EUROSMART

The Voice of the Digital Security Industry

EUCS

European Cybersecurity certification scheme for Cloud Services and compatibility with EU regulations – what is missing?

Table of Contents

Executive summary

EUCS last draft version (V1.0.413 | March 2024) from ENISA is today on hold for multiple reasons and no feedback is provided about a "High+" level, apparently no more included in the latest draft version.[see strengthening-cloud-security-and-safeguarding-digital-autonomy]
A EUCS level "High+" is missing to support **compatibility** of existing European regulations (GDPR, Data Act, NIS2) and the need to establish, by a European certification, sovereign usage of cloud infrastructures.

TS18026 technical standard - Three-level approach for a set of cybersecurity requirements for cloud services – has been written to provide security organizational and technical requirements for cloud services. It is supposed to be used as a technical backbone of the EUCS document. Thus we will mention below very interesting requirements in the TS18026 which can support the definition of a EUCS "high+" along with appropriate scope of usage for a better adequacy with EU regulations

Glossary of Acronyms

- **ANSSI** – Agence Nationale de la Sécurité des Systèmes d'Information (French National Cybersecurity Agency)
- **BSI** – Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, Germany)
- **CAB** – Conformity Assessment Body
- **C5** – Cloud Computing Compliance Criteria Catalogue (Germany)
- **CSP** – Cloud Service Provider
- **CSC** – Cloud Service Customer
- **CSA** – Cybersecurity Act (Regulation (EU) 2019/881)
- **ENISA** – European Union Agency for Cybersecurity
- **EUCS** – European Cybersecurity Certification Scheme for Cloud Services
- **GDPR** – General Data Protection Regulation (Regulation (EU) 2016/679)
- **HR** – Human Resources (prefix for related controls in TS18026)
- **IAM** – Identity and Access Management
- **IM** – Incident Management (prefix for related controls)
- **ISP** – Information Security Policy
- **IT** – Information Technology
- **NCCA** – National Cybersecurity Certification Authority
- **NIS2** – Directive on measures for a high common level of cybersecurity across the Union (Directive (EU) 2022/2555)
- **OPS** – Operations (prefix for controls related to cloud operations in TS18026)
- **PI** – Processing Interfaces (related to technical requirements in TS18026)
- **PM** – Policy Management or Performance Monitoring (depending on context)
- **PSS** – Physical Security and Site Requirements
- **TS18026** – CENELEC Technical Specification 18026:2024 – Cybersecurity Requirements for Cloud Services
- **WTO** – World Trade Organization

Facts & Elements

Current draft "High" Level EUCS from draft version is not enough for Confidentiality, Integrity, Availability and Accountability over data & business protection for digital sovereignty if we consider the utmost importance of:

- Protecting personal and business sensitive data
  - Data location
  - Applicable scope of European laws and regulations without compromise
- Ensuring and maintaining continuity and resilience in cloud infrastructures and services over time
  - Trusted circles
  - Confidence and transparency on critical actions and monitoring

The below sections will highlight important traceability, requirements and propose to use CENELEC Technical Specification TS18026-2024 and a precise scope of application to define what could be a EUCS "High+" level.

Protecting personal and business sensitive data

As stated in the EUCS draft, the purpose of the document is not to certify the compliance of a cloud service with any regulation beyond the CSA. In particular, it does not aim to verify compliance with the GDPR regarding the use of personal data in cloud infrastructure.

Nevertheless, the EUCS should aim to ensure compatibility and align, as much as possible, with the requirements of European laws applicable to European data.

As such, the current draft "High" level of EUCS is neither demanding enough nor a strong enabler to effectively support the following key objectives:

- Ensuring personal data is located in Europe—or, if outside Europe, accompanied by a full demonstration of adequate data protection in accordance with the GDPR[1].
- Safeguarding business-related data, especially that of high economic value or essential for operational continuity, as defined under the European Data Act[2].

In this context, to strengthen the EUCS proposal, a **"High+"** level should be introduced, with explicit requirements that clearly address these objectives.

[1] Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR), establishes rigorous guidelines for transferring personal data outside the European Union. It ensures that any country or organization receiving the data upholds a sufficient level of protection. To transfer personal data to non-EU countries, organizations are required to implement approved transfer mechanisms. These include Binding Corporate Rules (Articles 46-47), Standard Contractual Clauses (Article 46), ensuring the receiving country has an adequacy decision from the European Commission (Article 45), or obtaining the explicit consent of the data subject (Article 49). These provisions are designed to ensure that data protection accompanies the data, thus maintaining the privacy rights safeguarded by the GDPR, regardless of the data processing location.

[2] European Data Act (Regulation (EU) 2023/2854): aims to regulate and facilitate the sharing and use of data, particularly non-personal data and mixed datasets that include both personal and non-personal data. The Data Act addresses several key areas: Data Sharing B2B and B2C, **Fairness in Data Usage, Data Access by Public Sector Bodies,** Data Switching and Interoperability, Safeguards for Personal Data with respect to GDPR.

→ Data Location

For Availability protection, data location (storage at rest, processing and in transit) should be required to be European.

- TS18026
  - PSS-04.1 - Choice of Locations for Data Processing and Storage [PSS-04.1H & PSS-04.2H],
  - DOC-02.xH - DOC-02 Locations of Data Processing and Storage).

Coverage in EUCS level	Current draft “High” Level from EUCS –March 2024	“High+” Level in a `future revised version
Objective Purpose		
Data Location	As such, the EUCS does not enforce restrictions on geographical location of data or processing, or on applicable laws; however, it requires the CSP to be transparent about this information at all evaluation levels, and to make it publicly available and understandable as part of the information provided with the certificate	Business data (for sensitive sectors and industry) and Personal data should be ensured **to be stored and processed in European location.** With this prerequisite High+ should rely on strict application of TS18026 requirements: DOC-02 PSS-04 [PSS-04.1H & PSS-04.2H]

→ Applicable scope of European laws and regulations without compromise

For Accountability protection, the scope of applicable laws and regulations applicable should be required to be European to ensure EUCS compatibility with GDPR, NIS2, Data Act …

To meet this objective the below reference from TS18026 could be enforced:

- **TS18026**
  - CO-01.4H - Identification of Applicable Compliance Requirements [Proactive and up to date]
  - ISP-02 Topic-Specific Policies and Procedures [ISP-02.2H]
  - PM-04 Monitoring of Compliance with Requirements [PM-04.8H & PM- 04.9H]

Coverage in EUCS level	Current draft “High” Level from EUCS –March 2024	“High+” Level in a `future revised version
Objective Purpose		
Non-negotiable scope of European laws and regulations	**CO-05 Primacy of EU law** without link to compliance requirements from TS18026 for implementation guidance CO-05.1H “ All contracts between the CSPs and the CSCs related to the provision of the cloud service shall only be governed	At minimum, the mention that compliance to European laws and regulations **supersede** any others extra European laws and regulations (like GDPR and Data act) With this prerequisite High+ should rely on strict

	and construed by the law of an EU Member State " Not clear statements or requirements for enforced protection against Extra-territorial laws. CO-05 Automation of Compliance Monitoring [PM-04.8H & PM-04.9H] [CO-03.4H & CO-3.5H]	application of TS18026 requirements [CO-01.4H] [ISP-02.2H] [PM-04.8H] [PM-04.9H]

In summary, the analysis above demonstrates that the current EUCS "High" level falls short in addressing key **European** security concerns. It is therefore justified to introduce an additional "High+" level that more effectively ensures alignment with European data protection regulations and guarantees the robust application of **EU laws**.

Ensure and maintain continuity and resilience in cloud infrastructures and services over time for European businesses and operational resilience.

Sensitive and/or critical data protection is one thing, but associated cloud infrastructure should also ensure business and operation resilience within Europe. As such European companies should take benefits from the EUCS certification scheme and in particular European essential and important entities as defined in NIS2 directive (EU 2022/2555).
As such the Current draft "High" level of EUCS is not demanding enough and not enough a strong enabler to cover the main objectives of:

- Protecting essential and important entities in a trustworthiness ecosystem.
- Ensuring resilience by limiting to Europe and monitoring critical/sensitive actions.

This means the current EUCS have to align and facilitate the application of this directive and provide strong enablers into a "High+" level to ensure:

→ *Trusted circles*

For confidentiality and accountability protection - Trusted circle of actors on cloud infrastructures should be defined and approved by European stakeholders

- **TS18026**
  - Trusted employees (CSP & CSC):
    - It is preferred to be assign to an European employee to avoid any legal, social or extra European threats.
    - HR-01.xH Human Resource Policies and HR-06.xH Confidentiality Agreements and HR-02 Verification of Competence and Trustworthiness [HR-02.1H], HR-02.5H - Verification of Competence and Trustworthiness

- Trusted network:
  - Monitoring of Connections within the CSP’s Network [CS-03.1H & CS-03.2H],
  - Documentation and Security of Input and Output Interfaces [PI-01.4H & PI-01.5H]
- Trusted evaluation or assistance:
  - Obtaining the EUCS certification will require evaluations from accredited CABs following directives based on TS18072. And this should be completed by additional requirements to ensure that any security evaluation over time on the cloud infrastructures will rely on authorized trusted evaluators (by CABs or by NCCA National Cybersecurity Certification Agencies or other European approved security agencies)
- Trusted “high-privilege” roles:
  - IM-06 Evaluation and Learning Process [IM-06.2H],
  - Logging and Monitoring – Policies [OPS-10.2H]
- Trusted supply chain:
  - DEV-02 Development Supply Chain Security [Dev-02.3H]

Coverage in EUCS level	Current draft “High” Level from EUCS –March 2024	“High+” Level in a `future revised version
Objective Purpose		
Trusted cicles	Nothing on Trustworthiness of CSPs, CSCs or suppliers only a chapter on accredited CABs (§7 SPECIFIC REQUIREMENTS APPLICABLE TO A CAB, “the evaluation level CS-High, no specific accreditation is required to perform evaluation activities related to vulnerability identification and penetration testing. Nevertheless, personnel performing inspection activities shall have the necessary expertise to determine the cloud service’s resistance against specific attacks (penetration testing) by an attacker with significant skills and resources on the operation of the cloud service.”)	CSPs legal status and CSPs employees’ trustworthiness assessment should guarantee protection from extra-territorial laws (like US cloud-act). All critical actions should be possible by approved administrators over a trusted network. External parties (suppliers, auditors) should also be accredited or certified to be of trust. With this prerequisite High+ should rely on strict application of TS18026 requirements [HR-01.xH] [HR-02.1H][[CS-03.1H & CS-03.2H] [PI-01.4H & PI-01.5H] [IM-06.2H] [Dev-02.3H] [OPS-10.2H]

→ *Confidence and transparency on critical actions and monitoring*

For Confidentiality and integrity protection a strict Confidence in critical actions and monitoring for high privileged profiles is established by trusted stakeholders

To meet this objective the below reference from TS18026 could be enforced:

- **TS18026**
  - ISP-02 Topic-Specific Policies and Procedures [ISP-02.5H]
  - OIS-02 Segregation of Duties [OIS-02.3H, 02.4H, OIS-02.5-H, OIS-02.6H]
  - IAM-09 General Access Restrictions [IAM-09-7H, 09.8H,IAM-09.9H, IAM- 09.10H]

Coverage in EUCS level	Current draft “High” Level from EUCS –March 2024	“High+” Level in a `future revised version
Objective Purpose		
Tranparency on critical actions and monitoring	CO-05 Automation of Compliance Monitoring with OIS-2.6H	High privilege access or administration actions on the cloud infrastructure should be registered, confirmed by trusted employees with proper roles. Transparency and strict exception/noncompliance register should exist. Ensure that high privileged actions are approved by a trusted employee. Enforce audit by policies on permanent basis and that it exists ability to monitor access to sensitive / valuable data or cloud infrastructure. With this prerequisite High+ should rely on strict application of TS18026 requirements [ISP-02.5H] [OIS-02.3H, [OIS-02.4H, OIS-02.5-H, OIS-02.6H] [IAM-09-7H, 09.8H] [IAM-09.9H, IAM-09.10H]

In summary from the above points, we can compare what the current EUCS “High” Level is proposing and fairly conclude that an additional “High+” Level is needed which clearly meets **European** security risks prevention by clearly establishing a European **trust circle** and protect/monitor **any critical actions and controls** on cloud infrastructure. This is needed in order to override threats scenario from external European interests (geopolitical, legal or business).

Existing schemes from NCCAs (SecNumCloud (FR), C5 (DE))

National Cybersecurity Certification Agencies (NCCA) have already expressed the need for a verified and strict trust into cloud digital partners in charge of protecting their national valuable elements (business, data) for specific sectors. **These National schemes are deemed to disappear “as-is” once EUCS is officially approved**.

Main requirements highlighted above for a EUCS high+ requirements, are already covered or mentioned by existing NCCA cloud conformity schemes (German and French).

Objectives of a “high+” **NCCA cloud certification scheme and**	Data location	Applicable scope of European laws and regulations without compromise	Trusted circles	Confidence and transparence on critical actions and monitoring
German BSI C5-2020 Cloud Computing Compliance Criteria Catalogue – C5:2020	PSS-12 Locations of Data Processing and Storage	BC-01 - Information on jurisdiction and locations COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements	COS-06 Documentation of the network topology HR-01 Verification of qualification and trustworthiness COS-02 Security requirements for connections in the Cloud Service Provider's network	OIS-04 Separation of duties OPS-24 Separation of Datasets in the Cloud Infrastructure COS-05 Network s for administration IDM-06 Privileged access rights COS-03 Monitoring of connections in the Cloud Service Provider's network OPS-12 Logging and Monitoring – Access, Storage and Deletion PI-03 Secure deletion of data

French ANSSI SecNumCloud V3.2 -2020	19.2 - Data location 19.5 - Personal Data protection	19.6 - Measures of protection against European extra territorial laws	19.4 - Contract end / termination	9.6 – Access to administration interfaces 9.7 - Restriction of access to information 6.2 - Segregation of tasks 12.13 – remote actionson infrastructure components

Even if the Current draft “High” EUCS is stating having use inspiration from the elements from NCCAs for strict protection of highly valuable data and business elements, it seems these NCCAs cloud conformity schemes have not been enough re used.

Ways forward and call for actions

The current EUCS draft candidate scheme, represents a significant step toward harmonizing cloud security certification across Europe. However, it remains insufficient in fully addressing the needs of data protection, and resilience as provided by European regulations and the EU Fondamental rights. The chapter outlined above clearly demonstrates the necessity for an additional **“High+” certification level**, firmly grounded in **European legal, technical, and operational principles**.

To effectively move forward, several aspects should be envisaged:

1. Introduce a Formal “High+” Level within EUCS

“High+” certification level remains necessary in a future revision of the EUCS. This level should provide:

- Clear alignment with GDPR, NIS2, and the Data Act;
- Mandatory **data localization** in the EU or Third countries with equivalent level of protections for sensitive business and personal data based on the GDPR approach.;
- Strict compliance with **European jurisdiction** for legal, contractual, and operational matters.

2. Leverage and Harmonize with Existing National Schemes

The EUCS should not only be inspired by but also directly **reuse and align with key security principles from national schemes** like SecNumCloud (France) and C5 (Germany). These schemes already reflect a high level of trust, transparency, and legal protection that should be upheld at the European level.

3. Operationalize the Concept of Trusted Circles

Certification should ensure that **only verified, trustworthy entities** (whether CSPs, CSCs, or third-party service providers) handle sensitive roles and critical infrastructure. This includes:

- Trust verification of personnel;

- Certified supply chains;
- Network segmentation and secure interfaces;
- Oversight from accredited and approved evaluators.

4. Mandate Comprehensive Monitoring and Governance

To ensure confidence and control, the EUCS must enforce:

- Strict access control and high-privilege role oversight;
- Transparent logging and incident monitoring systems;
- Mandatory segregation of duties and policy-driven governance mechanisms.

5. Ensure Strong Alignment with NIS2 Directive

As shown in the mapping in annex, many TS18026 controls naturally support NIS2 implementation. A revised EUCS should incorporate these elements in a explicit manner to support **essential and important entities** and bolster resilience against systemic cyber risks.

6. Promote Policy and Political Commitment

A strong political mandate is required to **maximize European strategic autonomy** while **reducing external dependencies**, in full respect of WTO rules. The upcoming revision of the CSA, including the European Cybersecurity Certification Framework, should encompass:

- Legal frameworks to safeguard against extraterritorial influence;
- Binding commitments to preserve EU jurisdiction and legal control;
- Strategic incentives for CSPs to pursue **High+** certification.

Appendix on NIS2 compatibility

Defining tomorrow a EUCS "High+" Level as highlighted in above sections would provide compliance requirements to meet some of the NIS2 sections.
The table below as per ENISA implementation draft for compliance to NIS2 (Directive (EU) 2022/2555) (source: Implementation-guidance-on-nis-2-security-measures), summarizes references:

- To requirements using TS18026 requirements,
- And in blue the references also proposed to build a EUCS "High+" level.

Ref.	Title implementation	TS18026 reference
1,1	POLICY ON THE SECURITY OF NETWORK AND 219 INFORMATION SYSTEMS	ISP-01, ISP-02, OPS-01,OPS- 02, OPS-03
1,2	1.2 ROLES, RESPONSIBILITIES AND AUTHORITIES	ISP-02, OIS-02
2,2	COMPLIANCE MONITORING	CO-01, DOC-03, INQ-01,INQ-02, INQ-03
2,3	INDEPENDENT REVIEW OF INFORMATION AND NETWORK SECURITY	CO-01, CO-02, CO-03, CO-04
3,1	INCIDENT HANDLING POLICY	ISP-02, IM-01, IM-07
3,2	MONITORING AND LOGGING	OPS-10, OPS-11, OPS-12,OPS-13, OPS-14, OPS-15, OPS-16, OPS-23, CS-01, IM-07, PSS-01
5,1	SUPPLY CHAIN SECURITY POLICY	ISP-02, DEV-08, PM-01, PM-02, PM-04, PM-05
5,2	DIRECTORY OF SUPPLIERS AND SERVICE PROVIDERS	DEV-02, PM-03
6,1	SECURITY IN ACQUISITION OF ICT SERVICES, ICT SYSTEMS OR ICT PRODUCTS	OIS-04, AM-03, DEV-02,DEV-07, PM-01
6,2	SECURE DEVELOPMENT LIFE CYCLE	OIS-04, CCM-04, CCM-06,DEV-01, DEV-03, DEV-04,DEV-05, DEV-06
6,3	CONFIGURATION MANAGEMENT	OPS-21, PSS-03, PSS-04
6,4	CHANGE MANAGEMENT, REPAIRS AND MAINTENANCE	ISP-03, CCM-01, CCM-02,CCM-03, CCM-04, CCM-05,CCM-06
6,5	SECURITY TESTING	ISP-02, OPS-19, DEV-01,DEV-04, DEV-06
6,7	NETWORK SECURITY	PS-04, CS-01, CS-02, CS-03,CS-06, CS-07, CS-08, PSS-02

6,8	NETWORK SEGMENTATION	IAM-09, CS-02, CS-04, CS-05
6,9	PROTECTION AGAINST MALICIOUS AND UNAUTHORISED SOFTWARE	OPS-04, OPS-05, CS-03
7	POLICIES AND PROCEDURES TO ASSESS THE EFFECTIVENESS OF CYBERSECURITY RISK-MANAGEMENT MEASURES	ISP-02, OPS-20, CO-04
9	CRYPTOGRAPHY	ISP-02, CKM-01, CKM-02,CKM-03, CKM-04
11,1	ACCESS CONTROL POLICY	OIS-02, ISP-02, IAM-01
11,2	MANAGEMENT OF ACCESS RIGHTS	OIS-02, IAM-04, IAM-05,PSS-03, HR-05
11,3	PRIVILEGED ACCOUNTS AND SYSTEM ADMINISTRATION ACCOUNTS	ISP-02, IAM-05, IAM-06
11,4	ADMINISTRATION SYSTEMS	OIS-02, IAM-06, IAM-09
12,2	HANDLING OF ASSETS	ISP-02, AM-02, AM-03
12,3	REMOVABLE MEDIA POLICY	ISP-02, AM-02, PS-04

About us

Eurosmart, the Voice of the Digital Security Industry, is a European non-profit association located in Brussels, representing the Digital Security Industry for multisector applications. Founded in 1995, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com