The impact of EU Cyber-Security Act on Cloud

***Daniele Catteddu**, CSA Chief Technology Officer*

OUR Community

90,000+

INDIVIDUAL MEMBERS

75+

CHAPTERS

300+

CORPORATE MEMBERS

30+

ACTIVE WORKING GROUPS

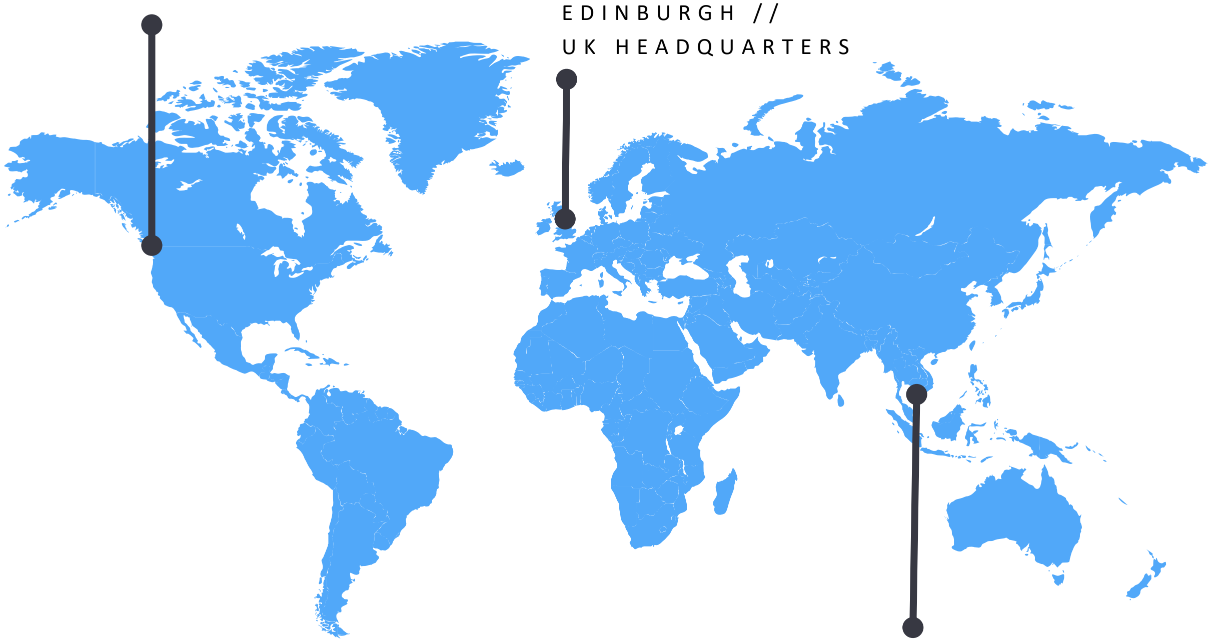
Strategic partnerships with governments, research institutions, professional associations and industry

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

CSA research is FREE!

2009

CSA FOUNDED

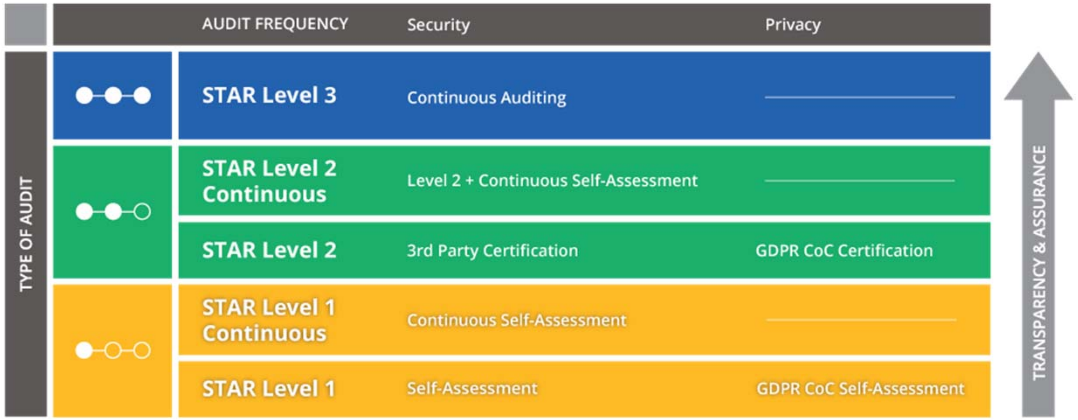


SEATTLE/Bellingham, WA //
US HEADQUARTERS

EDINBURGH //
UK HEADQUARTERS

SINGAPORE //
ASIA PACIFIC
HEADQUARTERS

CSA’s activities in Cloud Assurance and Certification



TYPE OF AUDIT	AUDIT FREQUENCY	Security	Privacy
●●●	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

CCM™

Cloud Controls Matrix

EUSEC

EU SECURITY CERTIFICATION

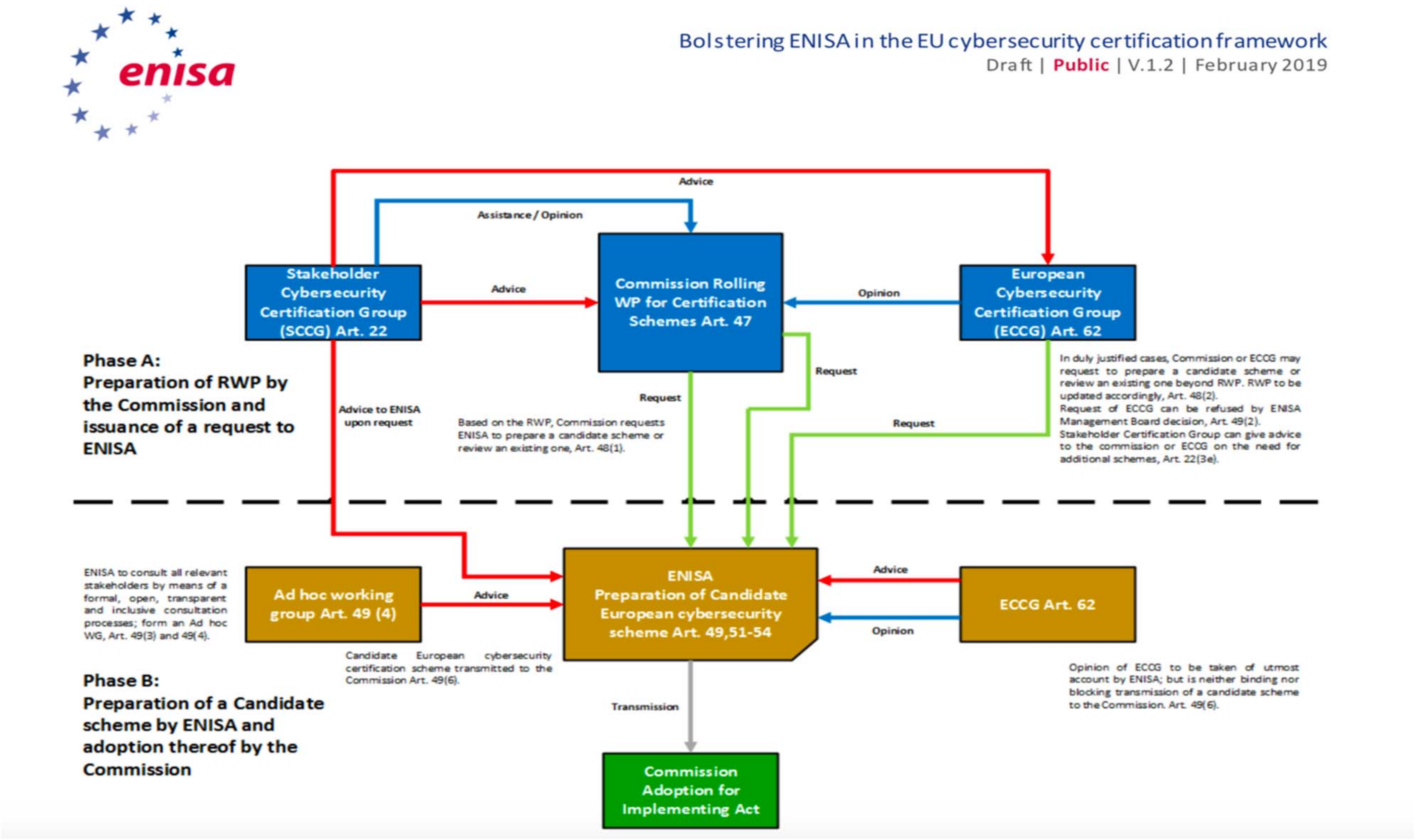
Background

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

Certification Scheme: the Process



Bolstering ENISA in the EU cybersecurity certification framework

Draft | Public | V.1.2 | February 2019

Phase A:
Preparation of RWP by the Commission and issuance of a request to ENISA

Advice to ENISA upon request

Based on the RWP, Commission requests ENISA to prepare a candidate scheme or review an existing one, Art. 48(1).

In duly justified cases, Commission or ECCG may request to prepare a candidate scheme or review an existing one beyond RWP. RWP to be updated accordingly, Art. 48(2).
Request of ECCG can be refused by ENISA Management Board decision, Art. 49(2).
Stakeholder Certification Group can give advice to the commission or ECCG on the need for additional schemes, Art. 22(3e).

ENISA to consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation processes; form an Ad hoc WG, Art. 49(3) and 49(4).

Candidate European cybersecurity certification scheme transmitted to the Commission Art. 49(6).

Opinion of ECCG to be taken of utmost account by ENISA; but is neither binding nor blocking transmission of a candidate scheme to the Commission. Art. 49(6).

Phase B:
Preparation of a Candidate scheme by ENISA and adoption thereof by the Commission

enisa
Advice
Assistance / Opinion
Stakeholder Cybersecurity Certification Group (SCCG) Art. 22
Advice
Commission Rolling WP for Certification Schemes Art. 47
Opinion
European Cybersecurity Certification Group (ECCG) Art. 62
Request
Request
Request
Ad hoc working group Art. 49 (4)
Advice
ENISA Preparation of Candidate European cybersecurity scheme Art. 49,51-54
Advice
Opinion
ECCG Art. 62
Transmission
Commission Adoption for Implementing Act

Proliferation of Schemes

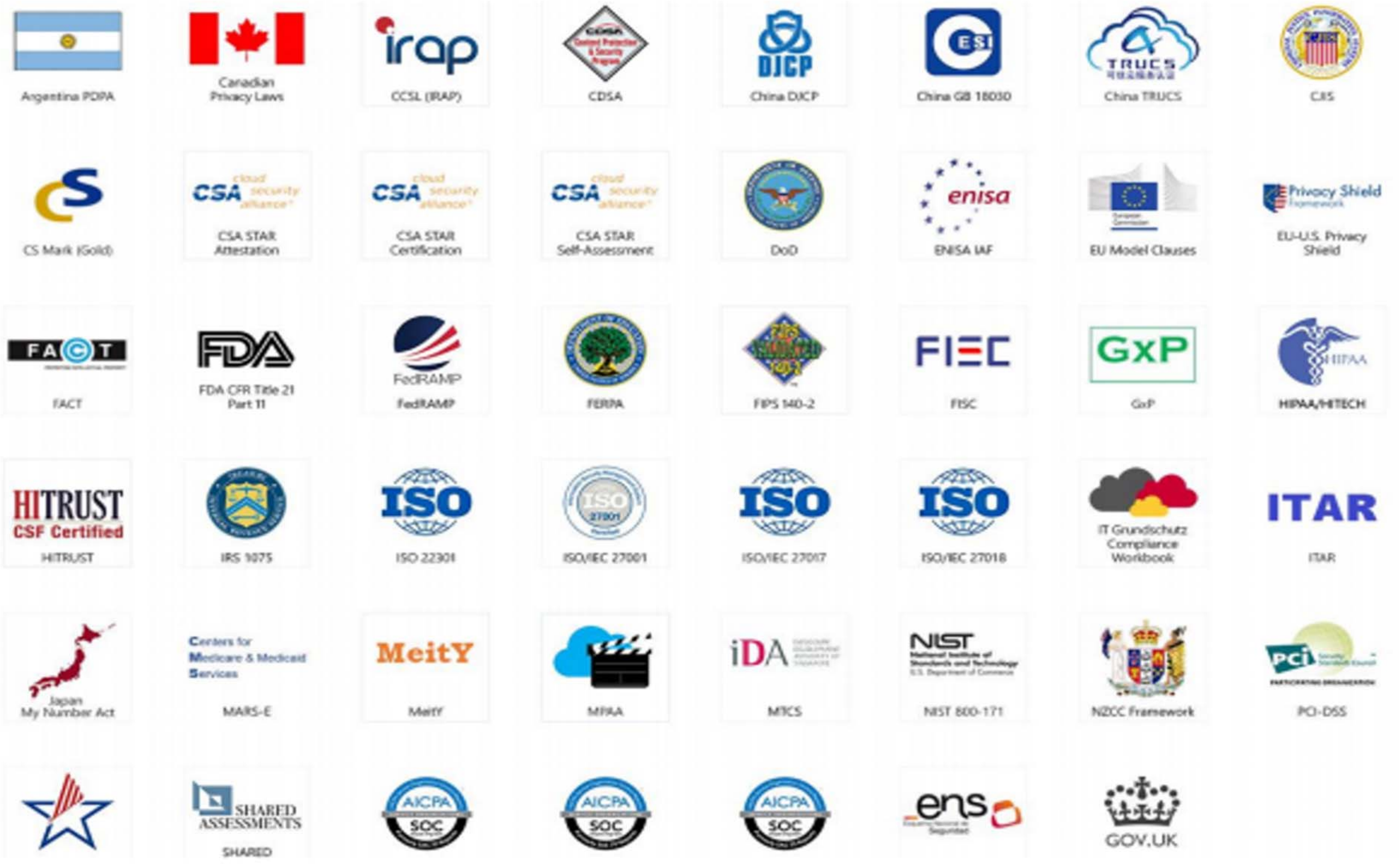


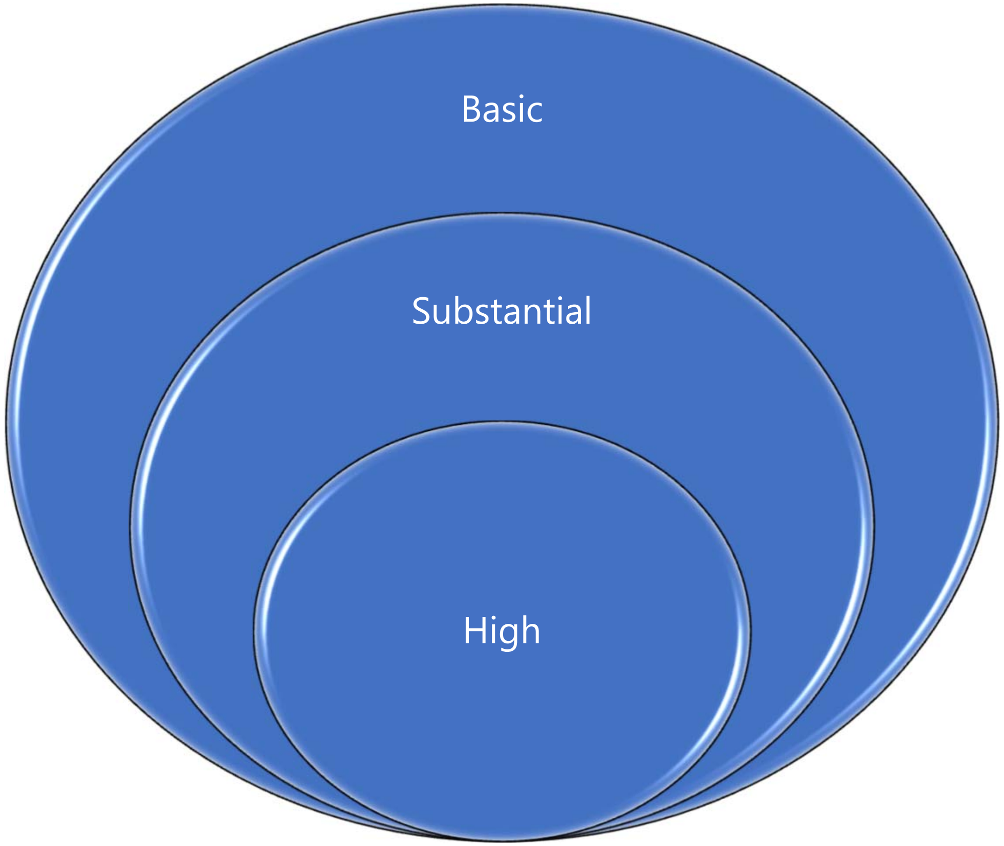
Fig1. Compliance Templates Provided By Microsoft

Lack of Clarity

Uneven Landscape

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*"

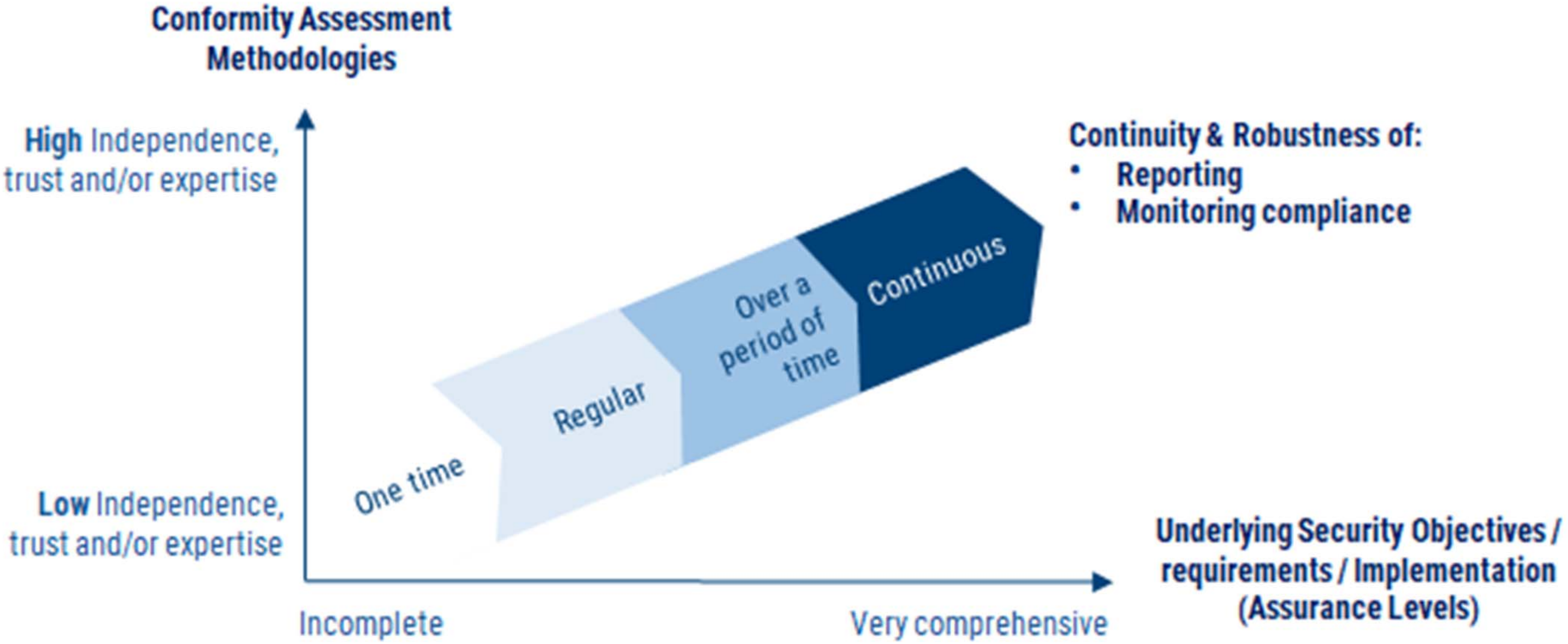


CSPCERT WG

The Cloud Service Provider Certifications Working group (CSPCERT WG) was created on December 12th 2017 to provide expert recommendations to the European Commission for a scheme on cybersecurity certification of cloud services.

The objective of the CSPCERT WG is to explore the possibility of developing a European Cloud Certification Scheme in the context of the Cybersecurity Act and come up with a recommendation that will be presented to the European Commission and ENISA.

Assurance Dimensions


Conformity Assessment Methodologies
High Independence, trust and/or expertise
Low Independence, trust and/or expertise
One time
Regular
Over a period of time
Continuous
Continuity & Robustness of:
• Reporting
• Monitoring compliance
Incomplete
Very comprehensive
Underlying Security Objectives / requirements / Implementation (Assurance Levels)

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 clear guidance on:

- tailored description of what the basic/substantial/high assurance level indicate, and
- examples of which level of assurance should be associated to which services.

Recommendations: Evaluation Criteria

The evaluation criteria (AKA security controls/requirements) should be based on a taxonomy so to allow the mapping between existing international standards and certifications (SecNumCloud, C5, ISO 27017, ISO 27018, CSA CCM, and NIST 800-53).

ENISA should create EU taxonomy so as to remain flexible for future updates, modifications or additions to new or existing international standards and certifications.

Recommendations: Evaluation Criteria

A baseline certification that could optionally be enhanced with further regulatory requirements coming from regulators, supervisors or the industry such as:

- GDPR certifications,
- Outsourcing requirements from the EBA,
- e-evidence,
- eIDAS,
- e-privacy
- ETC

Recommendations: Conformity Assessment

The CSPCERT WG proposes 3 suitable conformity assessment approaches:

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

The objective is to:

- reduce the level of auditor bias
- ensure that the level of trust provided by conformity assessment bodies and individual auditors is within acceptable ranges everywhere.

Recommendations: Conformity Assessment

- For Assurance levels High and Substantial an annual audit is a min. requirement.

- For High level it is recommended to adopt a continuous auditing approach so to increase the frequency of the evaluations and ensures a level of assurance that goes beyond “point in time” or “over-a-period-of-time”.

- Audit must measure operational effectiveness, and not merely control existence.

- ENISA should clarify what would trigger a new out-of-cycle review.

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 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:

- 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

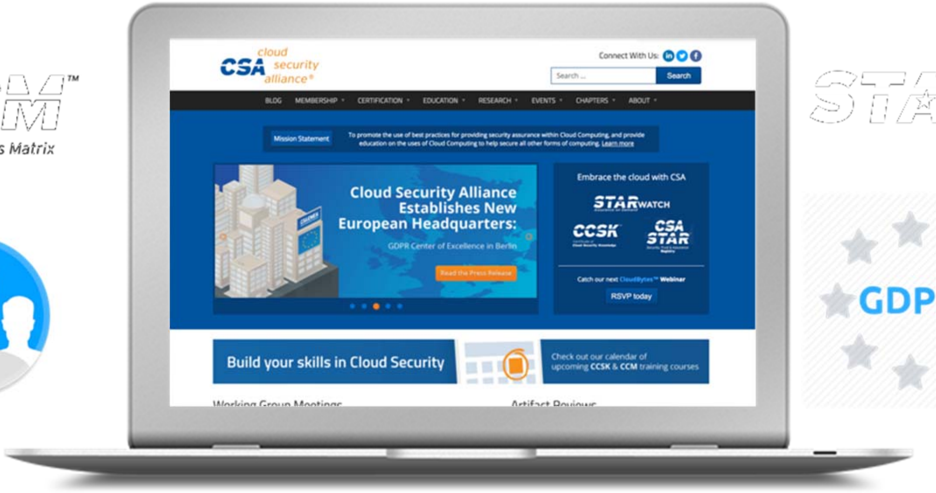
VIA WWW.CLOUDSECURITYALLIANCE.ORG

Cloud Controls Matrix

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

Open Certification Framework

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



To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing. Learn more

Cloud Security Alliance Establishes New European Headquarters:

GDPR Center of Excellence in Berlin

Embrace the cloud with CSA

Catch our next CloudBytes™ Webinar

Build your skills in Cloud Security

Check out our calendar of upcoming CCSK & CCM training courses

CSA STAR

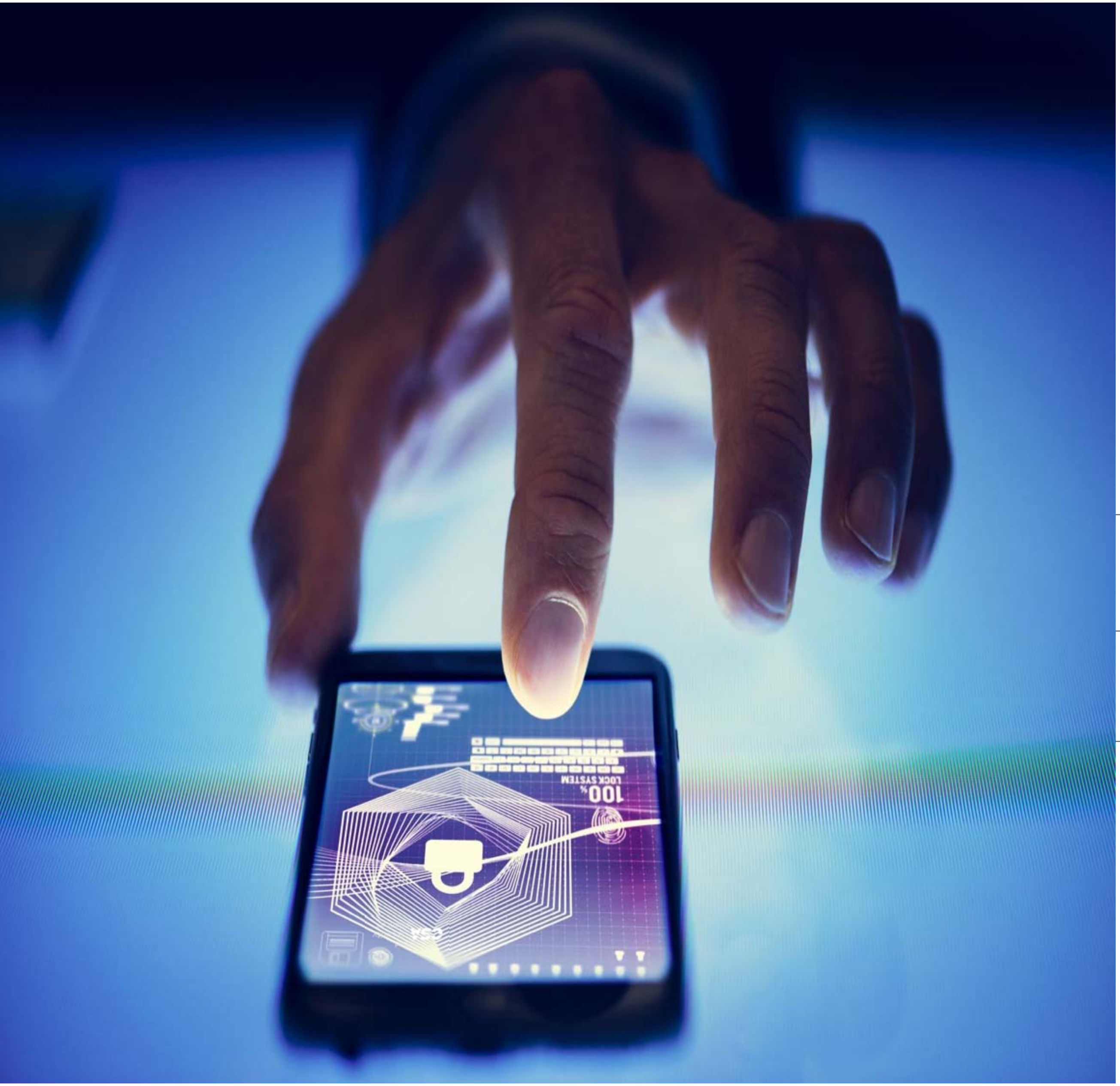
https://cloudsecurityalliance.org/star/#_overview

GDPR Center of Excellence

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

EU-SEC Project

https://www.sec-cert.eu



Contact

✉ dcatteddu@cloudsecurityalliance.org

Seattle > Bellingham > Berlin > Singapore

Visit us on the web at
www.cloudsecurityalliance.org

Follow and like us @cloudsa

Resources

- CLOUD CONTROL MATRIX: https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview
- STAR PROGRAM OVERVIEW: https://cloudsecurityalliance.org/star/#_overview
- CSA 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