

The background of the slide features a blue-toned image of two hands shaking, symbolizing agreement or partnership. This is overlaid on a faint world map. Scattered across the map are several circular icons, each containing a stylized human figure, connected by dotted lines, representing a global network or digital connectivity.

# The impact of EU Cyber-Security Act on Cloud

*Daniele Catteddu, CSA Chief Technology Officer*

90,000+

INDIVIDUAL  
MEMBERS

75+

CHAPTERS

300+

CORPORATE  
MEMBERS

30+

ACTIVE WORKING  
GROUPS

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

Active role in the standardization  
community: Liaison with ISO SC 27  
and SC38

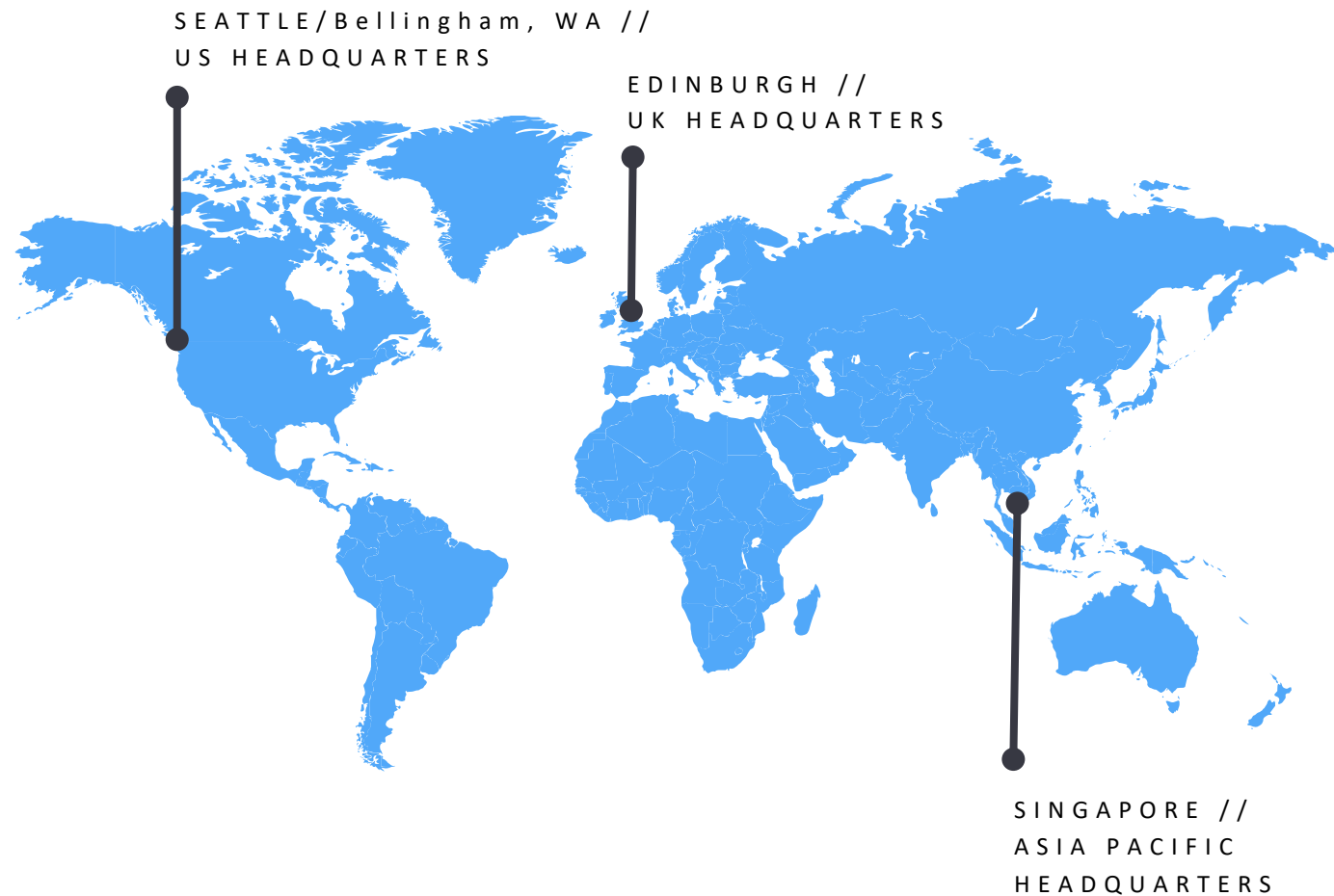
CSA research is FREE!

2009

CSA FOUNDED



OUR Community



# Background

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

The objective 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

# CONTEXT

# Proliferation of Schemes



Fig1. Compliance Templates Provided By Microsoft

# Lack of Clarity



# Uneven Landscape



# CSA's activities in Cloud Assurance and Certification

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

↑ TRANSPARENCY & ASSURANCE

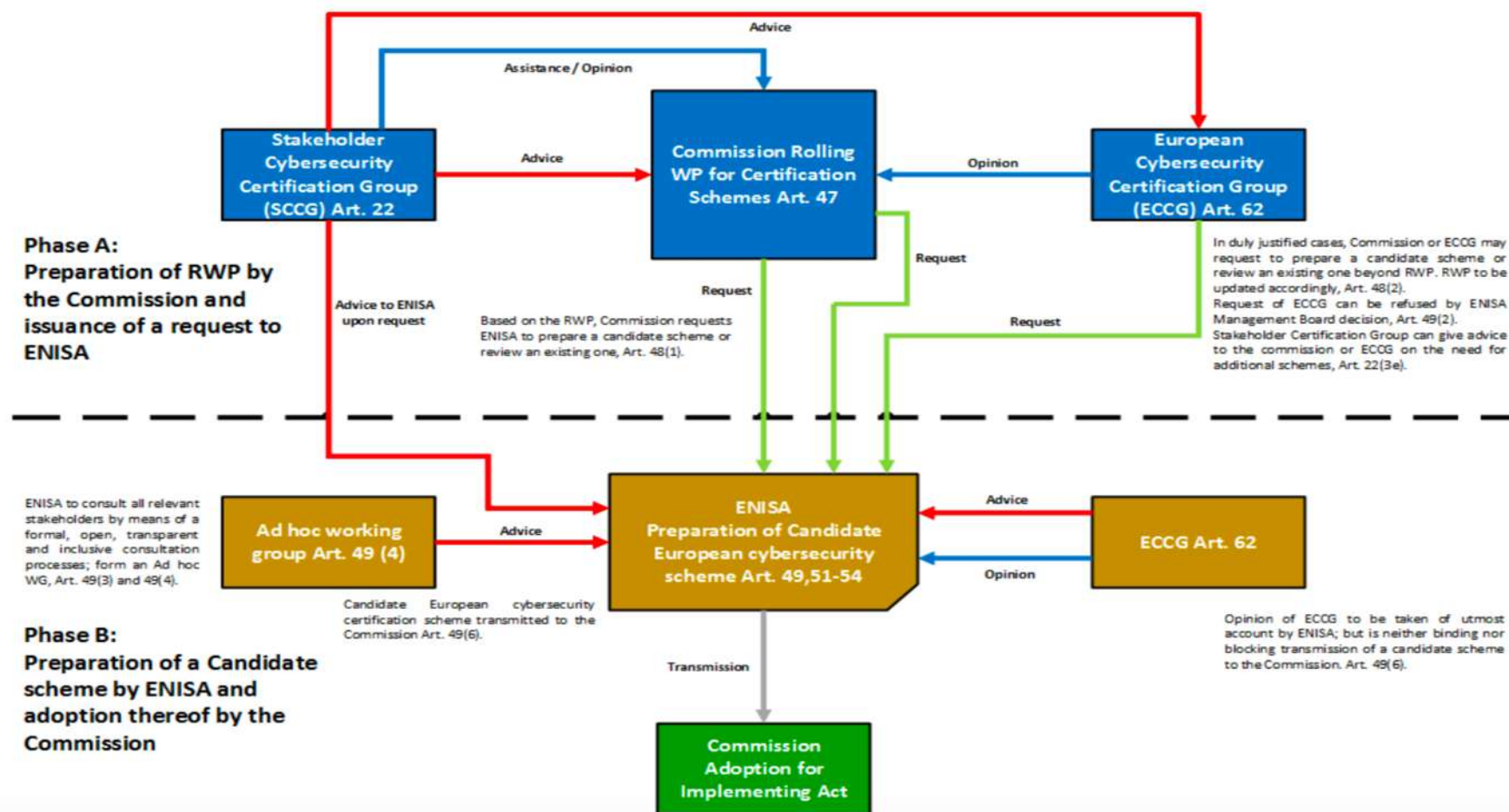


# The Process



Bolstering ENISA in the EU cybersecurity certification framework

Draft | **Public** | V.1.2 | February 2019



# CSPCERT WG

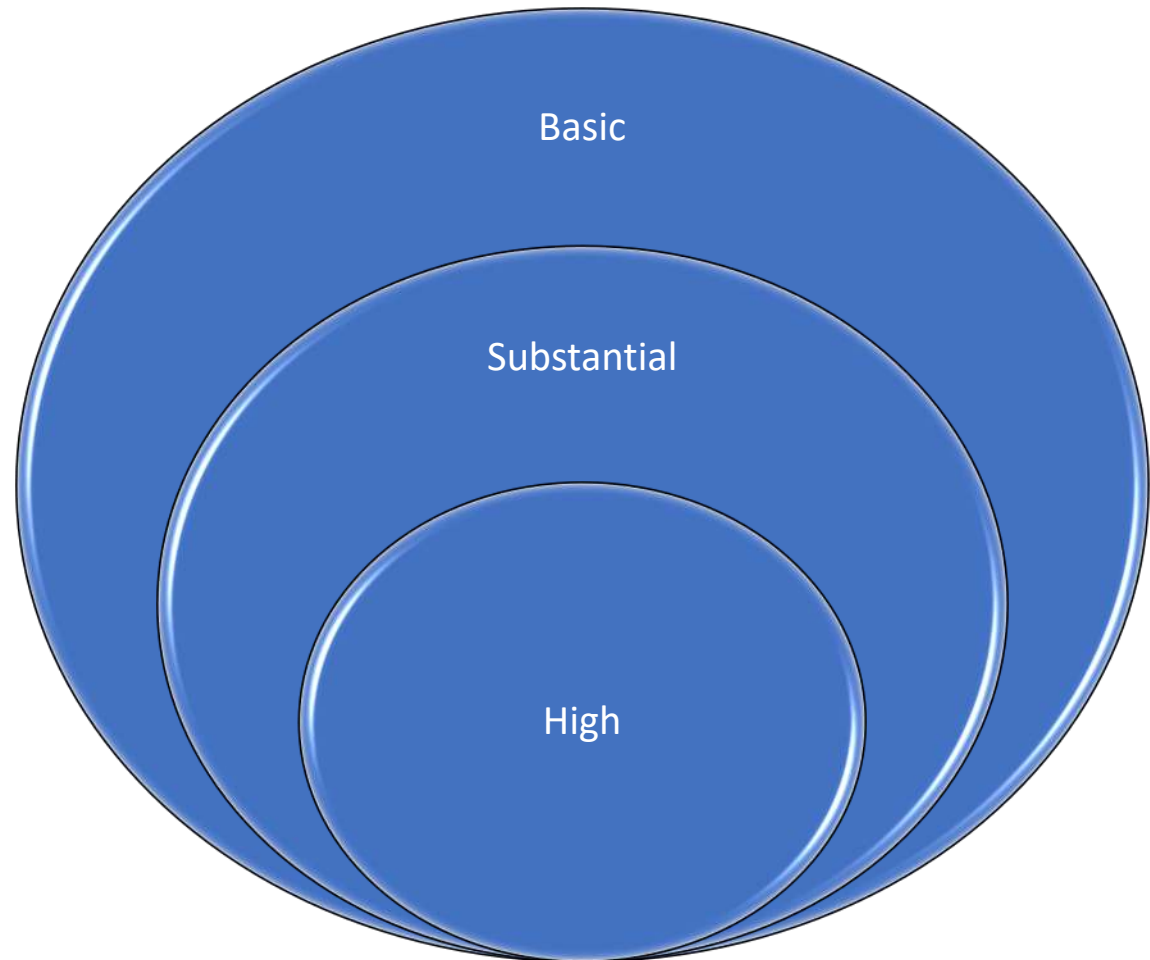
Established to provide expert recommendations to the EC for a scheme on cybersecurity certification of cloud services.

Composed by experts from Industry, National Security Agencies, Certification schemes owners, etc.

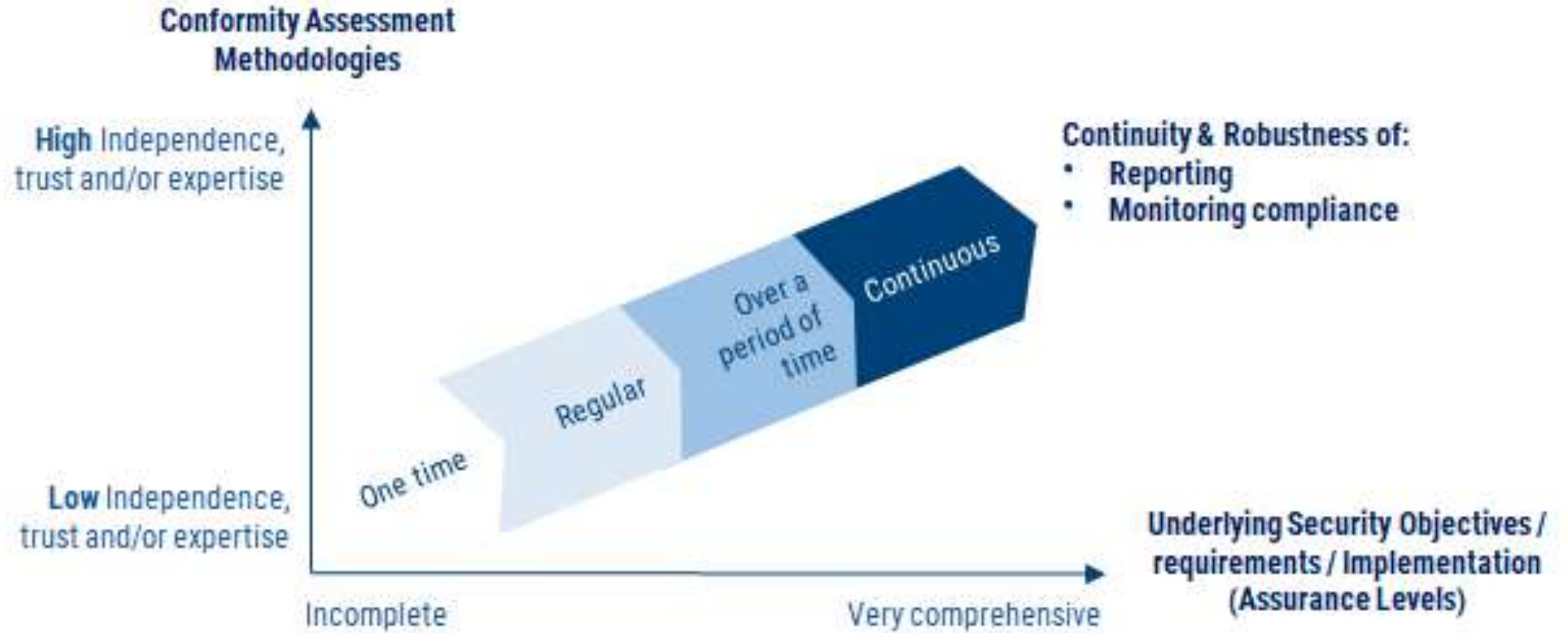


# Levels of Assurance – Art. 52

- Basic: *“a level which aims to minimise the known basic risks for cyber incidents and cyber attacks.”*
- Substantial: *“a level which aims to minimise known cyber risks, cyber incidents and cyber attacks carried out by actors with limited skills and resources.”*
- High: *“level which aims to minimise the risk of state-of-the-art cyber attacks carried out by actors with significant skills and resources”*



# Assurance Dimensions



# Recommendations: Approach

- NOT a completely new certification scheme
- Leverage existing and suitable industry, national and internationally recognized schemes
- Create a certification framework for them to co-exist

# Recommendations: Assurance Levels

The assurance level shall be commensurate with the level of the risk associated with the intended use of the cloud service.

ENISA should provide a guidance on:

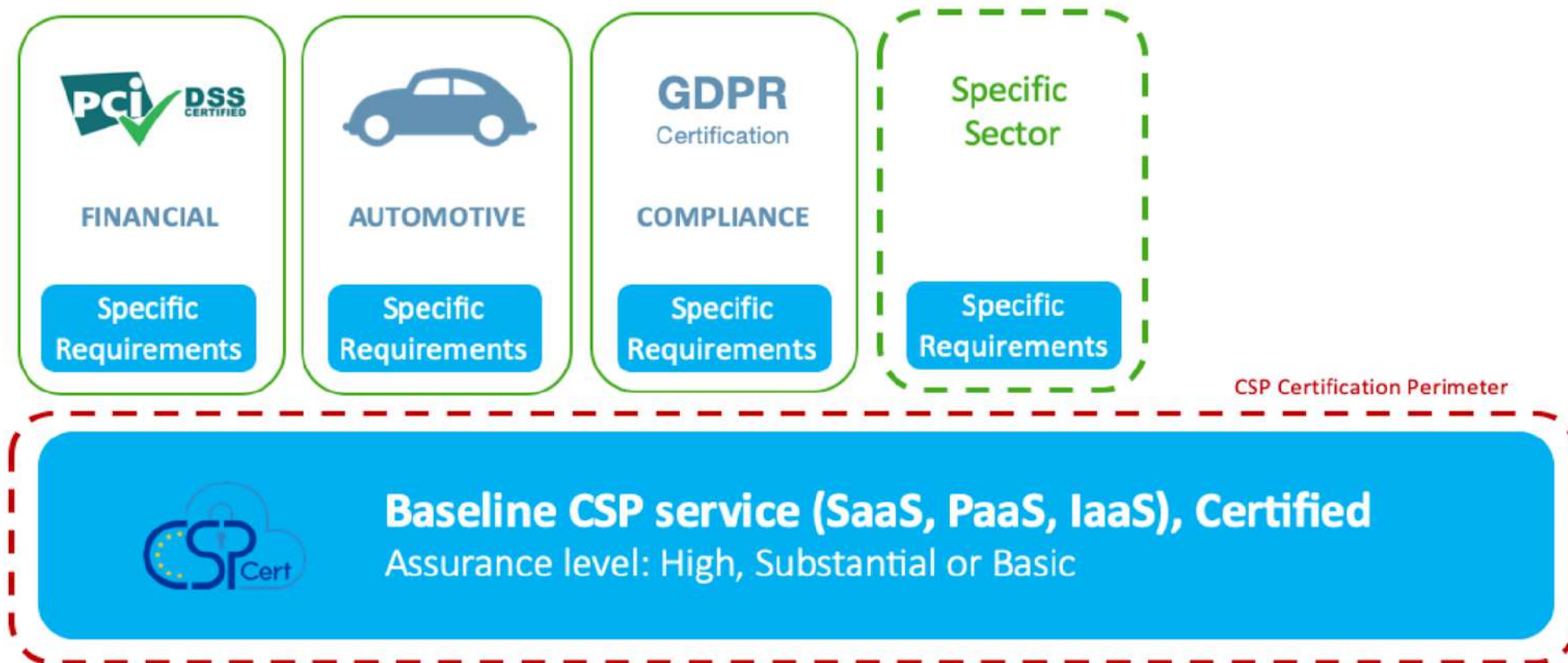
- what Basic/Substantial/High level indicate, and
- examples of type of service requires which level of assurance

# Recommendations: Evaluation Criteria

- Evaluation criteria/Security controls/requirements should be based on a taxonomy
- Allow mapping between existing standards & certs (SecNumCloud, C5, ISO 27017, ISO 27018, CSA CCM, and NIST 800-53).
- Remain flexible for future updates

# Recommendations: Evaluation Criteria

Create a baseline open to future regulatory and industry specific requirements



# Recommendations: Conformity Assessment

The scheme should:

- Reduce the level of auditor bias
- Ensure Conformity Assessment bodies & Auditors provide same level of trust
- At least annual audit required for High and Substantial
- Measure operational effectiveness, not merely control existence.

# Recommendations: Conformity Assessment

3 suitable conformity assessment approaches identified:

- Evidence Based Conformity Assessment
- ISO-based
- ISAE-based (assurance-based)

Pentesting and Continuous auditing required for HIGH

# Conclusions

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

The cloud certification framework under the CyberSec 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:

- Won't increase the compliance effort of mature CSP
- Create market pressure for less mature CSPs to improve their security posture
- Increase the level of transparency and accountability across the cloud supply chain

???



# Helpful Links

VIA [WWW.CLOUDSECURITYALLIANCE.ORG](http://WWW.CLOUDSECURITYALLIANCE.ORG)

## Cloud Controls Matrix

[https://cloudsecurityalliance.org/workin-g-groups/cloud-controls-matrix/#\\_downloads](https://cloudsecurityalliance.org/workin-g-groups/cloud-controls-matrix/#_downloads)



## Open Certification Framework

[https://cloudsecurityalliance.org/workin-g-groups/open-certification/#\\_overview](https://cloudsecurityalliance.org/workin-g-groups/open-certification/#_overview)



## CSA STAR

[https://cloudsecurityalliance.org/star/#\\_overview](https://cloudsecurityalliance.org/star/#_overview)



## GDPR Center of Excellence

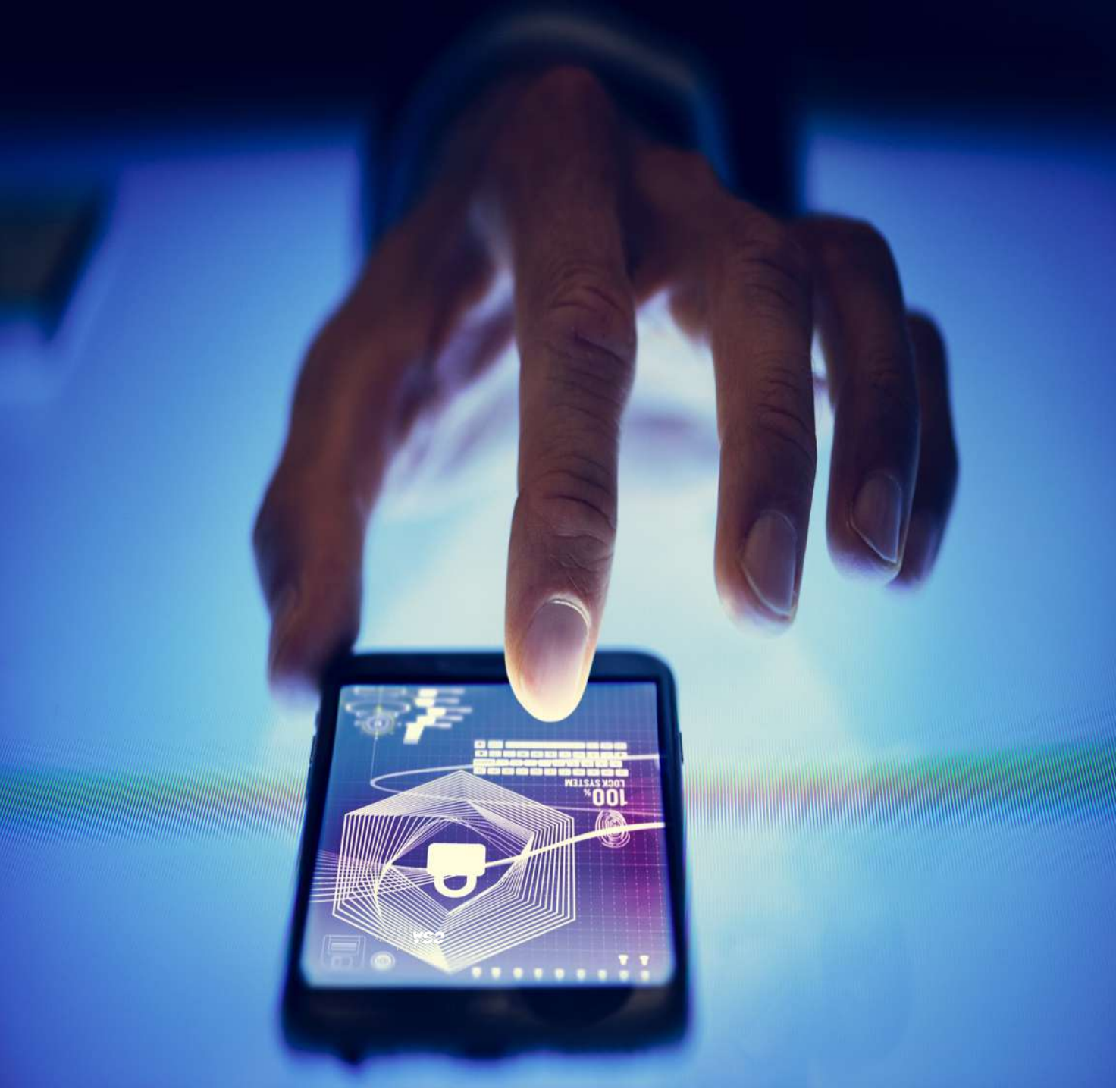
<https://gdpr.cloudsecurityalliance.org/resource-center/>




## EU-SEC Project

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







## Contact

 [dcatteddu@cloudsecurityalliance.org](mailto:dcatteddu@cloudsecurityalliance.org)


---

 Seattle > Bellingham > Berlin > Singapore

---

 Visit us on the web at  
[www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org)

---

 Follow and like us @cloudsa

# Resources

---

- CLOUD CONTROL MATRIX: [https://cloudsecurityalliance.org/group/cloud-controls-matrix/#\\_overview](https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview)
- STAR PROGRAM OVERVIEW: [https://cloudsecurityalliance.org/star/#\\_overview](https://cloudsecurityalliance.org/star/#_overview)
- CSA STAR REGISTRY: [https://cloudsecurityalliance.org/star/#\\_registry](https://cloudsecurityalliance.org/star/#_registry)
- EU-SEC Project: <https://www.sec-cert.eu>
- CSA Code of Conduct for GDPR Compliance: <https://gdpr.cloudsecurityalliance.org/public-registry/>
- CSA GDPR Center of Excellence: <https://gdpr.cloudsecurityalliance.org>
- CSPCert: <https://cspcerteurope.blogspot.com/2019/06/final-public-private-recommendation-for.html>