MEDINA

MEDINA: Standardization to enable continuous cloud cybersecurity certification

Jesus Luna Garcia (Robert Bosch GmbH, Germany)

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 952633

Background

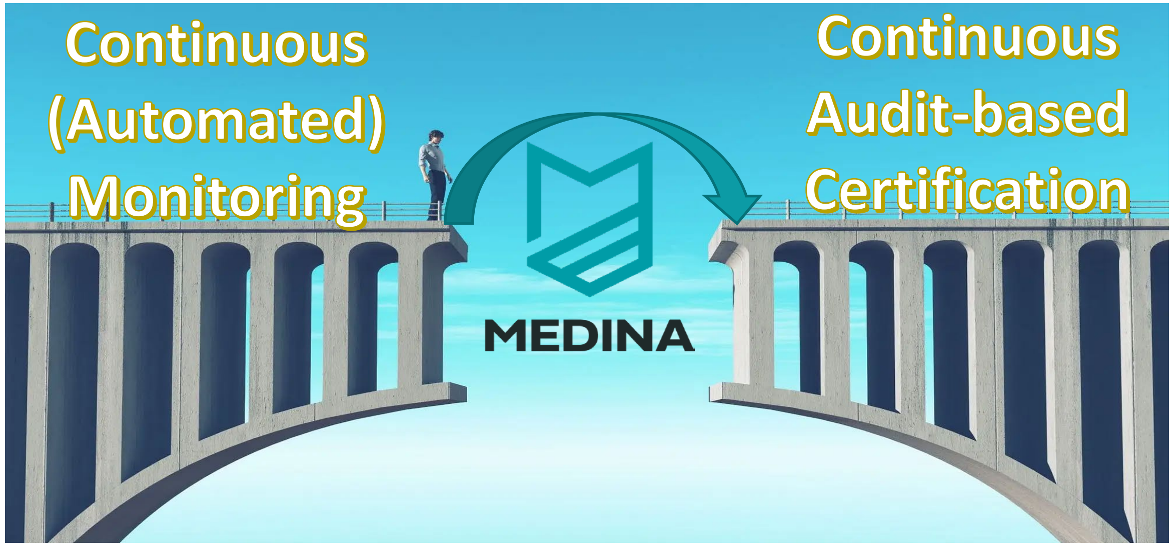
MEDINA

- The EU Cybersecurity Act (EUCSA, April-2019), proposes the creation **EU-wide cybersecurity certification schemes** in order to:
  - provide an ***standards-based*** cybersecurity baseline (requirements, audit methods)
  - ***enable continuous cybersecurity compliance***
- ENISA (EU Cybersecurity Agency) nominated as responsible for developing the new EU-certification schemes:
  - ***EUCS – EU Cybersecurity Certification Scheme for Cloud Services***

MEDINA Mission

Provision of a **security framework and tools** for achieving **continuous audit-based certification** aligned to EUCS.

- MEDINA primarily focuses on the **EUCS requirements**, where some degree of automation is needed.
- **Strong synergies with relevant standards.**


Continuous (Automated) Monitoring
MEDINA
Continuous Audit-based Certification

MEDINA At a Glance

MEDINA

- 1st November 2020 – 30th October 2023
- EU Budget 4,480,308.75€

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

BOSCH

Fraunhofer AISEC

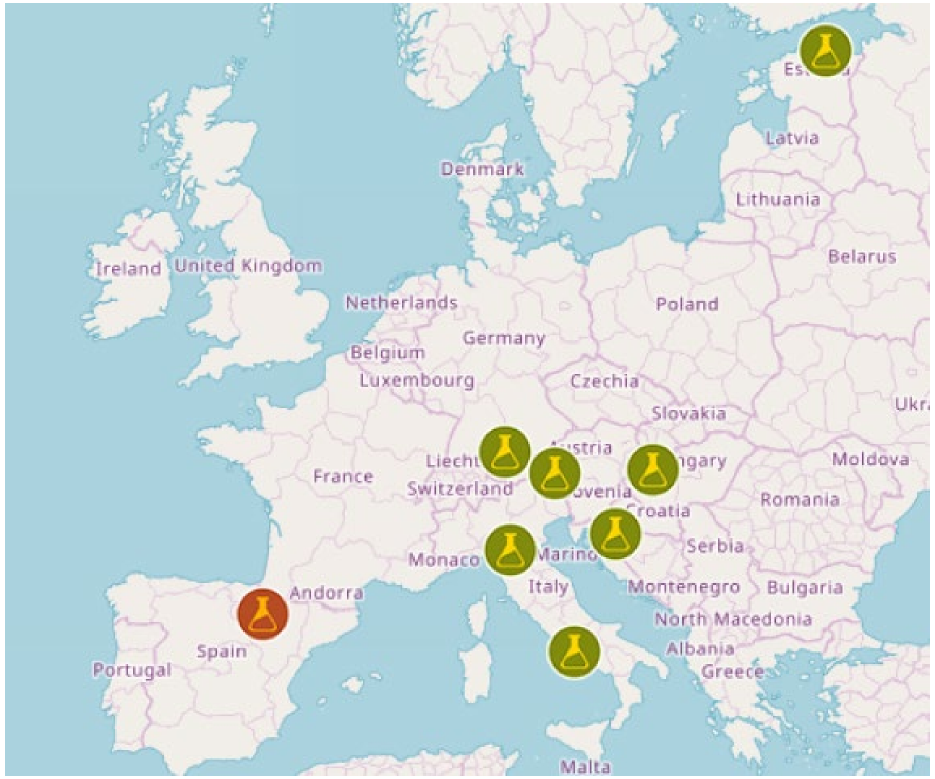
Fabasoft®

Hewlett Packard Enterprise

XLAB

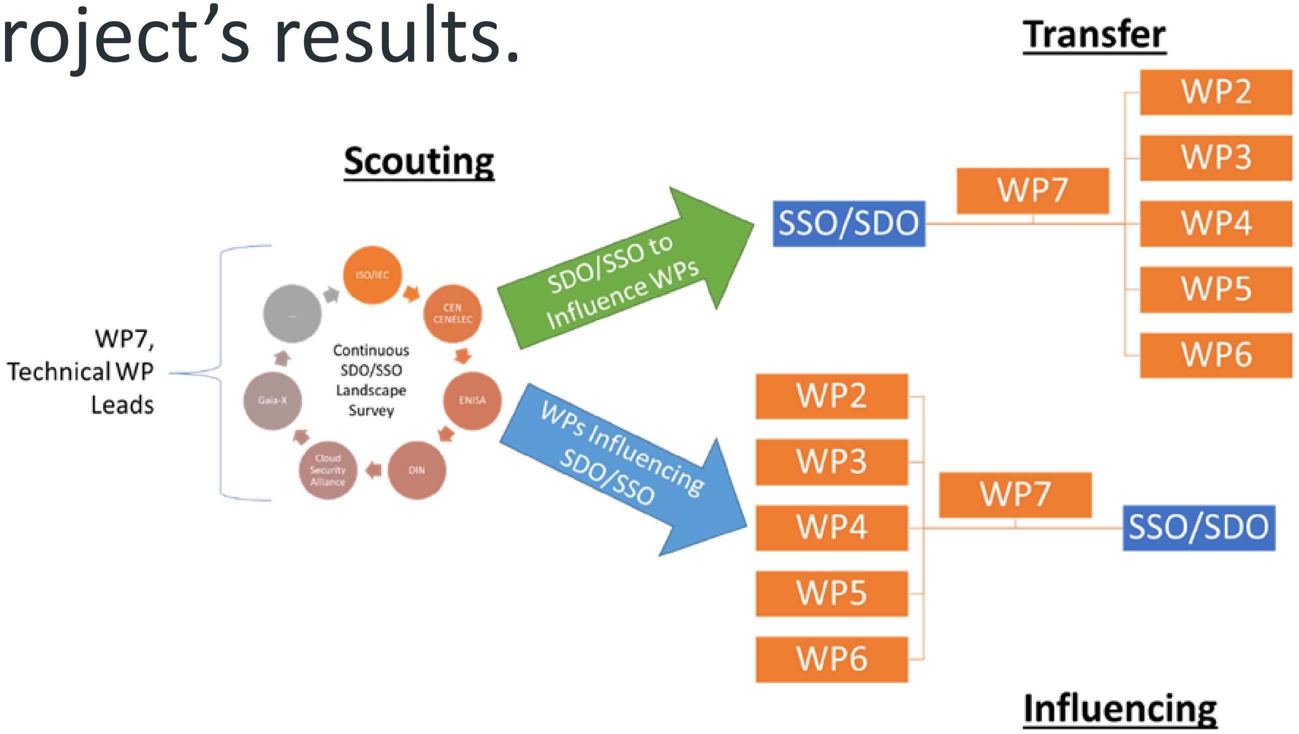
nixu cybersecurity.

Consiglio Nazionale delle Ricerche



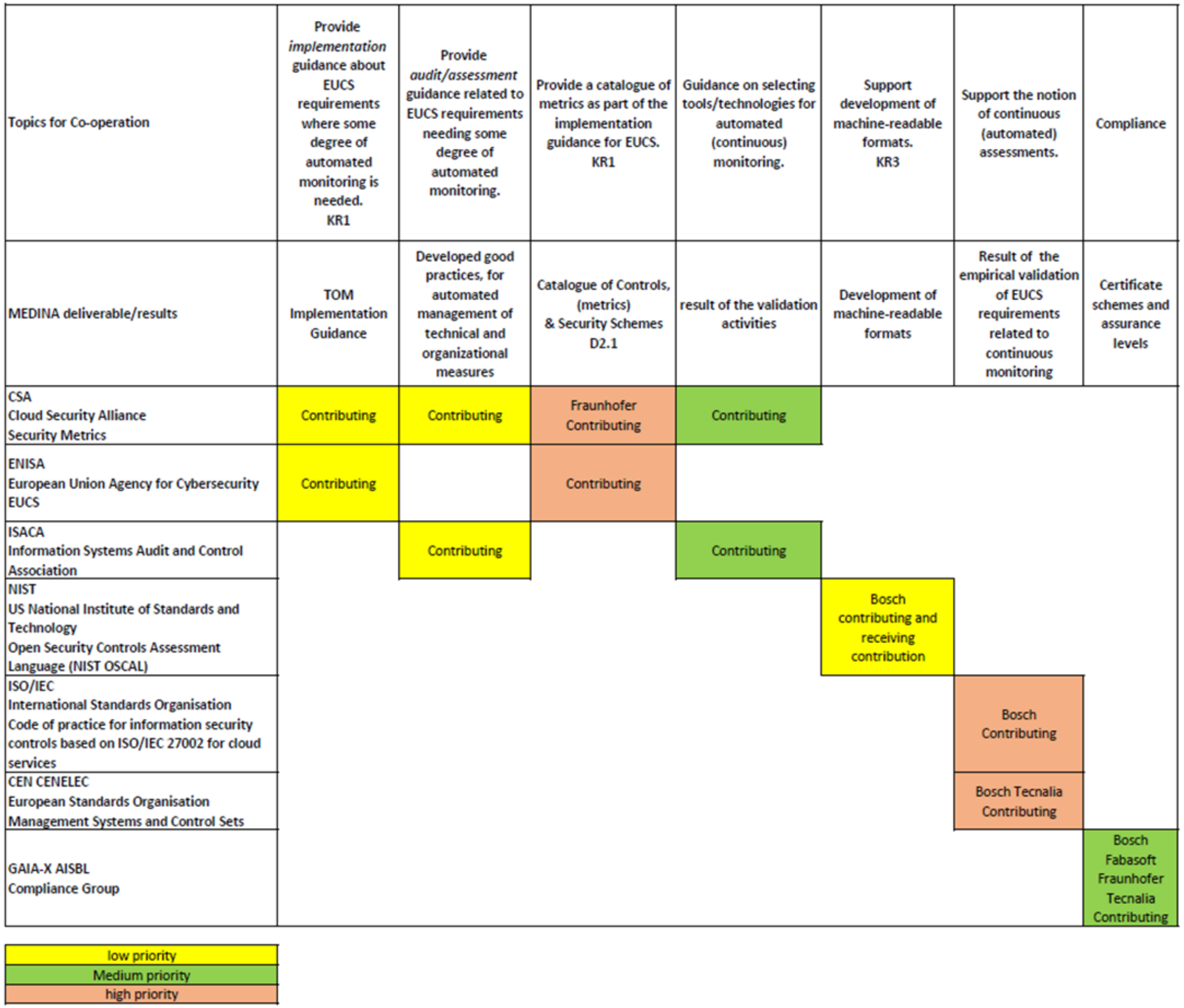
Standardization Objectives in MEDINA

- To ensure that the **relevant SDO communities** will be reached out to in an **interactive way**.
- To address the **future adoption** and ensure the **sustainability** of the project's results.



Standardization Roadmap (M18)

- Prioritizes adoption of **EUCS, metrics, and automation** in compliance assessments.
- **Continuously revised** to integrate new/relevant activities e.g., ETSI CYBER OSCAL.



Topics for Co-operation	Provide *implementation* guidance about EUCS requirements where some degree of automated monitoring is needed. KR1	Provide *audit/assessment* guidance related to EUCS requirements needing some degree of automated monitoring.	Provide a catalogue of metrics as part of the implementation guidance for EUCS. KR1	Guidance on selecting tools/technologies for automated (continuous) monitoring.	Support development of machine-readable formats. KR3	Support the notion of continuous (automated) assessments.	Compliance
MEDINA deliverable/results	TOM Implementation Guidance	Developed good practices, for automated management of technical and organizational measures	Catalogue of Controls, (metrics) & Security Schemes D2.1	result of the validation activities	Development of machine-readable formats	Result of the empirical validation of EUCS requirements related to continuous monitoring	Certificate schemes and assurance levels
CSA Cloud Security Alliance Security Metrics	🟨 Contributing	🟨 Contributing	🟧 Fraunhofer Contributing	🟩 Contributing			
ENISA European Union Agency for Cybersecurity EUCS	🟨 Contributing		🟧 Contributing				
ISACA Information Systems Audit and Control Association		🟨 Contributing		🟩 Contributing			
NIST US National Institute of Standards and Technology Open Security Controls Assessment Language (NIST OSCAL)					🟨 Bosch contributing and receiving contribution		
ISO/IEC International Standards Organisation Code of practice for information security controls based on ISO/IEC 27002 for cloud services						🟧 Bosch Contributing	
CEN CENELEC European Standards Organisation Management Systems and Control Sets						🟧 Bosch Tecnalia Contributing	
GAIA-X AISBL Compliance Group							🟩 Bosch Fabasoft Fraunhofer Tecnalia Contributing

🟨 low priority
🟩 Medium priority
🟧 high priority

D7.8 Standardization Roadmap-v1 (**M18**)

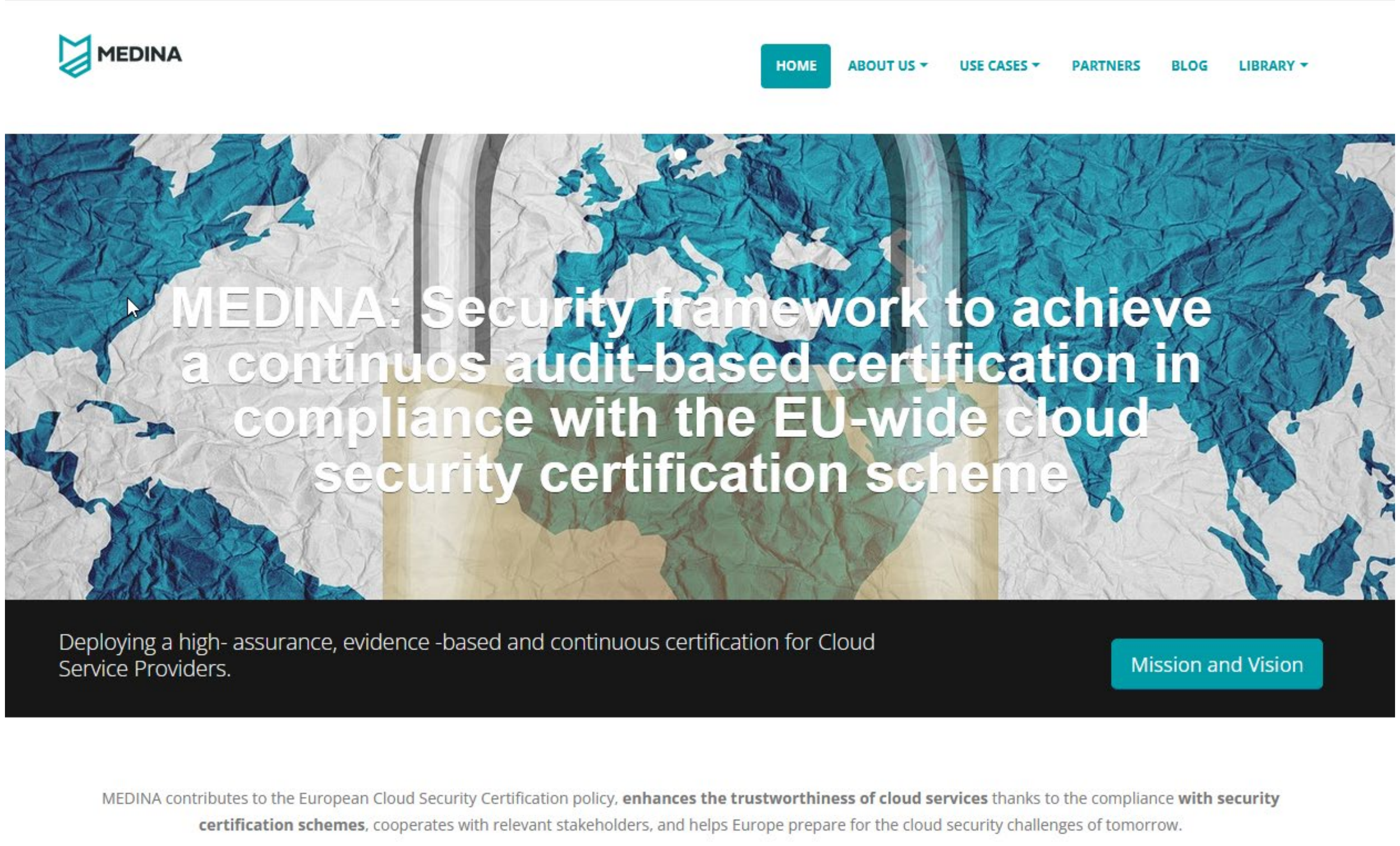
Standardization: (Selected) Achievements and Next Steps

MEDINA

MEDINA Achievements (Feb-2023)	Next Steps (Feb / Oct-2023)
Major support to ENISA on development/uptake of EUCS	Continuous EUCS1 support (CEN CENELEC), contribution to ENISA guidelines for automation
Proof-of-concept NIST OSCAL for EUCS catalogue Feedback to NIST SP 800-55	Representation of metrics/assessments, document experiences in whitepaper.
Adoption of “continuous” for Configuration Management in ISO/IEC 27017	Maintain contribution during upcoming review cycle

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at https://medina-project.eu/public-delivera
- Communication materials are available at https://medina-project.eu/communication-materials



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Thank you!

www.medina-project.eu // jesus.lunagarcia@de.bosch.com