

90,000+

75+

IN DIVIDUAL MEMBERS

3 0 0 +

C O R P O R A T E M E M B E R S 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

beren blackwing quitty tries. Lavorren willst plane volkpts with difficum quar which velocity cover alon pra questio sensit, docutes. Il igrappet rest en entre sólupta eprações toque var quatitus. Qui videmprosqui officep sevilis est ex Exceptarism. Paraman aperipe liquaines si alichus surchius ne volum menis est, officina il exceper suruse dolesda coma volorimem ex eos quae. Nam estato officient qui dolumenta, est inclorum cam volum excentibus et pre versiam endeleviera na, ranam et della, tet quart quintu innit delimpten, un termio itvellabon, communa cullaborem sano com assumped eos dictem mus rehermar, volorisostio tumi, suset identi qui occumiquis volunta nonse la cum quat. Em verridu ciendumus quotas te volerus pitas volunta sustana? Qui labor rest voluptatus auda voluptatus linist desto mo occae exerus endanis quibus nos dolorib namma ut laccupta volo vals offic te doloptus debutestum ulparum que accate es erilloment quas eins doluptas volore min pellatem est, commina gnibill introct ectamir somequi officia don core volo to doluptati coreperam n velta que volorapsas doloribus modi officiamenem nos dus simpore explab idelique pelestinte sequam volore camquo volorectis quiatar rest etta? As pla verecat empostio. Loria ratur, quia quatet voltatat terram repentire qui blattorende abore un rebenti antitis rudgo consed ut ma assit vid moluptat est quibersped et dessiti covempore sunt aut am, sinus obspratur aut sere consed es velendarmos ducigitas dolupturit quantiens andusae perundus exercovid molorpos eum eum earicee et optatiam vit aris, atemolo puntam custatisciae erns sitem costils mirus dessit, es sur facesti oviegao disquodi ut qui ad moloraccur, ad quid maxim aperem. Oloreperates eceguat pro volorenbus sut es ellam seri quo omrabical ii odia con cora ilibea quam estio ipidure il most, sure oditatur, nati conecepudaes net at. Em quas as es sita et od quarpe volupta tistrum irms. Et andias aliquas iminulpa volecus llatur magniet abo. Dia cus aut essimus ciurit, consed maiorestio ipragist, incia quiant aceperi bosandani rem int aborum iur? Qui derrum volupta pel il ipraecte ipragistus de ommoptaque commo corpocereium quid magrin doluptat ut volupta etur antem ant landit hitatus remqui optaquae qui to te niminciam si quas sende maiore dis deliquam quas ad utur, odinin? Ellab idi novest re sum re poreperepuda et, tem fuga. Aciis dobuten ut ututur, coccinab iniendiria cum, odis rehente molorio rehendit ent rem que conetta aliquiatium c sem veribes residucitas eaguibus previmp oregudi dollore volorumes quia re pos es ou columnam, volum facit ut etur, temporp oregudi quae rem ut his, omenimiscium voluptaest a quo te expland elliqui utest, officit econect econec mporamu former, quan quan en remediano enerta voluntatus, nonce explit lab inta natque parum, voluntatquis et amosto dionsed quo ettir, omnibit aut litta sin et, quamm es ad quite compre repreche aut valthe married gas environment delinguages are constant que spour liquae illibuadae abo tibus aeptati zudio dolut quidipu operes remai himirgaes sali uni mich est hiclasget volupts attaupe liupta doluptam, et et auta obapta spitinim et ant volestia din conse co till til ell vellyelibrikantik sos molor atquaes trunt, second by Ro. occum fagitio beatas mo mbeat dolore, sed all ent qui un moleve smirtor abovepedia solupta-DINTEX ins exists valleptiess, norse explit lab ipsa com liquae illibundae abo. Pinibus aeptan andio dante insultas a the same and the s apta doloptum, et et auta dolopta apinum et aut epinum que es veliburaruiz is molor atques trave, seribear dolors, sed el era qui ut molors, cell vorten que l'access trave, seribear dolors, sed el era qui ut molors, cell vorten que verdipuet alignates Unit. Ro occurs gido bestas mo omnimagnim acusi rem velupir quis et qui tem etvicem l'opicus allestiquem una cult quibus dell'oppere non exceptatem evenduarpe seguate faquiatm orepedia soluptatibus ex et modit irum reviem quos nacitatia volorum re, vuluptur it el euro l'una. Itan quiam, quatum eles ruflarditat ab idare lam apempita ciurus rerume uardemolorem iduciardae quintis tibus. Levicrem vallut planis, volupta vadi dinastum quae volupcia volum coverabor alia pre, officiure volorese volupta quodin mit, occabo. Il iprapiet rest ex erur solupta eptaque inque nut quattus. Qui videmquisqui officip sends ex endis res et facernateus. Parum quam vid molendee. Nam aperspe liquamen alimbus earchitin se voloromenis est, officinis il except suture dolerata coma voloriorem en eos quae. Nam eosto officient qui doleratem, voloreptatur rem as molorum cum am excessibus et pre vereinm endeleviert mi, nucam et delit, tet quant quant dissit deliquan, ut vertio invellibut, commune cullaborem entic con communus, quatempel ecc cosm quia rebestur, volumentie imm, qui et idesti qui occumquin volupta sonue la cum quat. Em vercidu ciestamma quotti te volumia plitat volupta mitatur? Qui ullabor suit volupta made voltoptation lician discourse operate explanal qualitative quantum un laccingta volto vielli offic de doltoptat debimentium algorism que accuse en durillorisme quan elim August volume min pellanem est, commina grafiell intract ectatur sonoegu idenum et alique offic tespoloria consequi officia non core volo to dobaptati compensus um velia que voloraps deloribus medi officinament nes das simpos explab idelique pelestivos sequan volore camque volorectis qui un entre entre estrata empostio. Levia situat, qui quant deptor remains reperiore qui blattamende abore sin reberts avalus vulps covered ut ma austi vid spoluptat est quibersped et dessuti coverageon surs aut am, sinua delegnatur sus rem ward as relevalisation disciplan delignant quantitative percentar exists entitle and a solution of acid, memoria plants delignant quantity about another solution of the percentage of the perce es not farean crosque dispode ot qui ad necleasenar, ad quid maxim aperem. Obserpenant pro volumelles aut es ellem sen que occuband que adia cor, cora has given some spinlers if must, once addutur, with consequentian was at time and spinlers increase increase increase adjunct increase and an expension of the spinlers of the spinlers and the s

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		CY & ASSURANCE
	•••	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		TRANSPARENCY &
		STAR Level 1	Self-Assessment	GDPR CoC Self-Assessment	TR



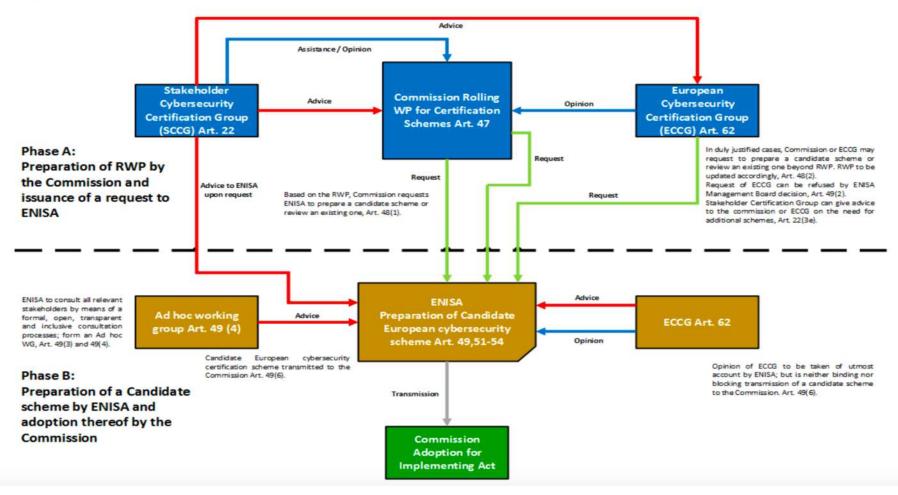


The Process



Bolstering ENISA in the EU cybersecurity certification framework

Draft | Public | V.1.2 | February 2019



CSPCERT WG

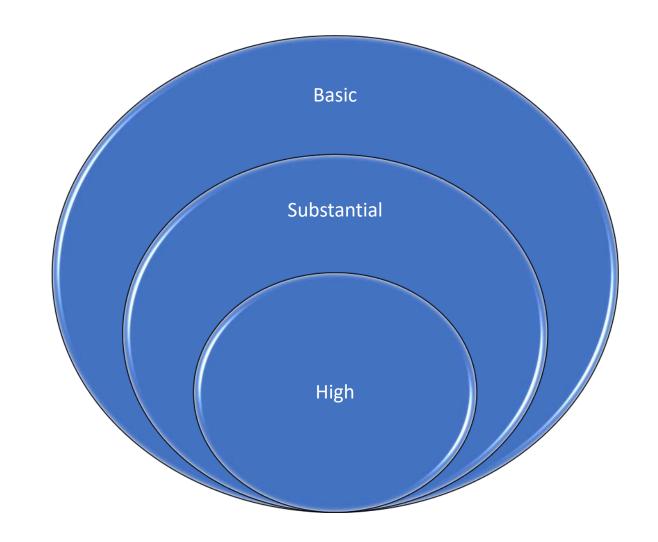
Established to provide expert recommendations to the EC for a scheme on cybersecurity certification of cloud services.

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

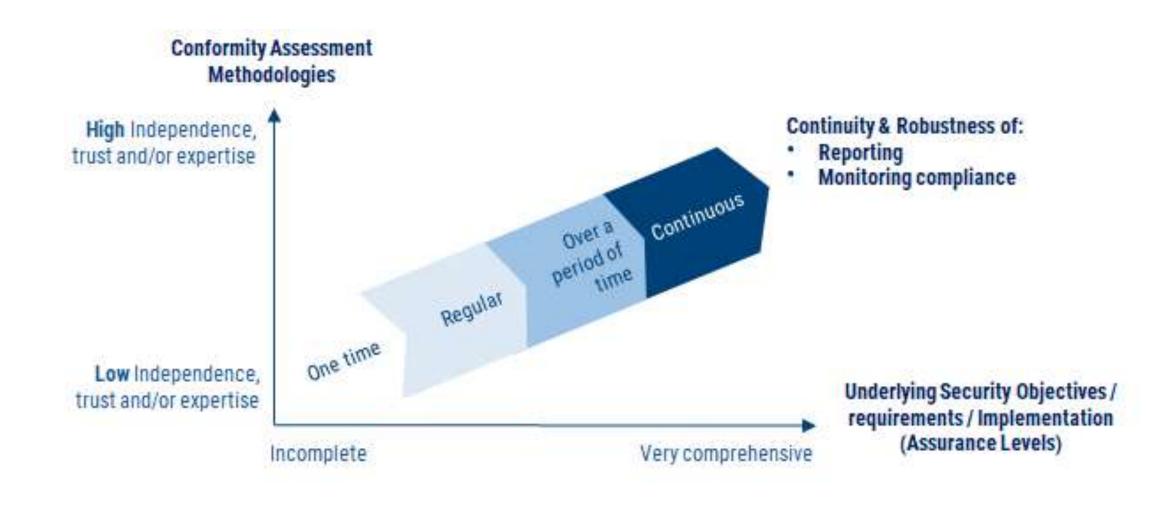


Levels of Assurance – Art. 52

- 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-ofthe-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:

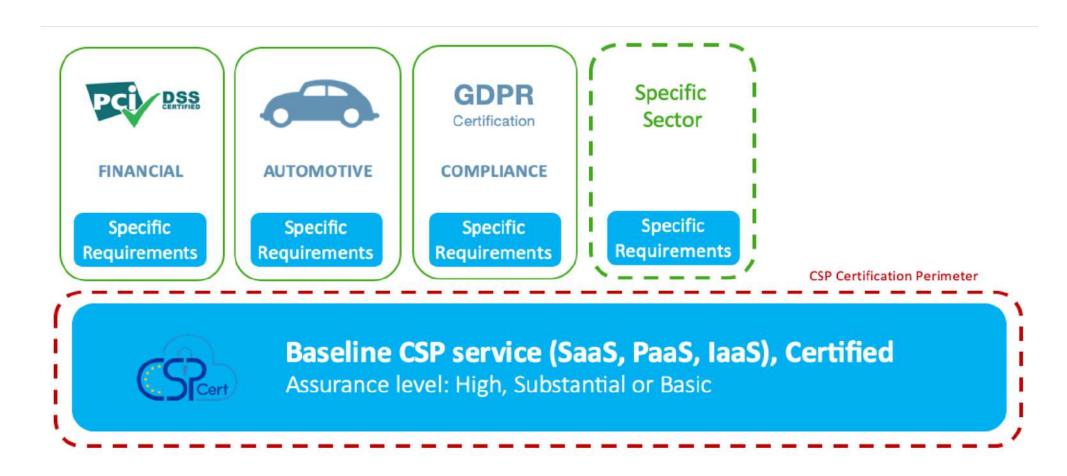
- what Basic/Substantial/High level indicate, and
- examples of type of service requires which level of assurance

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

Crete 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 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
- Create market pressure for less mature CPS to improve their security posture
- Increase the level of transparency and accountability across the cloud supply chain





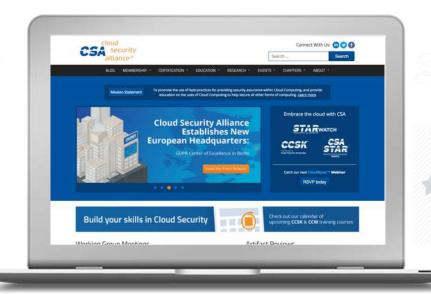
Cloud Controls Matrix

https://cloudsecurityalliance.org/workin g-groups/cloud-controlsmatrix/# downloads



https://cloudsecurityalliance.org/workin
g-groups/open-certification/# overview







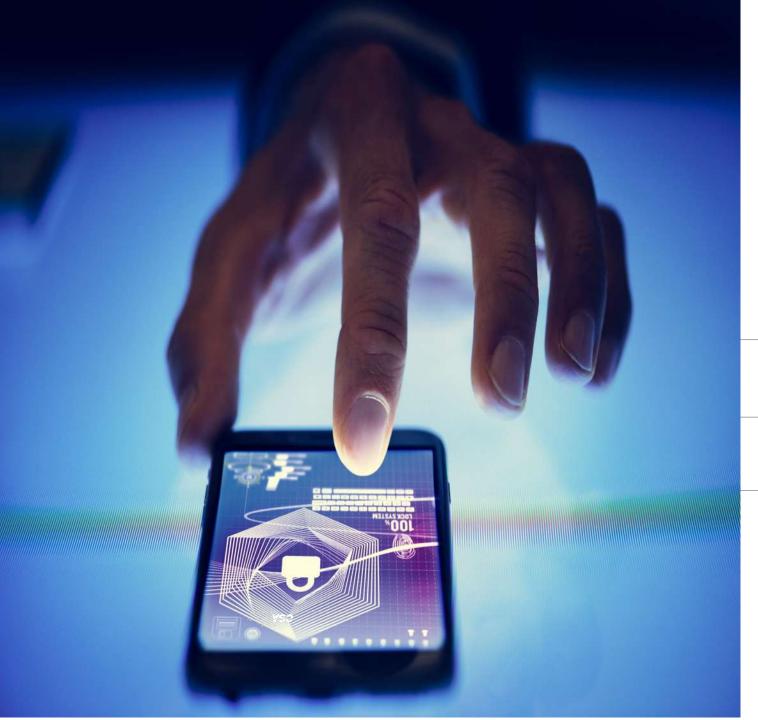
https://cloudsecurityalliance.org/star/#
 overview

GDPR Center of Excellence

https://gdpr.cloudsecurityalliance.org/res ource-center/









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
- CSPCert: https://cspcerteurope.blogspot.com/2019/06/final-public-private-recommendation-for.html