



The impact of EU Cyber-Security Act on Cloud

***Damir Savanovic**, Senior Innovation
Analyst
Cloud Security Alliance*

99,000

+
INDIVIDUAL
MEMBERS

55+
CHAPTERS

400+
CORPORATE
MEMBERS

28+
ACTIVE
WORKING
GROUPS



Strategic partnerships with governments, research institutions, professional associations and industry



CSA research is FREE!



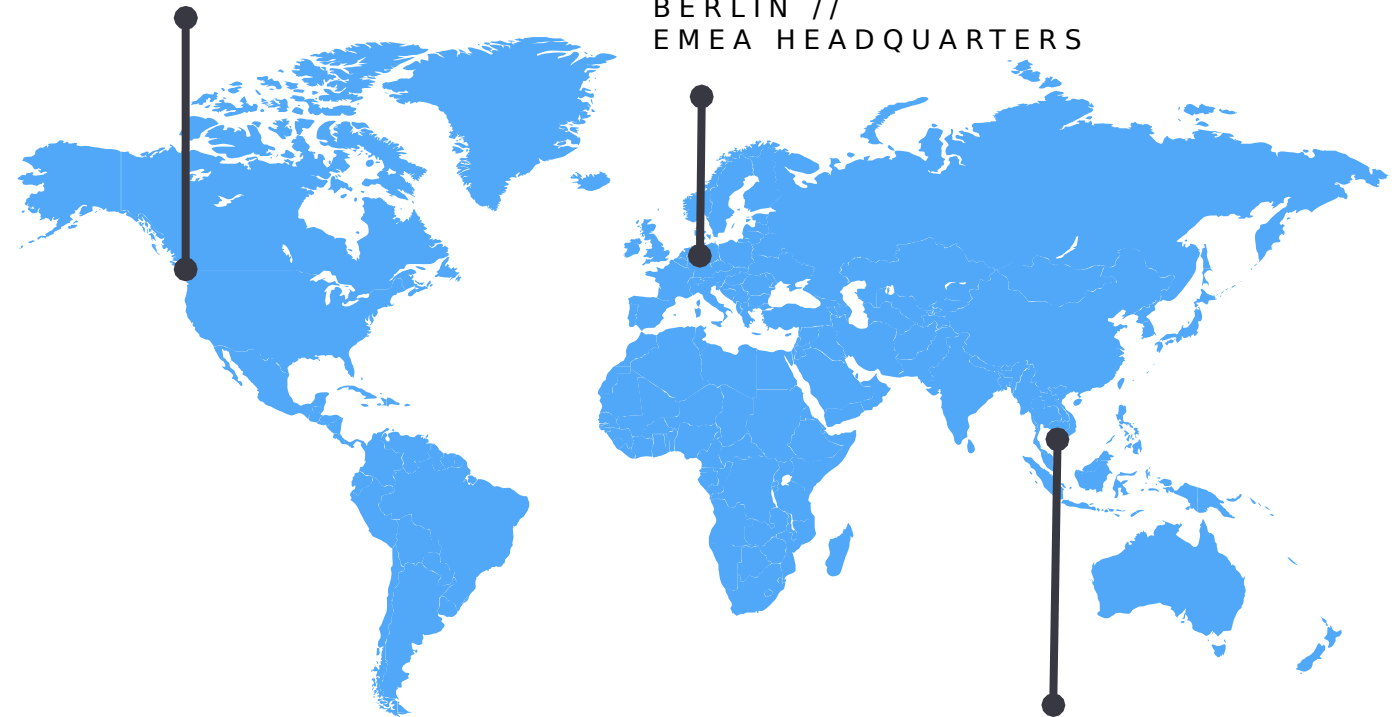
OUR COMMUNITY

2009

CSA FOUNDED

SEATTLE/BELLINGHAM, WA //
AMERICAS HEADQUARTERS

BERLIN //
EMEA HEADQUARTERS



SINGAPORE //
ASIA PACIFIC
HEADQUARTERS

Background
The EU Cybersecurity Act (EUCA) sets the ground to establish an EU framework for cybersecurity certification of ICT product and services

One of the objectives of the EUCA is to **increase the level of trust** in ICT services and products by introducing an **EU-wide security certification** providing for **common cybersecurity requirements** and evaluation criteria across national markets and sectors.

ENISA will play a key role. It has been tasked with developing and maintaining a cybersecurity certification framework, **building on existing best practices**, with a view to **increasing the transparency** of the **cybersecurity assurance** of ICT products, ICT services and ICT

Proliferation of Schemes



Fig1. Compliance Templates Provided By Microsoft

Lack of Clarity



Uneven Landscape



CSA's activities in Cloud Assurance and Certification

	AUDIT FREQUENCY	Security	Privacy
TYPE OF AUDIT	●●●○	STAR Level 3 Continuous Auditing	_____
	●●●○	STAR Level 2 Continuous Level 2 + Continuous Self-Assessment	_____
		STAR Level 2 3rd Party Certification	GDPR CoC Certification
	●○○○	STAR Level 1 Continuous Continuous Self-Assessment	_____
		STAR Level 1 Self-Assessment	GDPR CoC Self-Assessment

↑
TRANSPARENCY & ASSURANCE



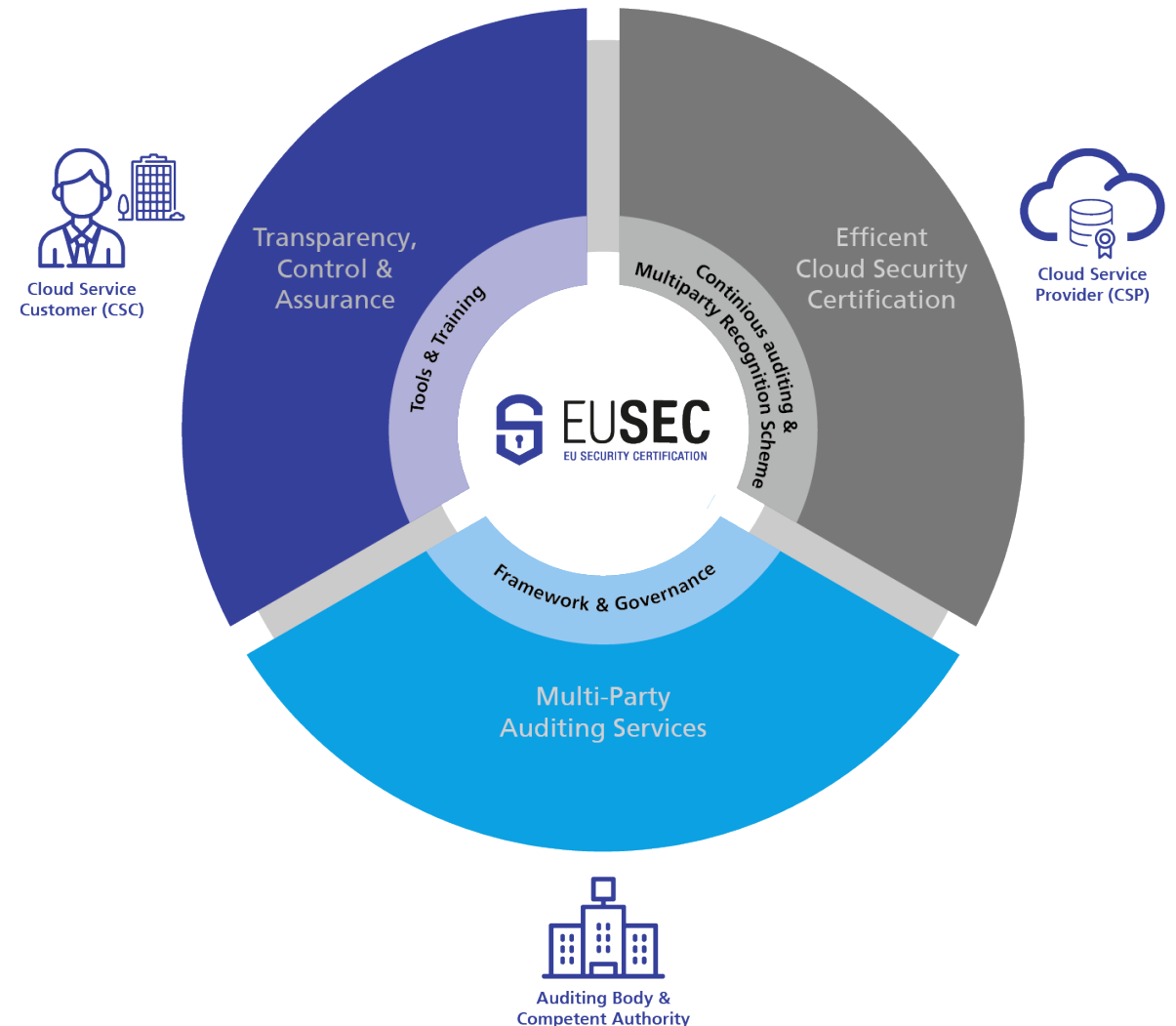
Trust in Cloud by Certification

The European Security Certification Framework (EU-SEC)



EU-SEC aims to create a framework under which existing certification and assurance approaches can co-exist. It has a goal to improve the business value, effectiveness and efficiency of existing **cloud security certification schemes**.

- **Multiparty Recognition Framework (MPRF)** for cloud security certifications,
- **Continuous Auditing-based Certification (CAC)**
- **Privacy Code of Conduct (PLA CoC)** , and
- **Governance Structure** for trustful and compliant use of cloud computing



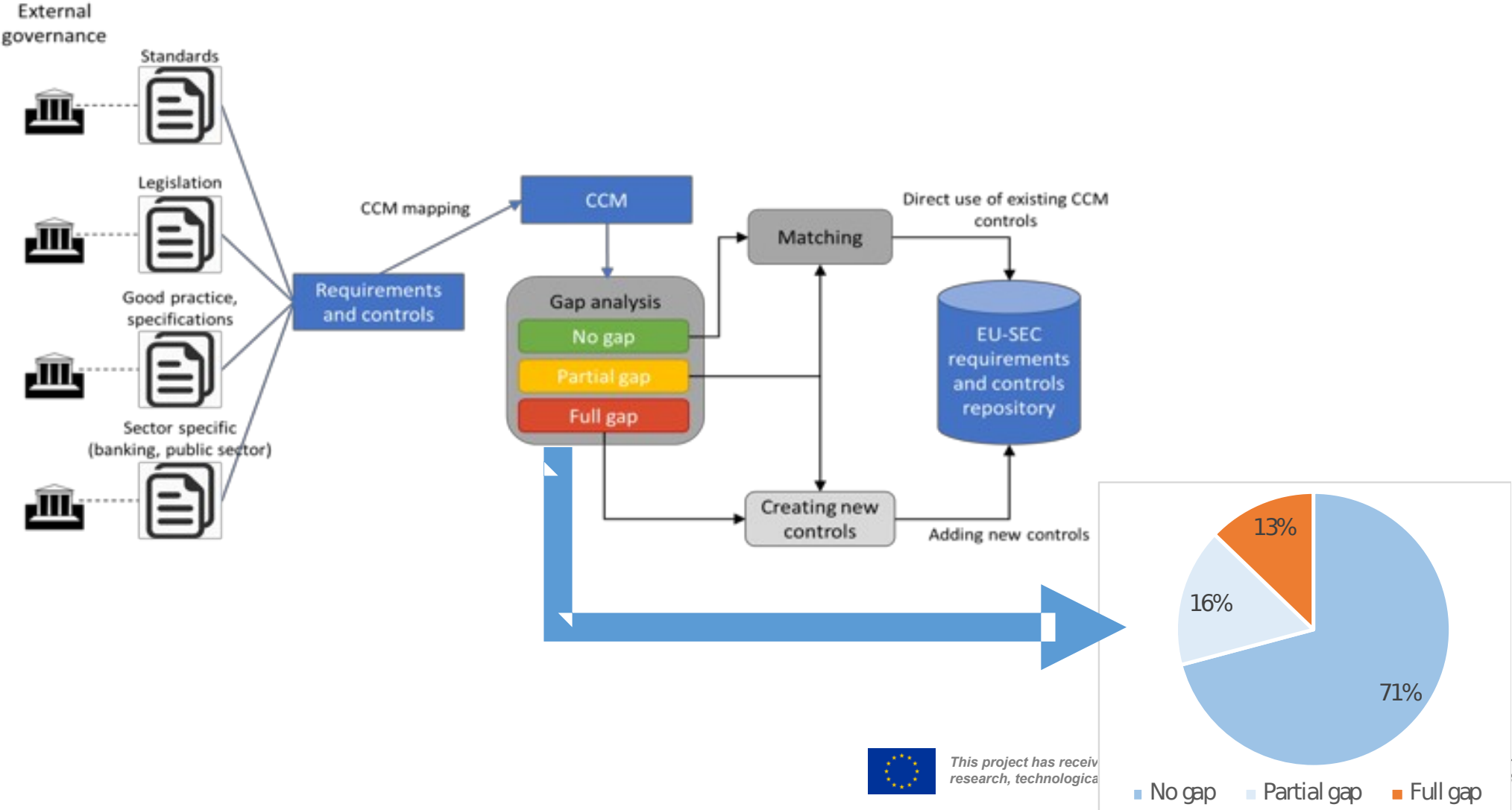
Multiparty Recognition Framework

Objectives

- Minimize the burden for a CSP
- Guide cloud stakeholders in understanding the certification landscape
- Streamline the cloud compliance

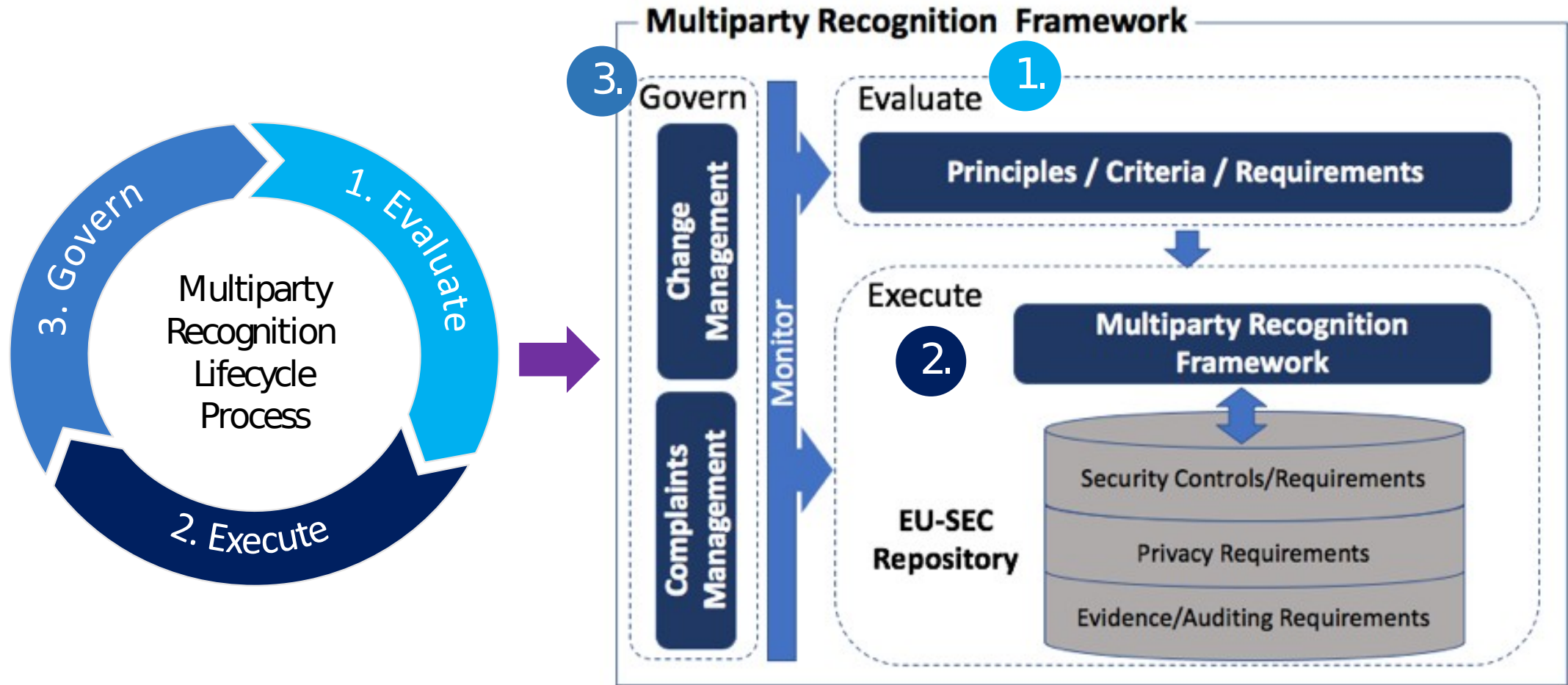
Multiparty Recognition Framework

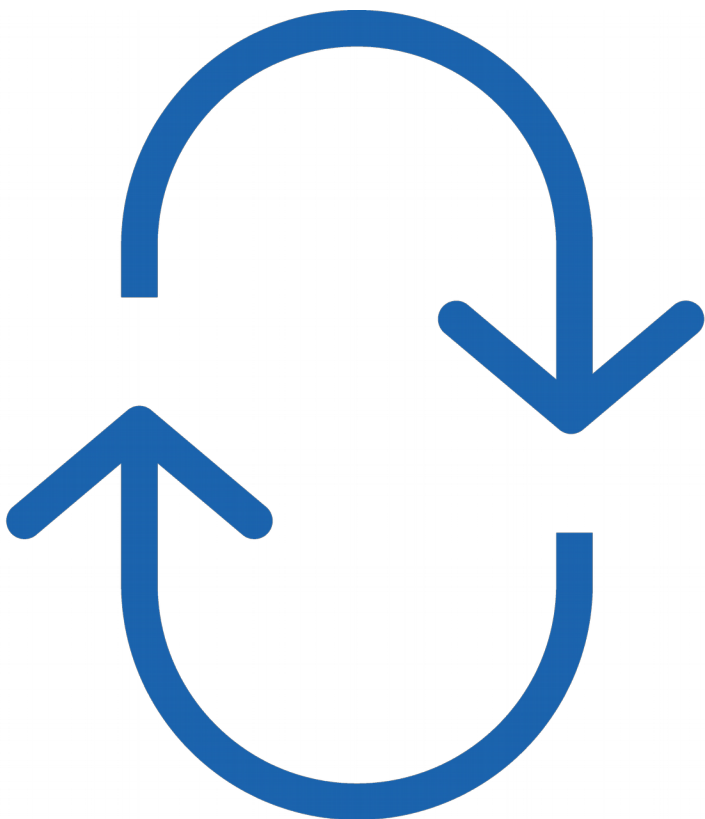
Requirements Collection and Analysis



Multiparty Recognition Framework

Lifecycle Overview





But...

For some cloud customers in heavily regulated industries such as banking, (bi-)annual certificates are not good enough.

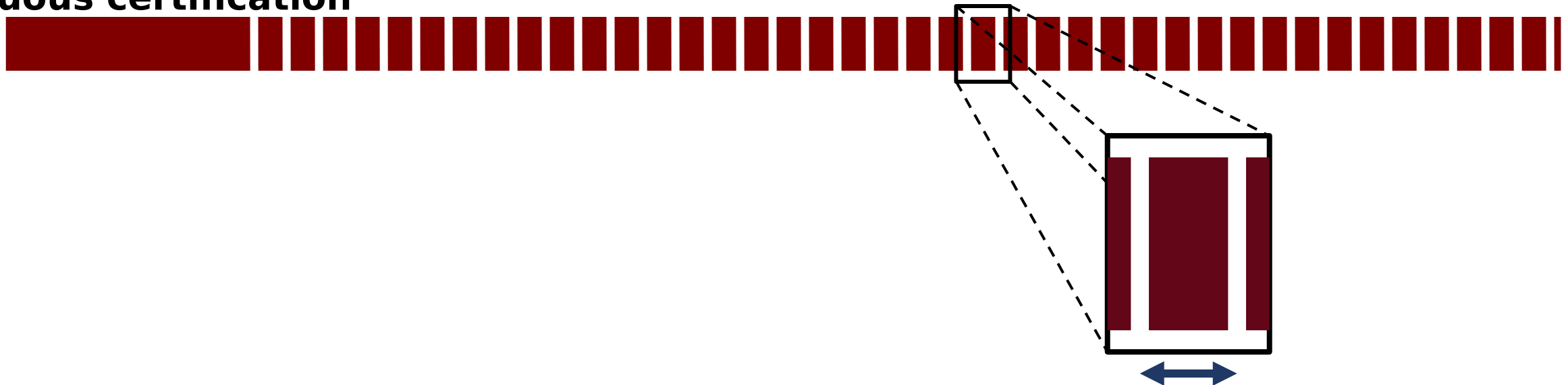
They need **CONTINUOUS** assurance.

EU-SEC introduces: continuous audit-based certification

Additional certification”



Continuous certification”



1 month, 1 day, 1 minute...

3 assurance levels



Continuous Auditing-based Certification

Methodology – phases

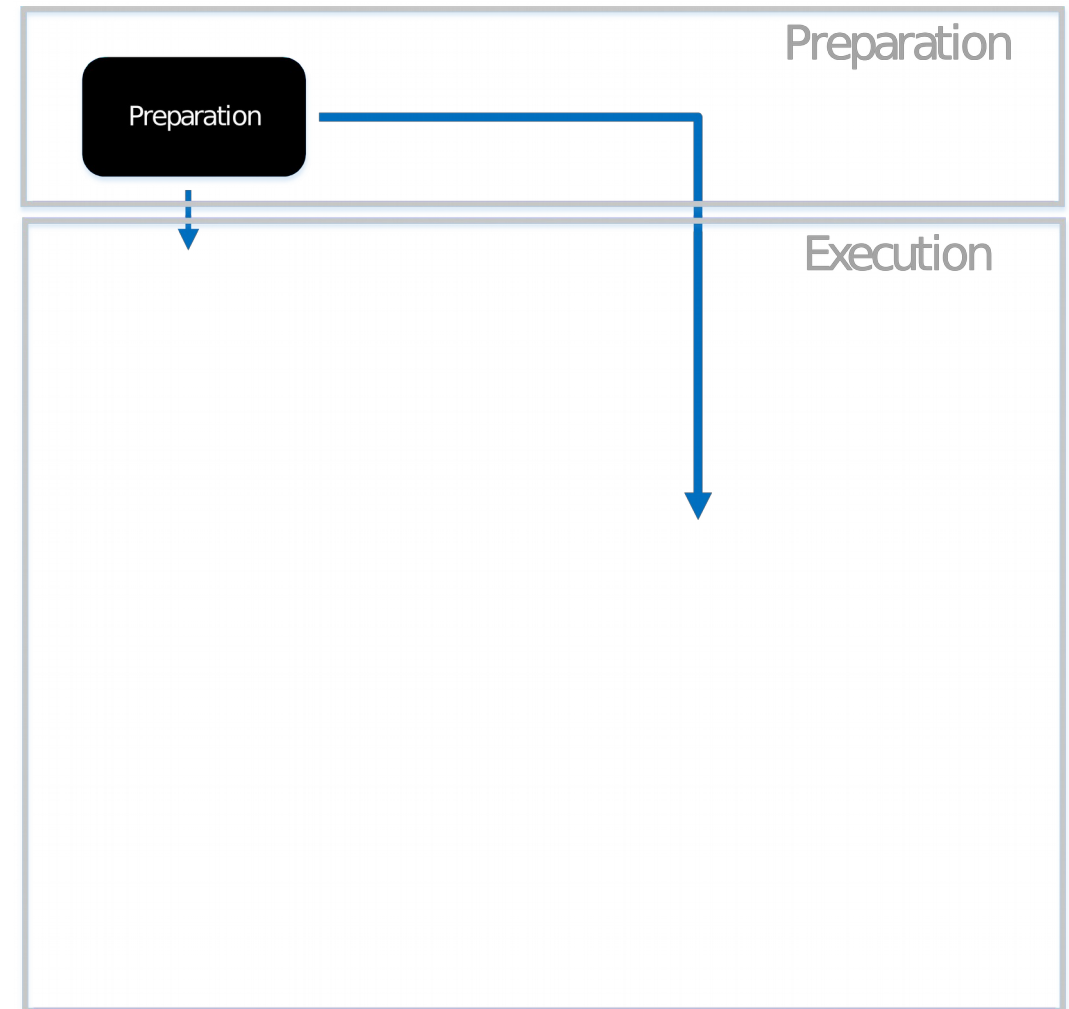
- 1. Preparation:** mainly devoted to the operationalisation of the controls
 - This initial setup is performed once
 - SLO's and SQO's are defined to describe controls
 - The output are: scope, SLO/SQO and frequency of assessment.

- 2. Collection:** devoted to the collection of evidence

- 3. Measurement:** the metrics are applied to the collected evidence.

- 4. Evaluation:** it checks if an objective is fulfilled.

- 5. Certification:** according to the result of the evaluation, a certification is issued.



Conclusions

- The current cloud certification landscape suffers of issues, such us: proliferation of schemes, lack of clarify, difficulties to compare existing schemes, lack of guidance of which scheme is suitable for what level of assurance.

The cloud certification framework under the Cybersecurity <Act should:

- Foster simplification and clarity
- Guide private and public companies to obtain the right level of assurance
- Increase user's trust in cloud services
- Facilitate free flow of data and support competitiveness

Likely the new cloud framework:

- Wont increase the compliance effort of mature CSP
- Will force less mature CPS to improve their security posture
- Increase the level of transparency and accountability across the cloud supply chain



???



Helpful Links

VIA WWW.CLOUDSECURITYALLIANCE.ORG

Cloud Controls Matrix

https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_downloads



Open Certification Framework

https://cloudsecurityalliance.org/working-groups/open-certification/#_overview



STAR™ CSA STAR

https://cloudsecurityalliance.org/star/#_overview



GDPR Center of Excellence

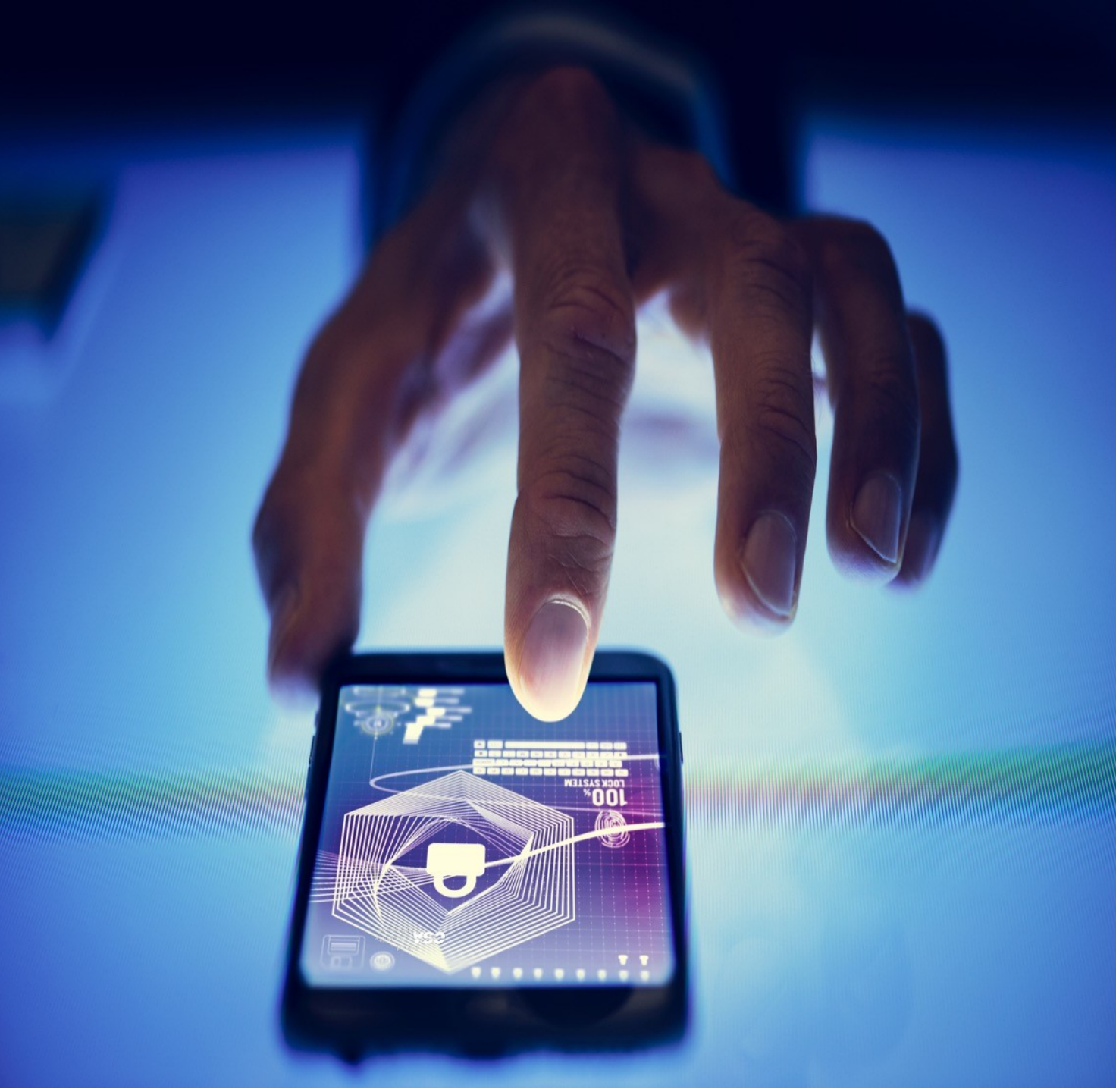
<https://gdpr.cloudsecurityalliance.org/resource-center/>



SEC Project

<https://www.sec-cert.eu>







Contact

 dsavanovic@cloudsecurityalliance.org

 Seattle > Bellingham > Berlin > Singapore

 Visit us on the web at
www.cloudsecurityalliance.org

 Follow and like us @cloudsa