MEDINA

Paving the Road Towards Continuous Certification: OSCAL and the EUCS

Jesus Luna Garcia (Robert Bosch GmbH)

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

Agenda

- Background
  - EU Cybersecurity Scheme for Cloud Services (EUCS)
  - Continuous Monitoring in the EUCS
- EC Funded H2020 MEDINA Project
  - From Continuous Monitoring to Continuous Certification
  - High-Level Approach and Architecture
  - Leveraging OSCAL
- Summary and Next Steps

Background

European Union Cybersecurity Certification Scheme for Cloud Services

What is the EUCS?

- The EU Cybersecurity Act (EUCSA, April-2019), proposes the creation an EU-wide cybersecurity certification framework in order to:
  - increase the use of cybersecurity certification in Europe
  - go beyond national schemes and offer mutual recognition at European level
  - enable customers to make informed decisions about cybersecurity.
- ENISA (EU Agency for Cybersecurity) organized an AdHoc WG to prepare the candidate **Cybersecurity Certification Scheme for Cloud Services (EUCS)**.

What is the EUCS?

MEDINA

- The EUCS defines:
  - rules for the management of certificates,
  - requirements for security controls,
  - levels of assurance, and
  - assessment processes.
- EUCS focuses on certifying **cloud services** (see ISO/IEC 17788), including composition of **sub-services**.
- Security requirements in EUSA are based on standards (e.g., BSI C5, SecNumCloud, ISO/IEC 270xx).

What is the EUCS?

Levels of Assurance

‘basic’ level

Minimise the **known basic** risks of incidents and cyberattacks (**low risk profile**)

- Limited assurance
- Self-assessment reviewed by a third-party
- Focus on the definition and existence of procedures and mechanisms

‘substantial’ level

Minimise **known** cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with **limited skills and resources (medium risk profile)**

- Reasonable assurance
- Design and operating effectiveness
- Functional testing

‘high’ level

Minimise the risk of **state-of-the-art** cyberattacks carried out by actors with **significant skills and resources (elevated risk profile)**

- Reasonable assurance
- Design and operating effectiveness
- **Continuous (automated) monitoring of compliance**

Continuous Monitoring in the EUCS

- Definition of “Continuous (Automated) Monitoring” in the EUCS:

  The requirements related to continuous monitoring typically mention “automated monitoring” or “automatically monitor” in their text. The intended meaning of “monitor automatically” is:

  1. *Gather data to analyse some aspects of the activity being monitored at discrete intervals at a sufficient frequency;*
  2. *Compare the gathered data to a reference or otherwise determine conformity to specified requirements in the EUCS scheme;*
  3. *Report deviations to subject matter experts who can analyse the deviations in a timely manner;*
  4. *If the deviation indicates a nonconformity, then initiate a process for fixing the nonconformity; and*
  5. *If the nonconformity is major, notify the CAB of the issue, analysis, and planned resolution.*

  ***These requirements stop short on requiring any notion of continuous auditing, because technologies have not reached an adequate level of maturity**. Nevertheless, **the introduction of continuous auditing, at least for level High, remains a mid- or long-term objective,** and the introduction of automated monitoring requirement in at least some areas is a first step in that direction, which can be met with the technology available today.*

Only for HIGH Assurance!

Continuous Monitoring in the EUCS

MEDINA

- Examples of “High” assurance requirements, related to “continuous monitoring”

Ref	Description	Ass. Level
OPS-05.1	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures	Basic
OPS-05.2	Signature-based and behaviour-based malware protection tools shall be updated at least daily	Substantial
OPS-05.3	The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of OPS-05.1	High
OPS-05.4	The CSP shall automatically monitor the antimalware scans to track detected malware or irregularities	High

Continuous Monitoring in the EUCS

MEDINA

Ref	Description	Ass. Level
AM-01.1	The CSP shall document and implement policies and procedures for maintaining an inventory of assets	Basic
AM-01.2	The inventory shall be performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset life cycle	Substantial
AM-01.3	The CSP shall record for each asset the information needed to apply the risk management procedure defined in RM-01.	Basic
AM-01.4	The information recorded with assets shall include the measures taken to manage the risks associated to the asset through its life cycle	Substantial
AM-01.5	The information about assets shall be considered by monitoring applications to identify the impact on cloud services and functions in case of events that could lead to a breach of protection objectives, and to support information provided to affected cloud customers in accordance with contractual agreements	High
AM-01.6	The CSP shall automatically monitor the inventory of assets to guarantee it is up-to-date	High

H2020 MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EUCS

Funded by

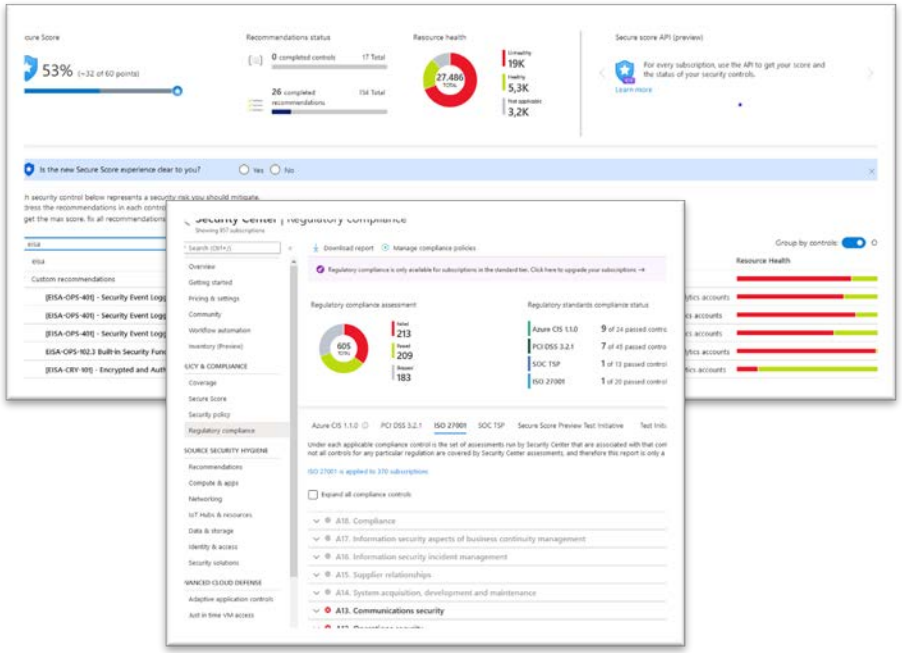
European Commission | Horizon 2020 European Union funding for Research & Innovation

MEDINA Project Objective

Provide a holistic **framework** that enhances cloud customers' control and trust in consumed cloud services, by supporting CSPs (IaaS, PaaS and SaaS providers) towards the **successful achievement of a continuous certification aligned to the EU Cybersecurity Act** (EUCSA).

From Continuous Monitoring to Continuous Certification

TODAY



BOSCH

DevOps

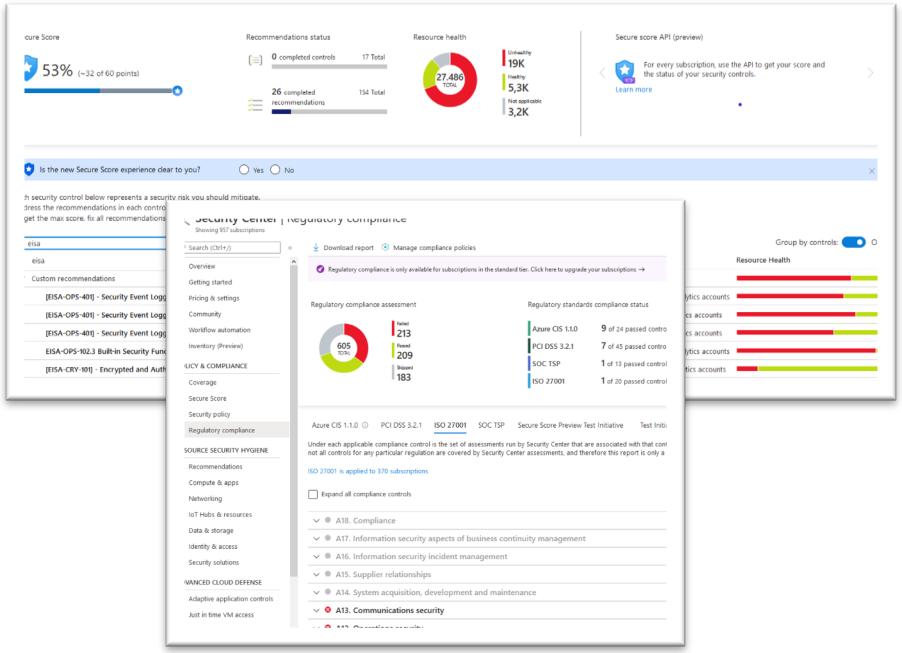
IT Security Governance

Internal Auditors

- Security Posture Management tools provide our internal stakeholders with “continuous” compliance data.
- Bosch-internal deployment (since mid-2019), monitors >28,000 cloud resources for compliance with our internal ISO/IEC 27001-based security control framework.

From Continuous Monitoring to Continuous Certification

TODAY



BOSCH

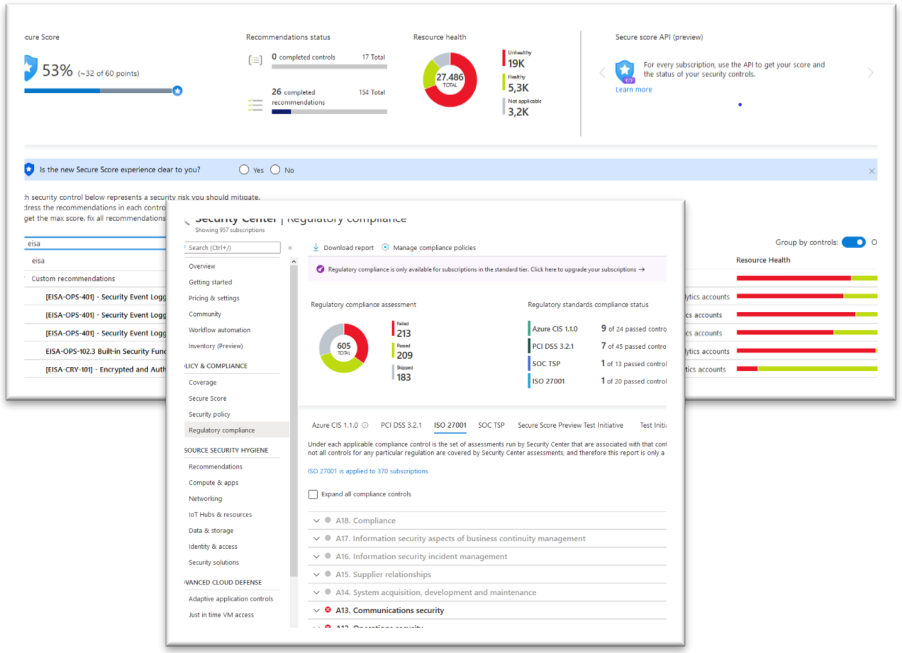
TOMORROW

External Auditor

nixu cybersecurity.

From Continuous Monitoring to Continuous Certification

TODAY



BOSCH

TOMORROW

MEDINA

funded by European Commission — Horizon 2020 European Union funding for Research & Innovation

(EUCS) Certification

ISO · 5 TESTED CLOUD COMPUTING COMPLIANCE CONTROLS CATALOGUE

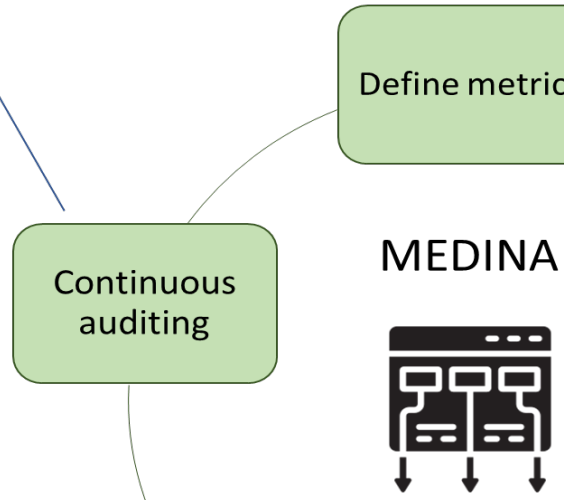
External Auditor

nixu cybersecurity.

MEDINA At a Glance

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

MEDINA Approach



- Technical and Organizational (TOM) measures
- Catalogue of metrics

KR1

- Risk-based approach to select the security controls in accordance to the CSP's risk appetite
- Identify core assets of the service
- Identify threats
- Propose optimal security controls

KR2

- Specify the EU wide cloud certification scheme under the Cybersecurity Act in a machine-readable way (DSL) using NLP
- Define a certification target: the scope of the certification, assurance level, conformity assessment method, and so on

KR3

OSCAL?

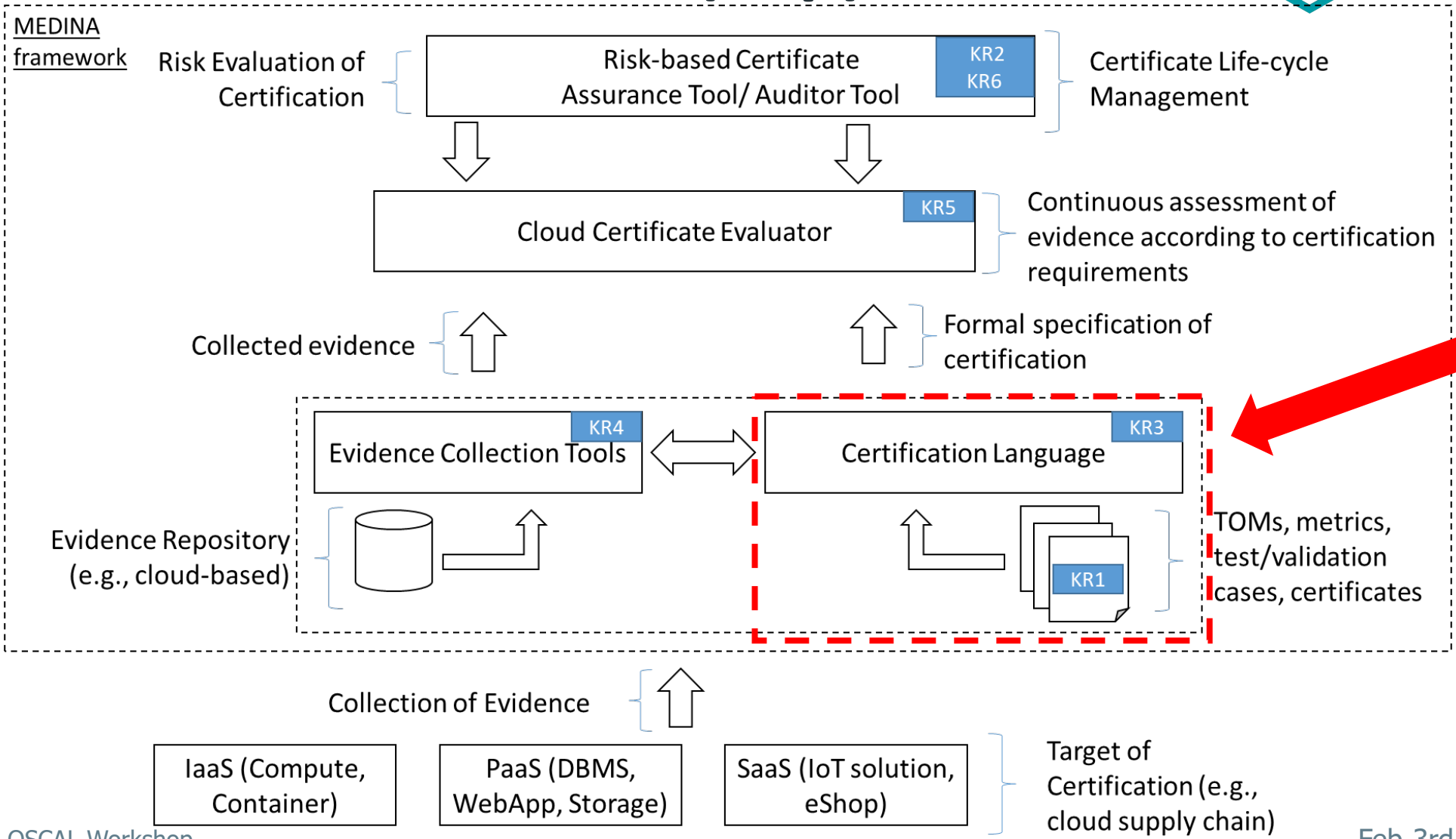
- Methods and tools for the management of cloud security certifications, in accordance to both chosen conformity method and assurance level
- Re-evaluate the risk and the selected security controls based on the continuous feedback loop with the evaluation component
- representation and management of cloud certifications based on smart contracts

KR5, KR6

KR4

- Tools and methodologies to collect evidence at code and service level at design and operation time
- tools and techniques needed to gather and manage cloud evidence's life-cycle
- Integrate these tools in new architectures (e.g. serverless) and paradigms (DevOps, IaC)
- improve the trustworthiness of gathered evidence with e.g. smart contracts

High-Level Architecture (wip)



Leveraging OSCAL (early thoughts)

MEDINA

- Machine-readable representation of security controls (e.g., EUCS, BSI C5).
  - Both for technical and organizational measures.
- Metrics descriptions (relationship with NIST SP 500-307?) for assessing compliance with security controls.
- Machine-readable certificate format.
- Policy-language for managing the certificate‘s life-cycle.
- Support for standardization roadmap and industrial adoption e.g., Gaia-X.

MEDINA

Summary and Next Steps

What comes next?

Summary and Next Steps

- The upcoming EUCS will promote the adoption of continuous compliance monitoring for cloud services in Europe.
- MEDINA seeks to bridge the gap between continuous compliance monitoring, and continuous certification.
- OSCAL seems to be a strong candidate for fulfilling our requirements related to machine-readable formats in MEDINA.
  - Strong interest in OSCAL from other EU cloud initiatives like Gaia-X.
- We are looking forward to a fruiful collaboration with US NIST on the topic of OSCAL!

Thank you!

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