DIGITALEUROPE

5 DECEMBER 2019

DIGITALEUROPE's commentary on CSPCERT's recommendations to ENISA for a Cloud Security Certification Scheme

Executive summary

DIGITALEUROPE supports the objective to improve the EU's level of cybersecurity and resilience. Greater homogeneity across all Member States will reduce barriers to entry for cloud service providers (CSPs), benefitting in particular the survivability and growth of European SMEs.

DIGITALEUROPE has witnessed a proliferation of cloud cybersecurity schemes and procurement specifications from many public sector bodies across the EU. Reducing this fragmentation is a noble goal, especially if an EU-wide scheme is sufficient to cover the broad needs of the public sector as well as other organisations. To this end:

- Existing, well-established international standards need to be prioritised to provide assurance to cloud customers.[1] Any gaps in international standards should be harmonised within the standardisation system, preferably with the goal of international endorsement.
- Where Member States' schemes exist, mutual recognition between Member States' existing cloud security schemes should be established while an EU-wide scheme is being developed. Failure to do so creates a substantial barrier to entry, particularly for SMEs who will not have the resources to survive across Member States in a very competitive market. The Commission should investigate whether SOG-IS, and its transition into an EU scheme, can help in this respect.
- Assurance levels should build upon each other by adding security and assurance requirements from basic to substantial and from substantial to

[1] In alignment to CSPCERT's statement (p. 9) that the WG 'is not proposing a completely new certification scheme but providing guidance for a scheme based on existing practices/schemes/standards used by the industry and internationally recognised.'

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

high. Other approaches would cause serious issues for SME providers trying to enhance security and could confuse customers.

- As mentioned in the CSPCERT Executive Summary, the suitability of the provided recommendations could be enhanced by the Commission's and ENISA's guidance through the refinement of the scheme to specific sectoral threats.

Table of contents

Introduction

DIGITALEUROPE supports the objective to improve the level of cybersecurity and resilience across Europe. The Cybersecurity Act, in particular, aims to contribute to this strategic priority by establishing an EU-wide cybersecurity certification framework ensuring a common approach in the European internal market. This will ultimately improve cybersecurity in a broad range of digital products and services.

The first Digital Single Market (DSM) Cloud Stakeholder Group met in June 2017 and since then has worked to explore a possible candidate certification scheme in the field of cloud security under the framework proposed by the Cybersecurity Act.

This work was underpinned by the study commissioned under SMART 2016/0029 'Certification schemes for cloud computing' from March 2017 to March 2018. The methodology used in the SMART-commissioned report included analysing current certification requirements, analysing the results of 150 completed surveys and conducting a workshop with 85 participants. The final recommendations from CSPCERT[2] were presented in June 2018 and in summary align to ENISA's Cloud Certification Schemes Metaframework with a variety of conformity assessments for different assurance levels.

The purpose of this commentary is to provide feedback on CSPCERT's recommendation for the implementation of the CSP certification scheme that can be used by the Commission when considering proposing a scheme and ENISA when preparing one.

The EU market, cybersecurity certification and standardisation

As the 'Certification schemes for cloud computing' study identified, CSPs are required to demonstrate alignment or compliance to over twenty different frameworks. This is required to address general misconceptions and misunderstandings about the security of cloud services, the control of data and compliance to existing frameworks. This is further complicated by the rise of mandatory schemes to provide assurance to public sector organisations in various Member States.[3]

This requires a significant amount of investment for cloud providers, including but not limited to: the costs related to instructing a third-party auditor throughout the lifecycle of the scheme; consultancy to advise on the requirements of the scheme;

---

2 CSPCERT WG (Milestone 3), 'Recommendations for the implementation of the CSP Certification scheme,' available at https://drive.google.com/file/d/1J2NJt-mk2iF_ewhPNnhTywpo0zOVcY8J/view

3 Most notably Germany's C5, France's SecNumCloud and Spain's ENS.

changes to the internal controls of the cloud provider's organisation; and technical enhancements of the cloud services. The result is that only the most well-resourced cloud providers can provide such level of investment to meet a plethora of requirements throughout the EU's internal market.

DIGITALEUROPE welcomes CSPCERT's acknowledgement of this resource constraint and the need to establish greater homogeneity in all Member States to reduce the barriers to entry for CSPs. This is critical to ensure the survivability and growth of DIGITALEUROPE's members, many of whom are SMEs. The suitability of CSPCERT's recommendations should be further investigated by ENISA while developing and refining the scope of an EU Cybersecurity Act scheme.

DIGITALEUROPE recommends that the Commission and ENISA be precise on the risk profiles that are to be covered by any new scheme, such as applicable to the public sector or operators of essential services (OES).[4] This would be in alignment to the principles documented within the Cybersecurity Act, specifically:

> *'(78) The choice of the appropriate certification and associated security requirements by the users of European cybersecurity certificates should be based on an analysis of the risks associated with the use of the ICT products, ICT services or ICT processes. Accordingly, the assurance level should be commensurate with the level of the risk associated with the intended use of an ICT product, ICT service or ICT process.'*

Whilst CSPCERT has admirably attempted to recognise this complexity with the three assurance levels required by the Act, the difficulty in defining three assurance levels to cover all risk profiles should not be underestimated.

For example, the public sector is presented with complexity across different bodies. These include on the one hand organisations that are more likely to fall prey to commodity attacks (such as a Ministry for Agriculture), and should therefore only need a 'basic' level of assurance, and on the other organisations that are more likely to be targeted by bespoke attacks (such as a Ministry for Defence) and would hence need a 'high' level of assurance.

DIGITALEUROPE is concerned that the analysis of the CSPCERT group has not sufficiently considered the respective roles and responsibilities of the CSP and the cloud customer in defining the right level of security, in particular for infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) providers. The recommendations assume that cloud customers can only rely on the level of assurance offered by a CSP and cannot build upon it. However, security is a shared

[4] As defined by the NIS Directive.

responsibility and cloud customers are generally able to enhance their overall security without exclusively relying upon the underlying CSP.

Furthermore, cloud customers not categorised as OES are more likely to experience much more effective security by migrating to cloud services than continuing to manage their own on-premise IT. For these organisations, cloud computing is no longer inherently a greater risk compared to managing their own ICT systems, though each customer should still conduct its own risk analysis.

We recommend that the Commission and ENISA undertake an in-depth risk assessment to help determine the risk profiles within the scope of any scheme.

Security objectives of European cybersecurity certification schemes

DIGITALEUROPE welcomes that the deliverables produced by CSPCERT are based on existing international standards and the Member States' cloud security certification schemes currently in force.[5]

Building upon CSPCERT's observation regarding the control differences of CSA CSM and NIST 800-53, we conclude that the gaps between the requirements of all the control frameworks considered in the CSPCERT analysis are rather small.

The acknowledgement of the overlaps present in existing schemes is critical. This highlights the growing burden CSPs face in having the same controls audited time and again. Not only is this inefficient and costly, but it also limits CSPs' resources away from the core task of providing the cloud service and confuses cloud customers who also have to understand multiple, yet very similar, schemes.

Taking this premise further, CSPs, whatever their size, cannot support such a burden without introducing a risk to the quality and security of the services provided. Given that many of the controls in the analysed schemes contain many of the controls that should be included in the management of any information system, the focus should be on identifying those controls that make cloud computing different. ISO/IEC 27017 provides an international baseline focused on the provision and use of cloud services, yet other schemes either do not build upon this standard or add to it.

DIGITALEUROPE believes that once the goals of a scheme have been identified, the required controls for such a scheme should be harmonised at European and International levels. This has the benefit of leveraging well-established schemes

[5] Notably, CSPCERT's work expanded upon the 'Certification schemes for cloud computing' study with a comparative analysis of ISO 27002, ISO 27017, ISO 27018, C5 and SecNumCloud. These were then cross-referenced to ENISA's Cloud Computing Schemes Metaframework.

maximising cloud customers' acceptance as well as cloud providers' own return on investment for their current compliance portfolios ('audit once, certify many').

Building assurance levels based on a harmonised set of controls enables substantial and high assurance levels to be defined based on extending existing prior levels. That is, a substantial assurance level should extend the security functionality and assurance requirements from a basic assurance level, and high should be an extension of substantial. Having each assurance level reference different control frameworks will make it harder for providers, especially SMEs, to build out their services and certify to additional assurance levels. It could also confuse customers as their responsibilities could be affected across assurance levels.

In the absence of international harmonisation and prior to the adoption of any EU scheme, a useful steppingstone would be to establish mutual recognition between Member States' individual cloud security schemes. This would significantly reduce the cost of doing business, particularly for SME providers, as well as reduce barriers for entry. In addition, the mutual recognition of existing schemes could be encouraged as part of the current review of the SOG-IS agreement and its transition under the EU Cybersecurity Framework.

Assurance levels of European cybersecurity schemes

DIGITALEUROPE welcomes CSPCERT's attempt to rationalise various conformity assessment methodologies in its proposed scheme. During its work, CSPCERT considered the applicability of recognised international approaches to conformity assessments, notably ISO 17021[6] and ISAE 3401. Admirably, CSPCERT has also considered emergent approaches to enhance the assurance provided by certifications, such as penetration testing and continuous auditing even if this not widely adopted in practice. The complexity from such a hybrid approach, whilst admittedly limited to substantial or high levels, will represent a challenge for all service providers.

Of the methodologies identified by CSPCERT, DIGITALEUROPE agrees that the most pragmatic form of assurance would be an approach using ISO 17021 or ISAE 3401. These approaches to conformity assessments are internationally recognised and accepted by service providers, as they are already used to provide assurance for their customers' own financial reporting.

From an academic perspective, ISO 17021 and ISAE 3402 can complement each other well, with one focusing on an organisation's governance structures

[6] The conformity assessment methodology used for the issuance of management system certifications, such as ISO 27001.

(essentially the design of the controls) and the latter focusing on control effectiveness. Such integration requires a high degree of maturity,[7] where controls are quantitatively managed and optimised by the service provider. This is something that takes years to achieve for any organisation, with significant investment in business process efficiencies and automation. It should also be noted that there are a limited number of firms that meet the competency requirements for both ISO 17021 and ISAE3402.[8] The use of such firms may also be cost prohibitive for some SMEs.

While CSPCERT makes interesting observations, DIGITALEUROPE suggests that ENISA considers these in the context of other potential non-cloud schemes, as consistency between all schemes will help reduce burden on national cybersecurity certification authorities, conformity assessment bodies and providers of multiple types of ICT products and services.

CSPCERT has admirably considered emergent approaches to enhance the assurance provided by certifications, such as continuous auditing and penetration testing.

Regarding continuous auditing, CSPCERT acknowledged that '[t]he use of continuous auditing approaches in the certification landscape is relatively new and not yet mature.'[9] DIGITALEUROPE fully agrees with this statement, which reflects a number of issues with the concept, including: establishing repeatable metrics of performance; secure transfer mechanism; amendments to service agreements; and enough resources within national cybersecurity certification authorities to provide oversight. These issues need to be further investigated and overcome by ENISA before continuous auditing is implemented as an appropriate form for establishing assurance.

Furthermore, the concept of establishing repeatable metrics, if too prescriptive and not based on international standards, would potentially threaten technological innovation. DIGITALEUROPE believes that this would not be in accordance with the principles of the Cybersecurity Act.[10]

---

7 The Capability Maturity Model is a useful mechanism to demonstrate the degree of formality and optimisation of processes, from ad hoc practices to formally defined steps, to managed result metrics, to active optimisation of the processes.

8 This requires a firm that is both a chartered public accountant and a firm that is also accredited to issue ISO 27001 certificates.

9 P. 53 of the Milestone 3 document.

10 See notably Recital 95: 'The design of the European cybersecurity certification schemes should take into account and allow for the development of innovations in the field of cybersecurity.'

Regarding using penetration tests for further assurance, DIGITALEUROPE agrees with the constraints recommended by CSPCERT[11] and further notes that penetration testing, if not controlled correctly in a way that understands the specific nature of cloud services, can cause a significant amount of damage and misleading results.

Most significantly, a high degree of trust is required from a relatively small number of firms engaged in penetration testing. We have a significant concern about a relatively small number of firms aggregating vulnerability data and identifying potential compromise paths for many cloud providers. Such information is extremely valuable, and these firms could find themselves targeted by threat actors to then be able to exploit the services that they have assessed. We recommended ENISA to consider this issue and propose how to mitigate the problem.

Data localisation

DIGITALEUROPE does not believe that the requirements associated with any of the three assurance levels should include data localisation. In particular, given the strict application of data localisation under SecNumCloud, we do not believe that it is appropriate to directly copy those requirements across to the 'high' assurance level in a proposed EU scheme. The concern here is that for most SaaS offerings, keeping all the data within Europe's borders is an unrealistic prospect and comes at the price of significant functionality and service loss. Furthermore, any personal data that leaves the EU's borders should be compliant with GDPR, which established transfer mechanisms that ensure an equivalent level of data protection.

Including localisation requirements in the proposed scheme will also hinder the expansion of EU companies' businesses outside of the EU. To maintain the quality and reliability of their operations, EU companies should be able to use cloud services with the same level of assurance as in the EU, no matter where they operate. It is therefore necessary that the benefit of EU-wide schemes can be 'exportable' by allowing cloud services provided from outside of the EU to be certified against EU schemes, without any localisation criteria. This is something that already exists with EU compliance mechanisms such as CE marking, which has demonstrated over the years its efficiency to protect EU consumers. Similarly to CE marking, the proposed EU scheme should allow providers to claim compliance of their cloud services with the EU cloud computing scheme regardless of where they operate.

Conclusion

DIGITALEUROPE agrees with CSPCERT that the current state, with over twenty requirements throughout the EU's internal market that cloud service providers must

[11] See Section 4.5 of 'CSPCERT WG (Milestone 3) Recommendations for the implementation of the CSP Certification scheme'.

comply with, is inefficient and costly. The work that CSPCERT has done provides a useful starting point for harmonising cloud certification schemes within the EU's internal market. A significant benefit of these recommendations is that it highlights existing international standards as a baseline for a new scheme. This conclusion should be taken further – existing international standards need to be fully leveraged and any additions or changes to international standards must be harmonised both at European and international level.

As a steppingstone to a full scheme, mutual recognition needs to be established between existing cloud security schemes. In addition, there are several enhancements that are required to improve the suitability and effectiveness of CSPCERT's recommendations. For example, ENISA should undertake a thorough risk assessment to determine the appropriate assurance level for users and avoid a scenario where the scheme is deemed inapplicable for a significant portion of higher-risk user communities. From that, the most appropriate form of conformity assessment will be able to be identified. We also urge the European Commission to be very clear on the scope of any scheme it requests ENISA to prepare, which should be based on risk profiles.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Senior Policy Manager for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK