATION PROCEDURE: REUSE


Possibility to reuse evaluation results from other ICT assessment
Possibility to reuse evaluation results from other ICT certification
CAB review evidences

New certification

Conditions:

- Evidence conforms to the requirements
- evidence have been evaluated following a methodology recognized by the scheme
- Authenticity of the evidence can be confirmed

A4CEF Co-financed by the Connecting Europe Facility of the European Union

KEY BENEFITS OF THE EUCS SCHEME?

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

KEY BENEFITS OF THE CERTIFICATION SCHEME

Scheme **harmonized** at the **European level**

Strong quality guarantees through the use

- of **third-party assessment** by accredited bodies,
- **supervision by national authorities**,
- and for the **High level**, **authorization by the national authorities** and **peer assessment between conformity assessment bodies**;

Flexibility offered by **three different assurance levels**, with the possibility for a certified cloud service to upgrade to a higher level in future evaluation cycles

Strong transparency guarantees, with security information made publicly available through a centralized web site

A4CEF Co-financed by the Connecting Europe Facility of the European Union

KEY BENEFITS OF THE CERTIFICATION SCHEME

Assurance maintained over time

with regular reassessments, operating effectiveness guarantees at the levels Substantial and High;

A maintenance framework for the EUCS scheme itself

endorsed by European institutions and Member states, providing strong guarantees on continued operation of the scheme

Integration in the European cybersecurity certification framework

which will facilitate the reuse of EUCS-certified cloud services in vertical schemes.

A4CEF Co-financed by the Connecting Europe Facility of the European Union

QUIZ

- Today the Cloud Computing Industry is not fragmented. True or False?

- Could you name 2 benefits of a single certification scheme globally?

- How the NCCA could be involved when it comes to certificates production?

- Could you name 2 principles of security profiles?

A4CEF Co-financed by the Connecting Europe Facility of the European Union

QUIZ

- Today the Cloud Computing Industry is not fragmented. True or False?

False. Ref: Currently, cloud computing products and services in France and Germany: Have to obtain two specific certifications to be accepted across the entirety of the EU: the secnumcloud and the compliance controls catalogue (C5).

- Could you name 2 benefits of a single certification scheme globally?

Cost Reduction, Shorter Certification Time, Improved Client Trust, Increased Market Competition, Lower R&D Expenses.

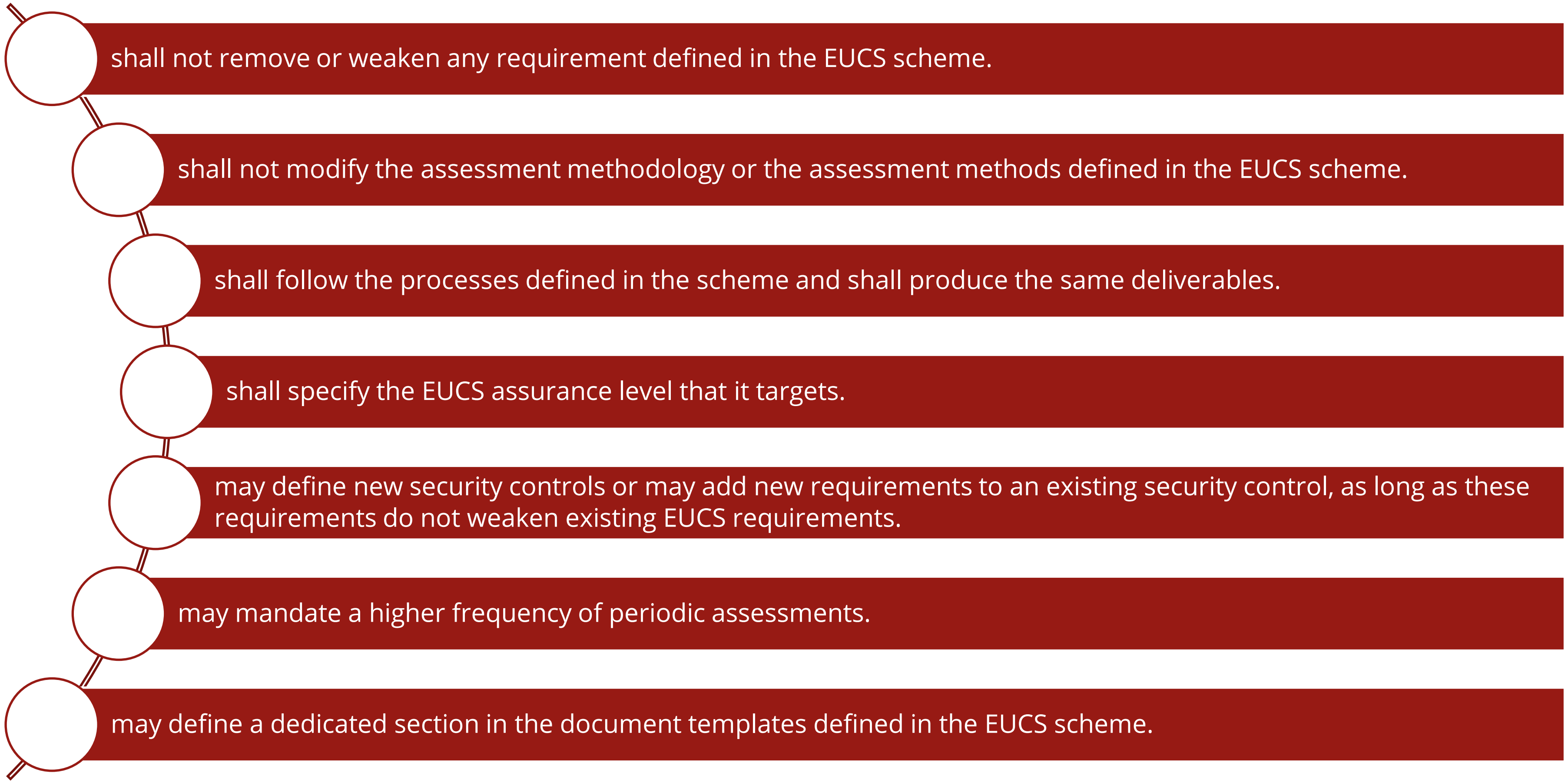
- How the NCCA could be involved when it comes to certificates production?

NCCA: As a CAB - For level ‘high’, the NCCA is involved and may perform the tasks of a CAB. This would include at least the Review and Certification role, and it may also include the Evaluation role. **NCCA: Compliance monitoring -** NCCAs have a Compliance Monitoring role, to ensure that certified cloud services remain compliant to the requirements of the scheme.

- Could you name 2 principles of security profiles?

QUIZ

- Could you name 2 principles of security profiles?



- shall not remove or weaken any requirement defined in the EUCS scheme.
- shall not modify the assessment methodology or the assessment methods defined in the EUCS scheme.
- shall follow the processes defined in the scheme and shall produce the same deliverables.
- shall specify the EUCS assurance level that it targets.
- may define new security controls or may add new requirements to an existing security control, as long as these requirements do not weaken existing EUCS requirements.
- may mandate a higher frequency of periodic assessments.
- may define a dedicated section in the document templates defined in the EUCS scheme.

A4CEF

Co-financed by the Connecting Europe
Facility of the European Union

03

OVERVIEW ON THE CERTIFICATION PROCESS FROM A-Z

- Security Objectives and Requirements for Cloud Services
- EUCS Security Assurance levels
- Conformity Assessment
- Self Assessment
- Specific requirements applicable to CAB
- Mutual Recognition
- Certificate Validity and Management
- Peer Assessment Scope and Overview

SECURITY OBJECTIVES AND REQUIREMENTS FOR CLOUD SERVICES

SECURITY OBJECTIVES AND REQUIREMENTS (ANNEX A)

Principles

- Defines the technical objectives and requirements that CSPs need to fulfil in order to get a cloud service certified.
- The requirements defined in Annex A shall be complemented by guidance, to be published by ENISA with the support of the ECCG
- The requirements are labelled Basic, Substantial or High
- The requirements related to continuous monitoring typically mention “automated monitoring” or “automatically monitor” in their text.

A4CEF Co-financed by the Connecting Europe Facility of the European Union

SECURITY REQUIREMENTS

Organization

The requirements are grouped in 20 categories, and each category is divided in a number of themes. Each theme is structured as follows:

An objective that the requirements aim at achieving.

Requirements to be met by the controls implemented in support of the certified cloud services, with each requirement associated to an assurance level.

In some cases, an indication of guidance to be made available

EUCS ASSURANCE LEVELS

ASSURANCE LEVELS – PARAMETERS

The Assurance Levels are currently differentiated by:

- Intention
- Suitability
- Assumed Attacker profile
- Scope
- Depth
- Rigor

A4CEF Co-financed by the Connecting Europe Facility of the European Union

ASSURANCE LEVELS - PARAMETERS

Intention

- The intention provides a general description of the Assurance Level, most likely matching quite closely the definition from the EU CSA.

Suitability

- Suitability is about potential restrictions of the types and categories that may be covered.

Attacker profile

- The attacker profile cannot be very specific, because of the great variety of attackers, and it always defines a wide category of attackers.

Scope of the Evaluation

- The scope of the evaluation should comprise the service provided by the CSP and clearly identify all underlying and supporting services and processes.

Depth

- The general principle is to follow an incremental approach, *i.e.*, that all requirements of a lower level are similarly included in the depth of the higher level.

Rigour

- This is about requiring more structure in the service (for instance, a security model based on a specific formalism/method) or adding more structure to the assessment (for instance, requiring a specific method to collect evidence or provide results).

A4CEF

Co-financed by the Connecting Europe Facility of the European Union

REMINDER – CSA ASSURANCE LEVEL

EUCSA’s Article 52

Basic

Assurance level ‘basic’ provides assurance that the ICT products, services and processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level **intended to minimise the known basic risks of cyber incidents and cyberattacks.**

Substantial

Assurance level ‘substantial’ provides assurance that the ICT products, services and processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level **intended to minimise cybersecurity risks, cyber incidents and cyberattacks carried out by actors with limited skills and resources.**

High

A European cybersecurity certificate referring to assurance level ‘high’ provides assurance that the ICT products, services and processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level **intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources.**

A4CEF Co-financed by the Connecting Europe Facility of the European Union

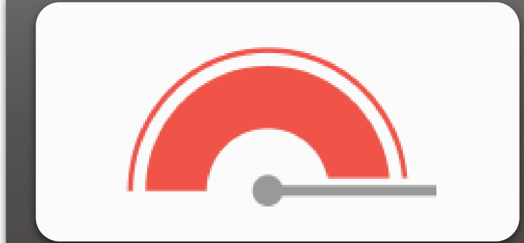
ASSURANCE LEVEL – UNDERSTANDING THE LEVELS

CS-Basic

- Demonstrates an intention from the CSP to implement security controls
- Intended to minimize the known basic risks of incidents and cyberattacks
- Document review is required
- Entry level with limited guarantees, suitable for cloud services that are designed to meet typical security requirements on services for non-critical data and systems.

CS-Substantial

- Demonstrates that the CSP has correctly implemented security controls
- Intended to minimise known cybersecurity risks & cyberattacks carried out by actors with limited skills and resources
- Functional testing and limited penetration testing using known attacks is required
- Core level with real guarantees, suitable for cloud services that are designed to meet typical security requirements on services for business-critical data and systems



CS-High

- Demonstrates the effectiveness of the CSP’s controls against attacks
- Intended to resist complex attacks using state-of-the-art techniques
- Penetration testing is required
- Level with strong guarantees, be suitable for cloud services that are designed to meet specific (exceeding level ‘substantial’) security requirements for mission-critical data and systems.

ASSURANCE LEVELS – PARAMETERS (EXAMPLE)

Assumed Attacker profile

CS-Basic

Single person

- With limited skills
- Repeating known attacks
- With limited resources
- No abilities like social engineering

CS-Substantial

Small team

- With good skills to repeat even complex attacks
- With limited resources
- With access to a wide range of techniques, including social engineering, but no ability to discover new vulnerabilities

CS-High

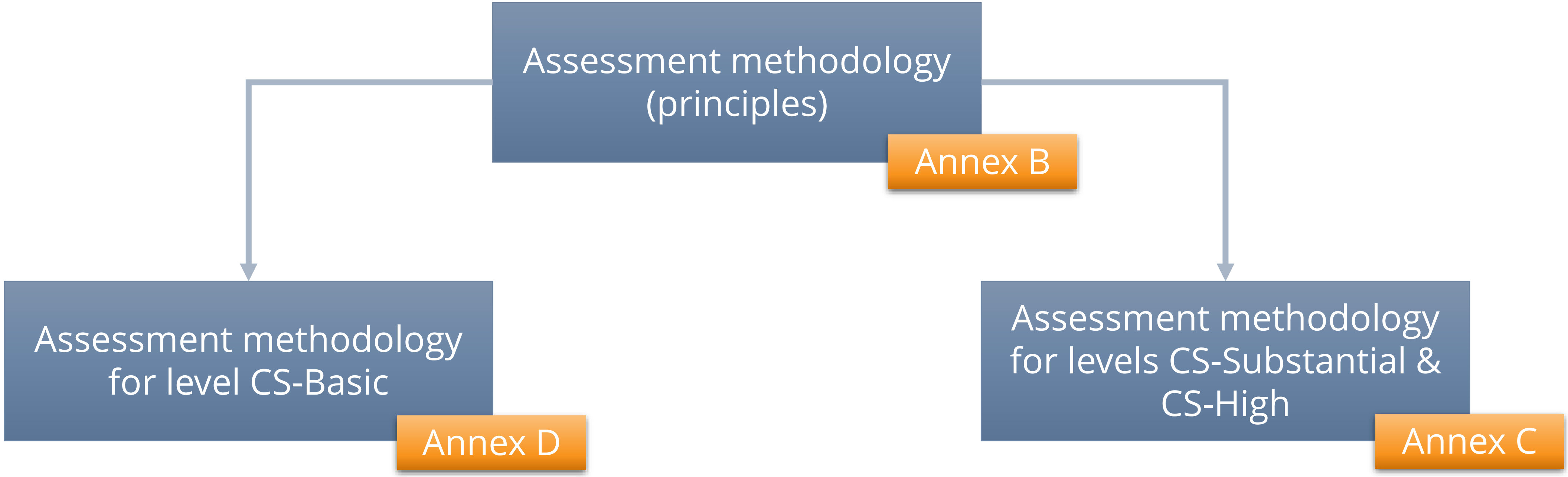
Team of experts

- With diverse high-level skills
- With the ability to discover and perform complex attacks
- With significant resources
- With the ability to find or buy access to previously unknown vulnerabilities

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

HOW CONFORMITY ASSESSMENT IS DONE?

ASSESSMENT METHODOLOGY



Assessment methodology (principles)

Annex B

Assessment methodology for level CS-Basic

Annex D

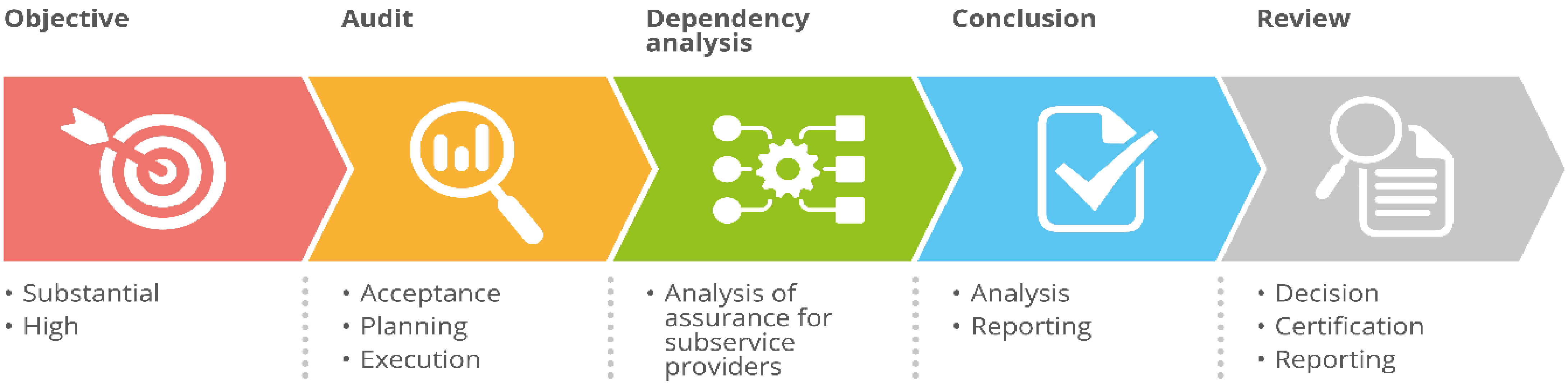
Assessment methodology for levels CS-Substantial & CS-High

Annex C

A4CEF Co-financed by the Connecting Europe Facility of the European Union

ASSESSMENT METHODOLOGY: META-APPROACH

The structure of this meta-approach starts with defining a clear objective, followed by the development and execution of an audit plan, and ending with the analysis of the gathered evidence and the delivery of an assurance report.



Objective

- Substantial
- High

Audit

- Acceptance
- Planning
- Execution

Dependency analysis

- Analysis of assurance for subservice providers

Conclusion

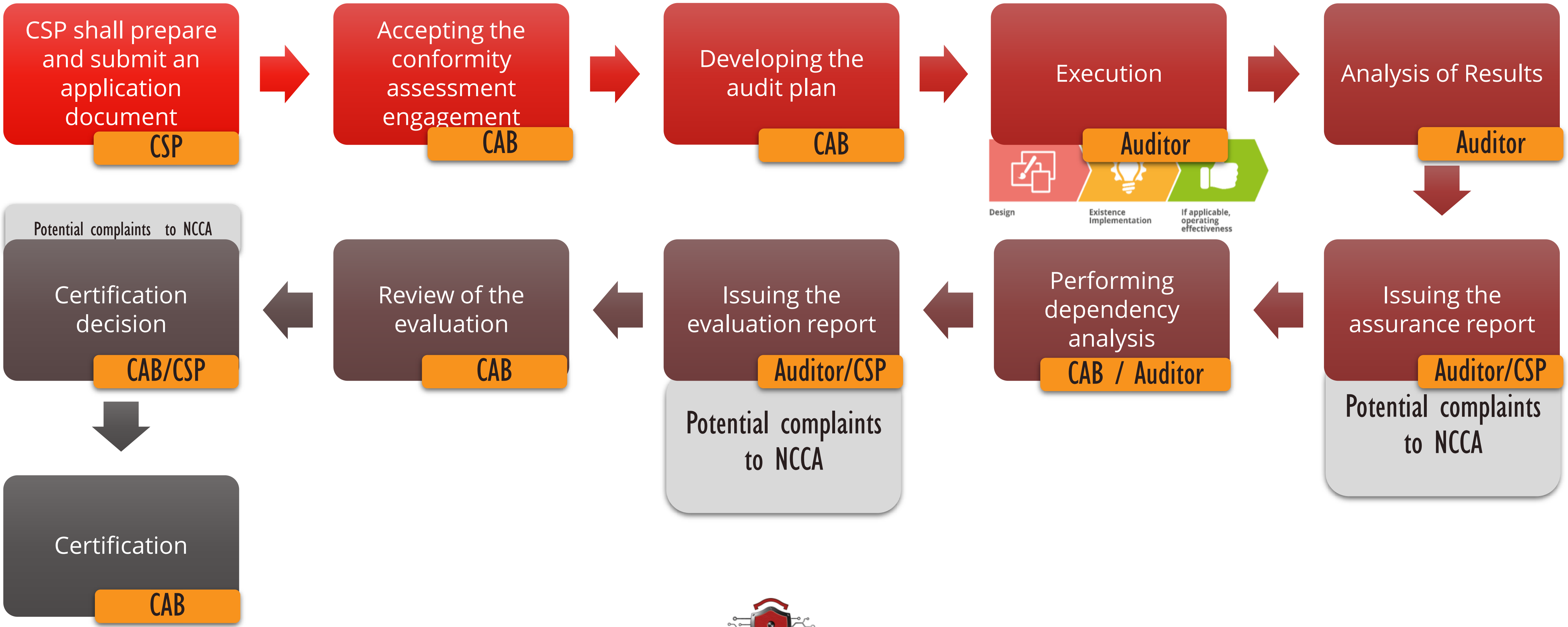
- Analysis
- Reporting

Review

- Decision
- Certification
- Reporting

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

ASSESSMENT METHODOLOGY: META-APPROACH



CSP shall prepare and submit an application document – CSP

Accepting the conformity assessment engagement – CAB

Developing the audit plan – CAB

Execution – Auditor

Design

Existence Implementation

If applicable, operating effectiveness

Analysis of Results – Auditor

Issuing the assurance report – Auditor/CSP

Potential complaints to NCCA

Performing dependency analysis – CAB / Auditor

Issuing the evaluation report – Auditor/CSP

Potential complaints to NCCA

Review of the evaluation – CAB

Potential complaints to NCCA

Certification decision – CAB/CSP

Certification – CAB

A4CEF
Co-financed by the Connecting Europe Facility of the European Union

QUIZ

- How many security requirements category exist in the EUCS?
- Each category of requirement is associated to an assurance level. True or False?
- Could you name 2 parameters of the EUCS assurance levels ?
- Document review is required for Basic. True or False?
- Penetration testing is required for Substantial. True or False?

A4CEF
Co-financed by the Connecting Europe
Facility of the European Union

QUIZ

- How many security requirements category exist in the EUCS?

20

- Each category of requirement is associated to an assurance level. True or False?

False. Each requirement is associated to an assurance level.

- Could you name 2 parameters of the EUCS assurance levels ?

Intention, Suitability, Assumed Attacker Profile, Scope, Depth, Rigor

- Document review is required for Basic. True or False?

True.

- Penetration testing is required for Substantial. True or False?

False. Functional testing is required for Substantial and penetration testing is required for High.

A4CEF Co-financed by the Connecting Europe Facility of the European Union

QUESTIONS ?