

H2020 Project

MEDINA

Presented by: Bjoern Fanta | Head of Research

For: Fabasoft

05/10/2022



Context: European Cloud Services Certification Scheme (EUCCS)



'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

Context: Continuous Monitoring



EUCS – CLOUD SERVICES SCHEME
December 2020

Continuous monitoring

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.

Further guidance will be provided about acceptable mechanisms and processes.

*“gather,
compare,
report”*



Context: Continuous Monitoring



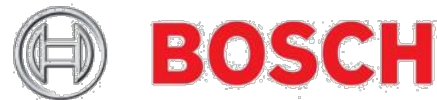
Example - EUCS draft Dec-2020

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

MEDINA at a Glance



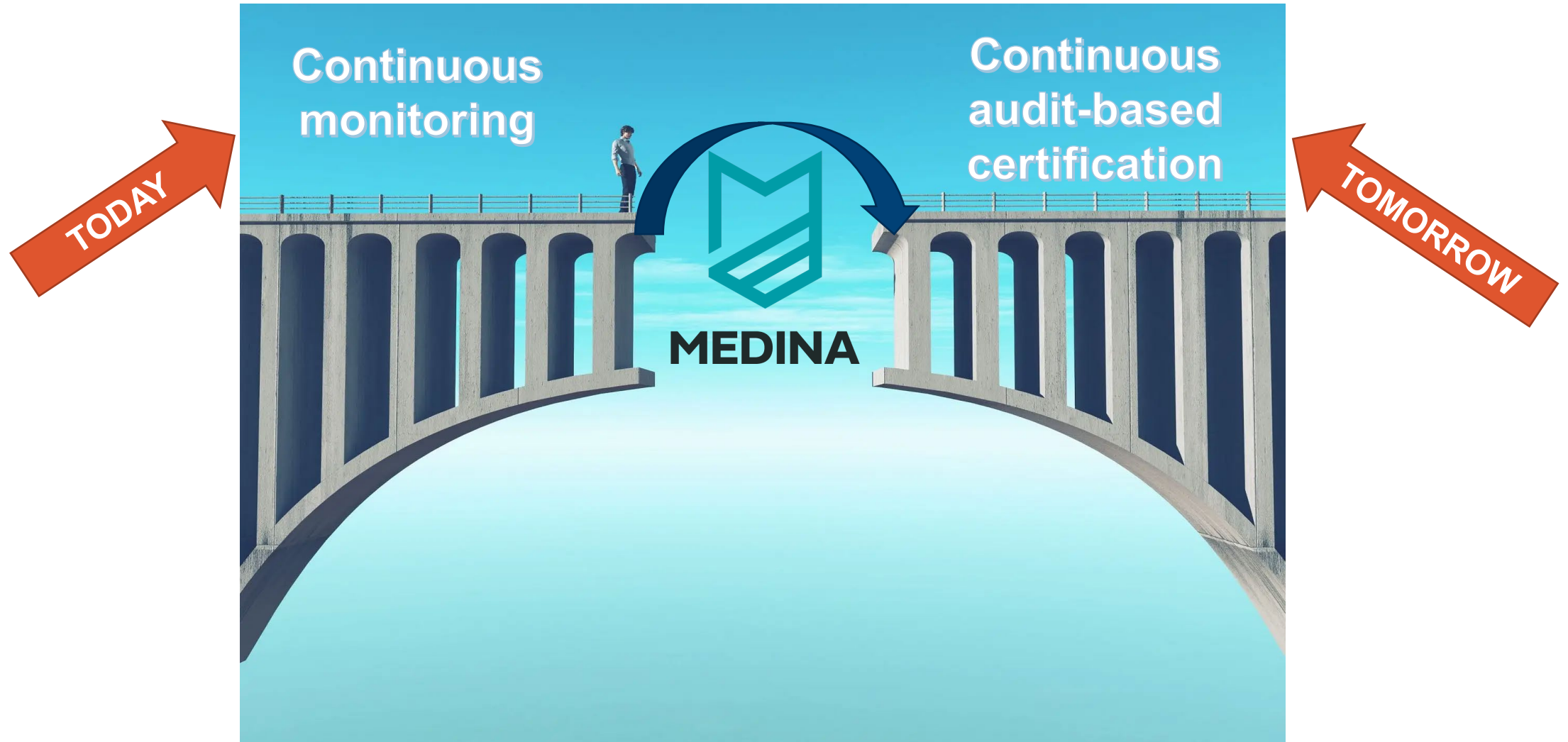
- 1st November 2020 – 30th October 2023
- EU budget 4,480,308€



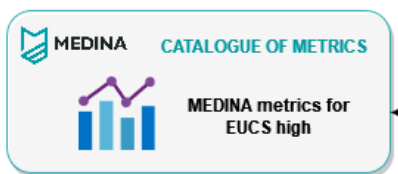
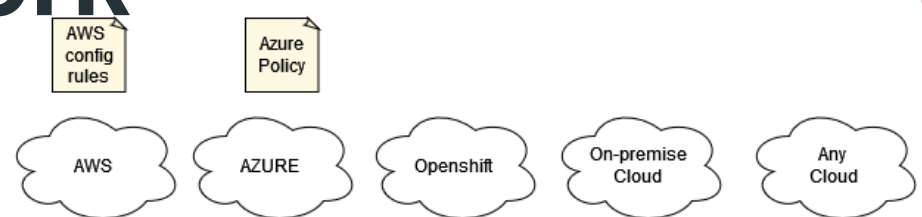
Consiglio Nazionale
delle Ricerche



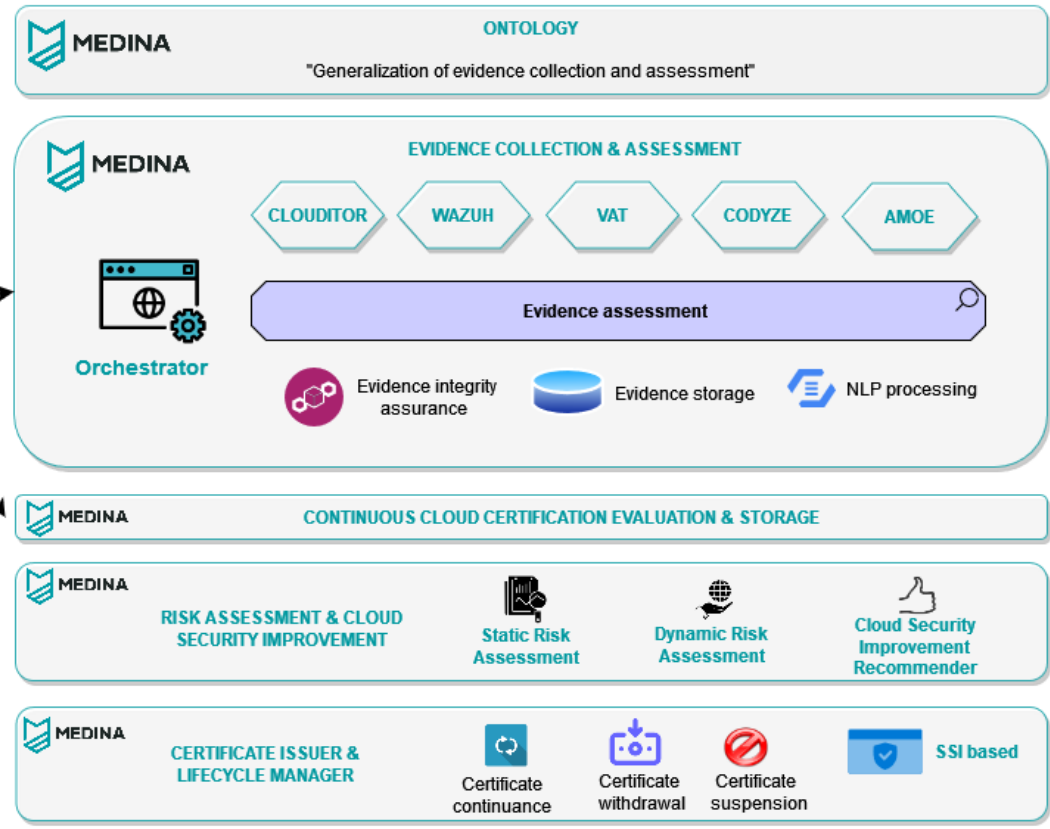
Bridging the Gap



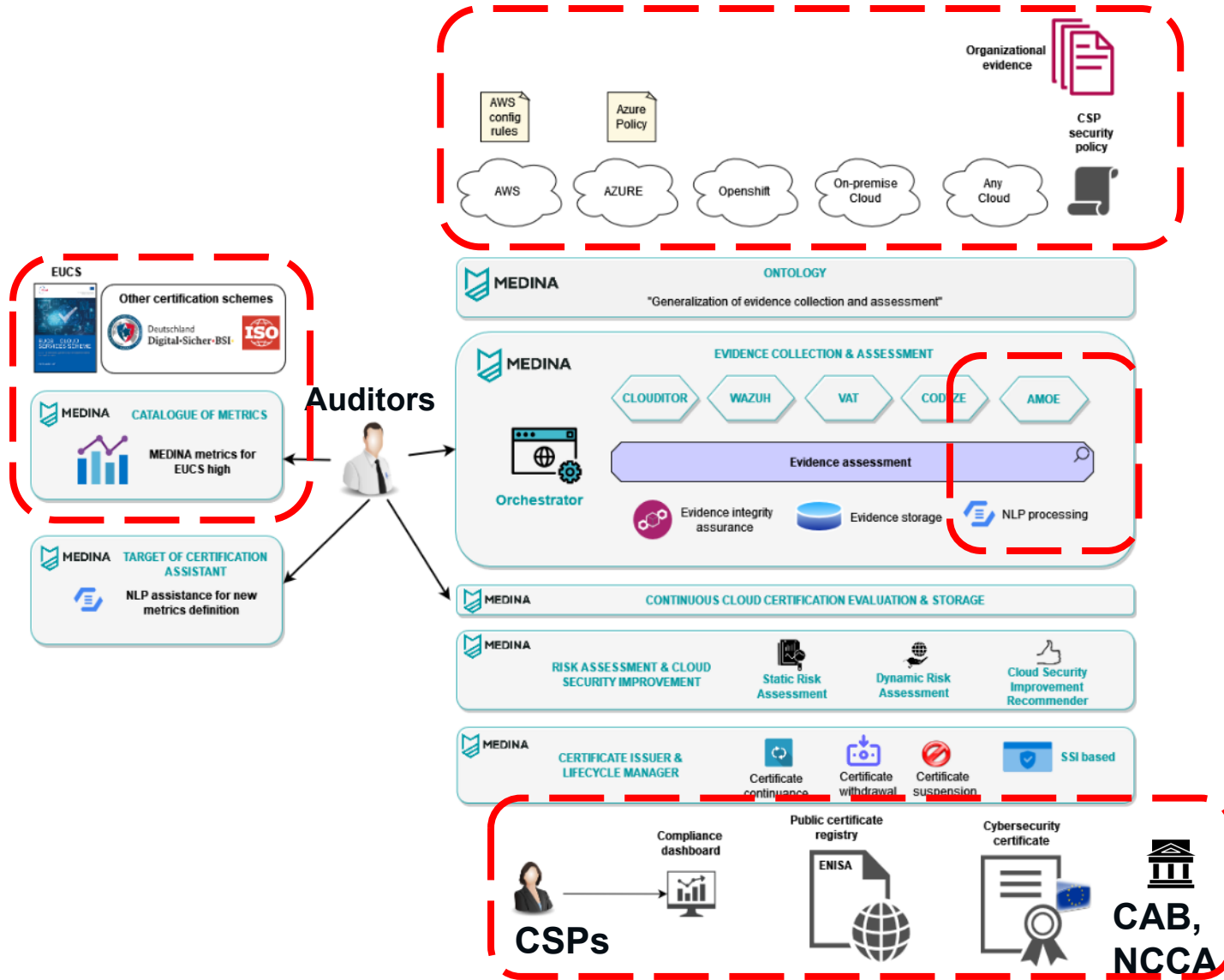
MEDINA Framework



Auditors



Fabasoft's Role



- Use case coordinator
- Integration & validation in **Company Compliance Dashboard (CCD)** & cloud testbeds
- PoC: **NLP enhanced assessment (AMOE)**

>demotable



Information about the file	Filter CAB assessment [?]
Cloud service 813d82df-2d31-4ee1-9ca6-f38137bd1f14	Compliant: 7 / 67
File id 6319a5142a1d444db5d4428e	Not compliant: 0 / 67
File name MEDINA_dummy_policies_Fabasoft_M18v5.pdf	Undefined: 59 / 67
Uploaded on 2022-09-08 08:17:24 by admin	<button>Reset filter</button>
Number of metrics 67 / 67	

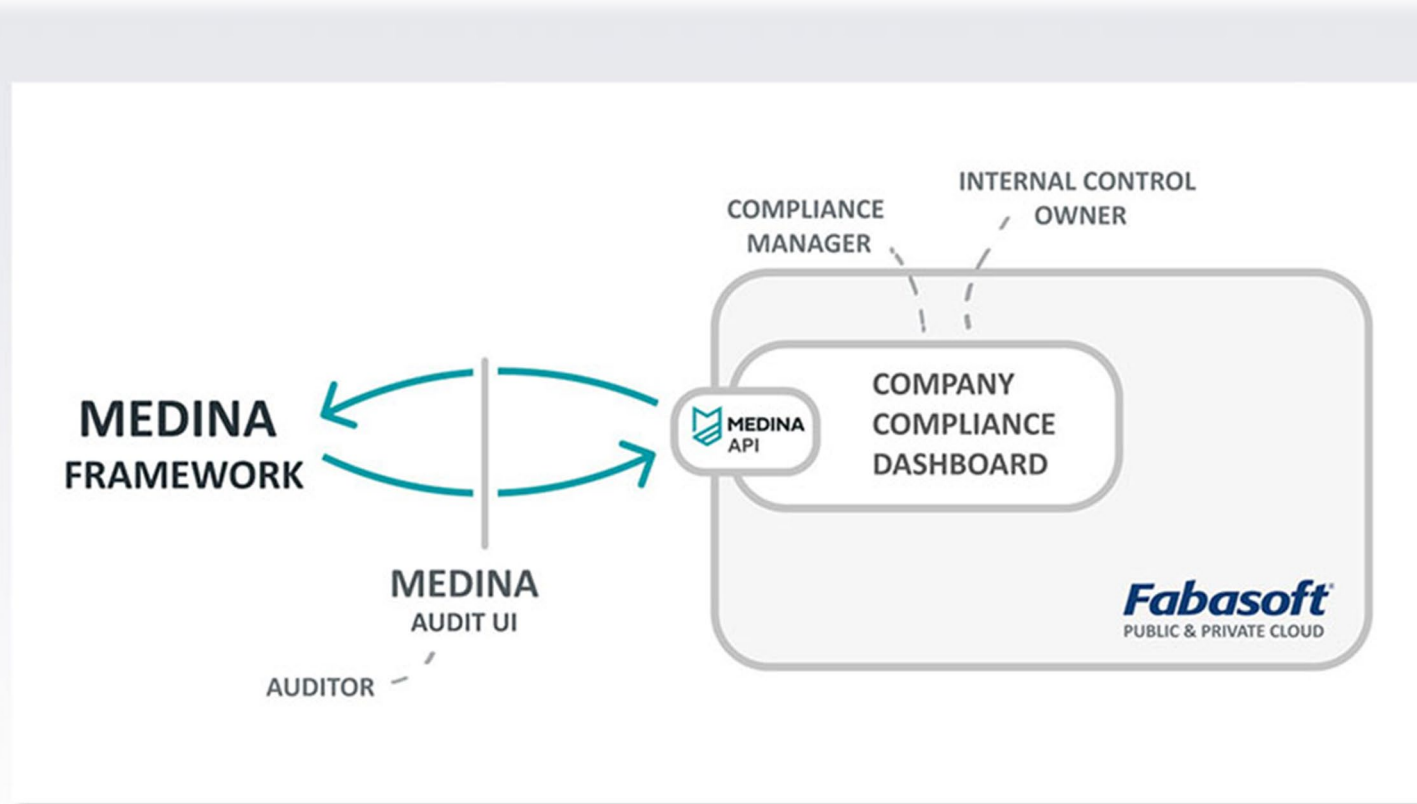
Extracted evidence

Show entries

Search:

MetricID	Question	Answer	AMOE assessment hint [?]	CAB assessment [?]	Submitted to Orchestrator [?]
AntimalwareScanFrequencyQ1	How frequent are antimalware scans done?	each week	× False	✓ True	✓ Submitted
AssetManagementPolicy01	Which asset management policy is defined?	Exact classification rules	Undefined	✓ True	<button>Submit </button>

Fabasoft Use Case



Company Compliance Dashboard - Benefits



Documented guidance on how to perform the checks, what actions to take, and what supporting evidence is required greatly minimizes the overall time commitment.



Comprehensive support regarding continuous compliance with metrics related to the EUCS reduces the labor, cost, and risk involved in achieving and maintaining certification.

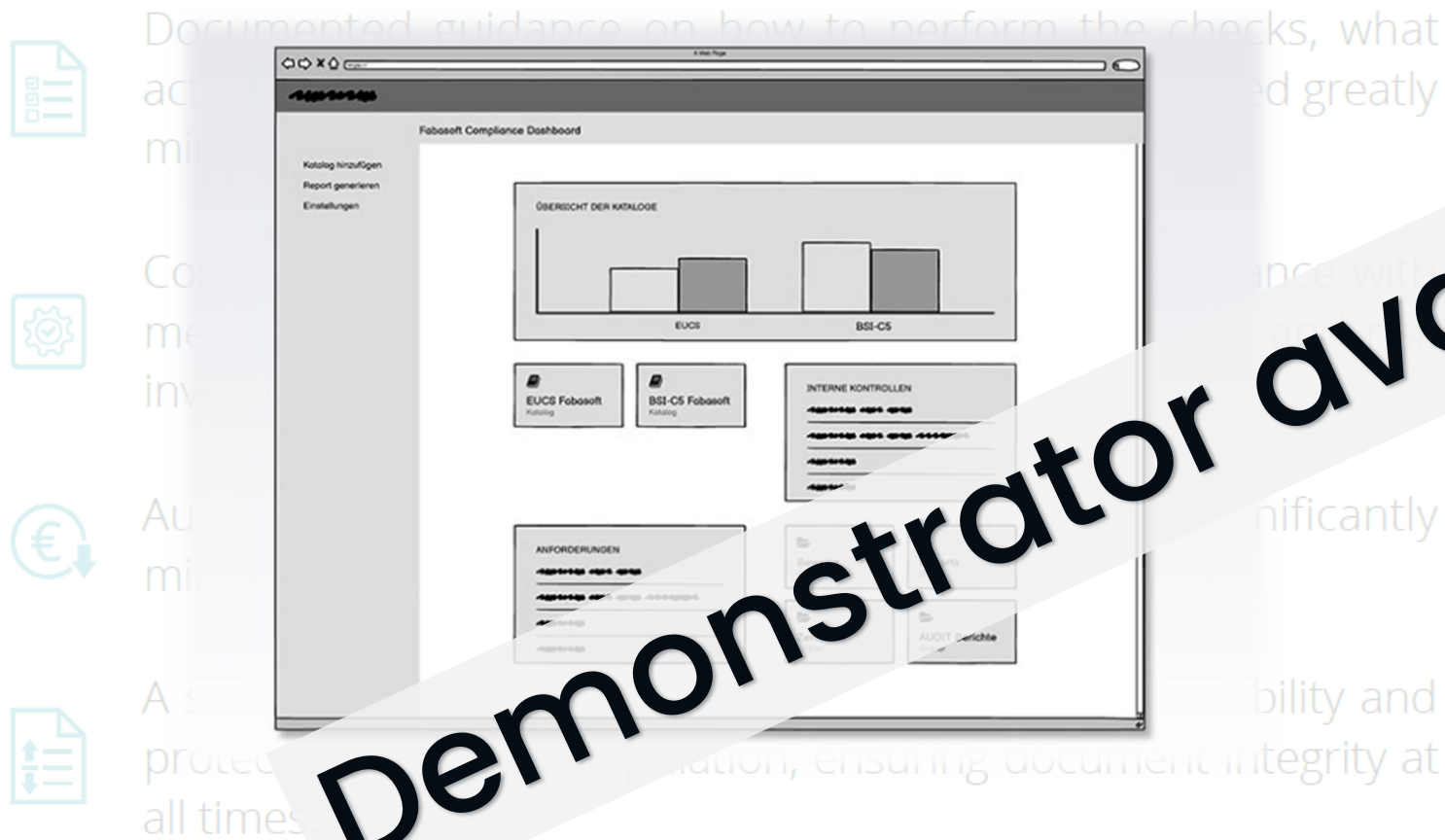


Automatic collection and evaluation of evidence significantly minimizes both workload and costs.

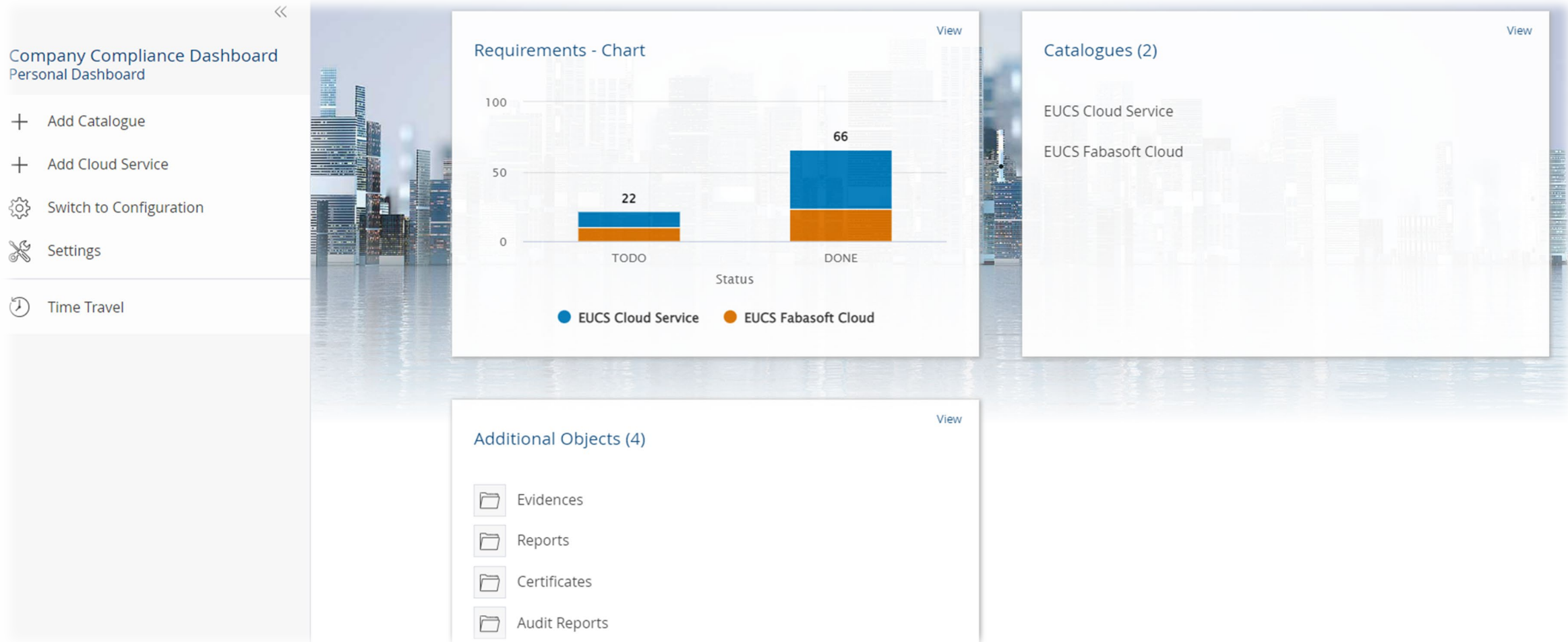


A seamless audit trail of the evidence provides traceability and protection against manipulation, ensuring document integrity at all times.

Company Compliance Dashboard – “CCD”



CCD - Demonstrator




CCD - Demonstrator



Signatures

Last Signature Type

 Confirm Metric Implementation

Last Signature by

 Briere0004 William

Last Signature on/at





10/03/2022 07:51:42 AM

Remark of Last Signature

implemented metric via AMOE

Signatures

Show Details (2)

<input type="checkbox"/>	Signature Type	Signed by	Signed on/at	Remark
1	 Assign Metric	 Carney0004 Wanda	10/03/2022 07:51:24 AM	please implement metric
2	 Confirm Metric Implementation	 Briere0004 William	10/03/2022 07:51:42 AM	implemented metric via AMOE

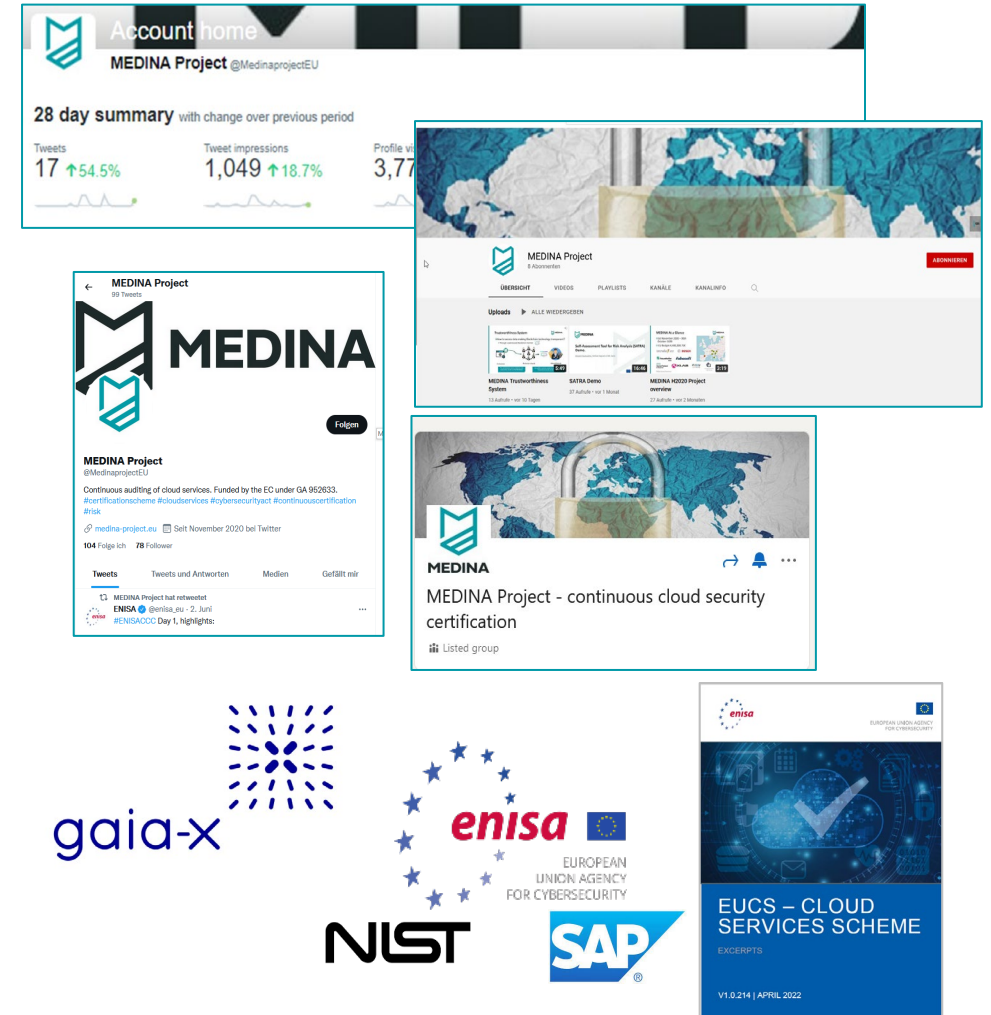
Additional Achievements



Concrete collaborations with ENISA (EUCS) and NIST (OSCAL)

Initial validation of “actionable” technical/organizational metrics

PoC designed and deployed



How-To EUCS Continuous?

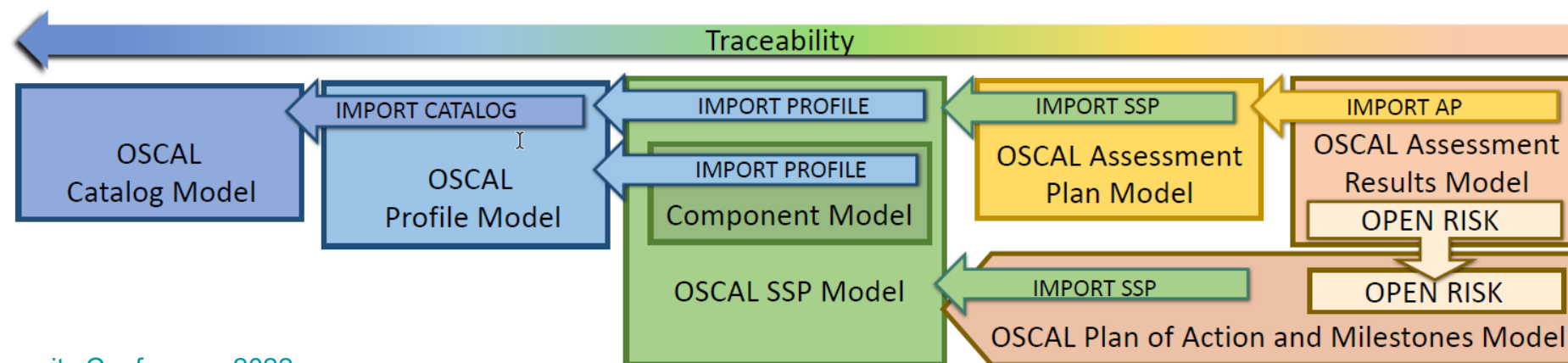


1. Provide **implementation/audit guidance** about EUCS requirements where some degree of automated monitoring is needed
2. Consider integrating a **catalogue of metrics** as part of the implementation guidance for EUCS
3. **Guidance on selecting tools/technologies** for automated (continuous) monitoring
4. Actively monitor the development of **NIST OSCAL**

A Few Words About OSCAL



- The Open Security Controls Assessment Language was born as a collaboration between NIST and FedRAMP
- OSCAL provides a single machine-readable language to **represent and trace** security controls frameworks, implementation guidance, implementation of security controls, security assessment plans, security assessment results/reports



Leveraging OSCAL



- ✧ Machine-readable representation of security controls (e.g., EUCS, BSI C5)
 - Both for technical and organizational measures
- ✧ Metrics descriptions for assessing compliance with security controls
- ✧ Leverage for assessment results
- ✧ Support for standardization roadmap and industrial adoption e.g., Gaia-X

OSCAL <> EUCS

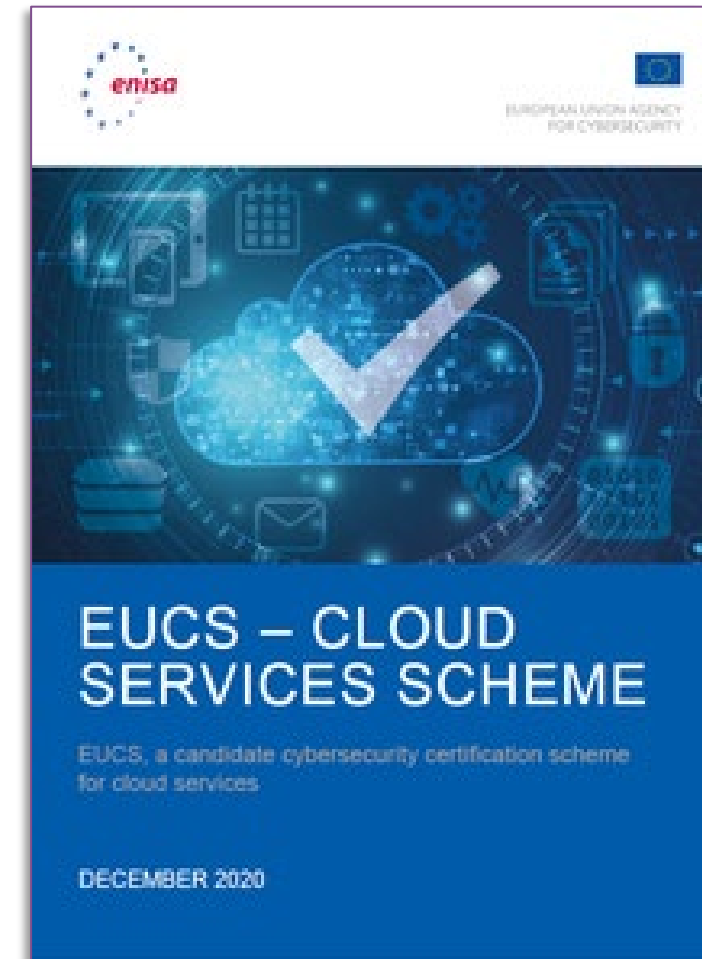
- Machine-readability benefits EUCS continuous
- NIST OSCAL as a promising alternative for representing EUCS' catalogue and assessments
- Initial discussions ENISA – MEDINA - NIST

OSCAL	EUCS	Examples
Groups/ID	Domain	A7
Groups/title	Category	A7 Operational Security
Groups/parts/prose(objective)	Objective	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Groups/Controls/properties/value(label)	Control ID	OPS-02
Groups/Controls/title	Control	CAPACITY MANAGEMENT - MONITORING
Groups/Controls/parts/prose/(control-objective)	Control Objective	The capacities of critical resources such as personnel and IT resources are monitored.
Groups/Controls/parts/parts/properties/value(label)	Requirement ID	OPS-02.3
Groups/Controls/parts/parts/prose(item)	Requirement	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1

Summary



- EUCS is coming fast!
 - CEN CENELEC
 - NIS2 Directive
- Early EUCS adopters might benefit from good practices/guidelines
- MEDINA aims to facilitate adoption of EUCS continuous
 - Open-source access
 - Demo available on request



>getintouch

