Harmonizing People, Processes, and Technology for Robust Cybersecurity

D1.4 Annual report on KPIs assessment v2

Document Summary Information

Grant Agreement No	101158555	**Acronym**	CYberSynchrony
Full Title	Harmonizing People, Processes, and Technology for Robust Cybersecurity		
Start Date	01/06/2024	**Duration**	36 months
Project URL	https://www.cybersynchrony.eu/		
Deliverable	D1.4 Annual report on KPIs assessment v2		
Work Package	WP1 Project Management		
Contractual due date	30.06.2026	**Actual submission date**	08.07.2026
Type	R	**Dissemination Level**	PU
Lead Beneficiary	MAG		
Responsible Author	Violeta Vasileva (MAG)		
Contributions from	Violeta Vasileva (MAG), Evangelos Michos (IANUS), Eleni Keliri (EBOS)		

Funded by the European Union

ECCC

Funded by the European Union under Grant Agreement no. 101158555 and supported by the European Cybersecurity Competence Centre (ECCC). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Revision history

Version	Date	Changes	Contributor(s)
0.1	31.03.2026	Initial Deliverable structure	Violeta Vasileva (MAG)
0.2	06.04.2026	Updated ToC and KPIs framework alignment	Violeta Vasileva (MAG)
0.3	15.05.2026	Consolidated KPIs methodology	Violeta Vasileva (MAG)
0.4	08.06.2026	Consolidated KPIs methodology inputs from all WP owners	Violeta Vasileva (MAG), Evangelos Michos (IANUS), Eleni Keliri (eBOS)
0.5	24.06.2026	Final draft ready for internal review	Violeta Vasileva (MAG)
0.6	26.06.2026	Peer review	Demetris Koutras (FP)
0.7	29.06.2026	Peer review	Eleni Keliri (eBOS)
0.8	03.07.2026	Final draft addressing comments from internal review	Violeta Vasileva (MAG)
0.9	06.07.2026	Final quality check	Eleni Keliri (EBOS)
1.0	08.07.2026	Final version ready for submission	Violeta Vasileva (MAG)

Disclaimer

The content of the document herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the CYberSynchrony consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© CYberSynchrony Consortium This Deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

[1] According to CYberSynchrony's Quality Assurance Process for reports:

- 3 months before Deliverable's Due Date: Table of Contents ready to be reviewed by WP leader/ Technical Manager/ Quality Manager
- 2 months before Deliverable's Due Date: 50% should be complete. Review by the Quality Manager (& Technical Manager for software).
- 1 month before Deliverable's Due Date:100% should be complete. Review by the Quality Manager and Peer Reviewers.
- M: Sent to PC for Submission to the EC after addressing all comments by Quality Manager and Peer Reviewers

Table of Contents

1 Executive Summary 6
2 Introduction 7
2.1 Mapping CYberSynchrony Outputs 7
2.2 Linkage to other project outputs 7
2.3 Deliverable Structure 8
3 KPIs Progress Assessment: M24 Status 9
3.1 Objective 1 9
3.2 Objective 2 14
3.3 Objective 3 16
3.4 Objective 4 18
3.5 Objective 5 19
3.6 Objective 6 20
3.7 Objective 7 21
3.8 Objective 8 21
3.9 Objective 9 24
4 Use Case KPIs: M24 Status 28
4.1 UC1 – Digital Healthcare: KPIs Status 28
4.2 UC2 – Public Administration: KPIs Status 29
4.3 UC3 – Higher Education: KPIs Status 31
4.4 Open Call KPIs 33
5 Key Exploitable Results (KERs): Update 34
6 KPIs Summary Table 38
7 M12 vs M24 Comparison (D1.3 vs D1.4) 42
8 Deviations and Mitigation Measures 45
8.1 Confirmed Deviations 45
8.2 Mitigation Measures Applied 46
8.3 Revised Targets and Outlook 46
8.4 KPIs TEMPLATE 47
9 Conclusions 48
Annex I - KPIs Template for Cybersynchrony KPIs Mapping 49

Table 1: Adherence to CYberSynchrony's GA 7
Table 2: Links to other Project Outputs/Work 7
Table 3 : KPIs for Objective 1 9
Table 4 Objective 2 KPIs 14
Table 5 Objective 3 KPIs 16
Table 6 Objective 4 KPIs 18
Table 7 Objective 5 KPIs 19
Table 8 Objective 6 KPIs 21
Table 9 Objective 7 KPIs 21
Table 10 Objective 8 KPIs 22
Table 11 Objective 9 KPIs 25

© CYberSynchrony, 2026

Table 12 UC1 – Healthcare KPIs 28
Table 13 UC2 - Public Administration KPIs 29
Table 14 : UC3 – Higher Education KPIs 31
Table 15 KER Overview 34
Table 16 KER Exploitation Plans and Benefits by Partner 35
Table 17 KPIs Dashboard Summary 38
Table 18 Communication and Dissemination KPIs – M12 vs M24 40
Table 19 M12 vs M24 KPIs Comparison 42

© CYberSynchrony, 2026

Acronyms and abbreviations

Abbreviation / Term	Description
AI	Artificial Intelligence
CISO	Chief Information Security Officer
CYBERA	Cyber Analytics and Risk Assessment Module
CYBERGOPLUS	Compliance and Governance Framework Module
CYBERWISE	Cybersecurity Awareness and Training Platform
CYBRITE	Cyber Response and Incident Tracking Environment
CROSS-CORE	Secure Data Exchange and Coordination Platform
CYRESCUE	Penetration Testing and Incident Simulation Toolkit
D&C	Dissemination and Communication
DORA	Digital Operational Resilience Act
ECCC	European Cybersecurity Competence Centre
EHR/EMR	Electronic Health Records / Electronic Medical Records
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
IoMT	Internet of Medical Things
IPR	Intellectual Property Rights
IT	Information Technology
KPIS	Key Performance Indicator
KER	Key Exploitable Result
MISP	Malware Information Sharing Platform
MOS	Mean Opinion Score (used for usability ratings)
MS	Member States
NIS2	Network and Information Security Directive 2
OA	Open Access
PEN Test	Penetration Test
PII	Personally Identifiable Information
SOAR	Security Orchestration, Automation and Response
SIEM	Security Information and Event Management
STIX/TAXII	Structured Threat Information Expression / Trusted Automated Exchange of Intelligence Information
TTPs	Tactics, Techniques, and Procedures
UPRC	University of Piraeus Research Center
WP	Work Package

© CYberSynchrony, 2026

1 Executive Summary

This document constitutes D1.4 – the second Annual Report on KPIs Assessment for the CYberSynchrony project. It provides a comprehensive update on the project's Key Performance Indicators (KPIs) framework at M24 building directly on the baseline established in D1.3.

A key outcome of the M24 review is the consolidation of the KPIs set. The original D1.3 framework contained **39 Objective KPIs entries** across 9 objectives, many of which were duplicated across objectives. Following consortium-wide alignment, the framework has been refined to **25 unique Objective KPIs**, with duplicates formally identified and cross-referenced. This ensures clarity, avoids double-counting, and strengthens the traceability of evidence to outcomes.

Significant progress has been made across all KPIs dimensions:

- Measurement methodologies have been substantially enhanced for all 25 objective KPIs, with formal registers (Threat Assessment Register, Risk Scenario Register, Vulnerability Register, Incident/Response Register, Information Sharing Log, and Cross-Border Exercise Register) now operational or in active preparation.
- KPIs ownership has been assigned to specific consortium partners for each indicator, with verification deliverables explicitly mapped.
- Partial quantitative results are available for KPI3.3 (Phishing Campaigns: IANUS 29 participants, MAG 53 participants, UPRC: 117 participants), and KPI9.4 (D&C engagement: 56% increase, target exceeded).
- Communication and Dissemination KPIs show strong M24 performance: website traffic doubled (3.6K users), press releases increased from 4 to 39, scientific papers from 3 to 10, and video content from 0 to 5 video clips.
- Within WP8, the pilot Use Cases in Healthcare, Public Administration and Education (AMC, EGL, UPRC) have defined their exact KPIS scenarios, aligned measurement methodologies with technical partners, and initiated baseline data collection.
- For some KPIs also supportive material, such as User Satisfaction Questionnaires, pre- and post-training surveys, has been prepared and evaluated.

One notable revision from D1.3 concerns KPI2.1 (Penetration Tests): the original target of 60 tests was identified as infeasible. Following consortium review, the target has been revised to 6 targeted penetration tests (aligned with the 3 use case environments). Similarly, KPI1.4 (Platform Usability) has been updated from the MOS rating scale to the standardized System Usability Scale (SUS), providing a more robust and internationally comparable measurement.

KPI9.1 was refined from “Policy Compliance Rate” to “Policy Awareness and Compliance Readiness Rate”. The original KPIs referred to measuring compliance with EU-wide cybersecurity policies and standards, which is difficult to assess within the project and cannot be fully controlled by the consortium. The revised KPIs keeps the same policy-oriented ambition but focuses on what the project can directly support and evidence: stakeholder engagement with the CYberSynchrony Policy Toolkit and related policy guidance. KPI9.3 (of version D1.3) was removed as cybersecurity certification attainment is outside the project's direct scope and control. The related objective is partially covered by KPI9.2, which focuses on the adoption of cybersecurity standards and best practices. KPI7.1 is not monitored as a separate active KPIs, as it duplicates KPI3.4/KPI4.4. Its evidence will therefore be captured through the primary vulnerability discovery indicator, where the 15% reduction target and vulnerability evidence register are maintained. The original wording referred to reducing high-severity vulnerabilities by 15% while maintaining the overall discovery rate. In the updated KPIs framework, the indicator is expressed more simply as a 15% reduction compared to other approaches.

The CYberSynchrony consortium enters Year 3 with a mature, operationalised KPIs framework ready to deliver measurable evidence of impact. The pilot deployment phase commencing at M25/M26 will generate the quantitative data required for the final consolidated KPIs report in D1.5.

© CYberSynchrony, 2026

2 Introduction

2.1 Mapping CYberSynchrony Outputs

This section presents the CYberSynchrony's Grant Agreement (GA) commitments, as extracted from the formal deliverable and task description, in respect to their outputs and work to be performed.

Table 1: Adherence to CYberSynchrony's GA

Component no	Component title	Respective Document Chapter(s)	Justification
DELIVERABLE			
D1.4	Annual Report on KPIs Assessment v2	Chapters 3-8	Provides a comprehensive review of all KPIs, linking them to project objectives and use cases. Lays the updates and progress on KPIs measurement and outlines methodology, deviations, and mitigation strategies.
TASKS			
Task T1.3	KPIs Monitoring and Reporting Framework	Chapters 3, 4, 6, 7, 8	Establishes the updated KPIs set (25 Objective KPIs), refined tracking methodology, ownership assignments, partner/tool mapping, evidence requirements, and M24 progress dashboard.

2.2 Linkage to other project outputs

The table below explains how the deliverable is related to other project outputs and specific deliverables.

Table 2: Links to other Project Outputs/Work

WP Number	Task Number	Deliverable Number related	Content
WP1	T1.1, T1.3	D1.3	D1.4 builds directly on D1.3 by updating, refining, and consolidating the KPIs tracking and reporting system for M24.

© CYberSynchrony, 2026

WP3	T3.1, T3.3, T3.4	D3.3, D3.4	Provides technical inputs for threat intelligence, risk assessment, and anomaly detectio(KPI1.1, KPI1.3, KPI1.5, KPI3.6, KPI3.7).
WP4	T4.1, T4.3, T4.4	D4.3, D4.4	Core input for incident detection, response, and vulnerability management KPIs (KPI2.1–KPI2.4, KPI3.4, KPI4.3).
WP5	T5.1, T5.2, T5.3	D5.3, D5.4	Related to cross-border exercise and information sharing KPIs (KPI4.2, KPI4.5, KPI5.1, KPI5.2).
WP6	T6.1, T6.2, T6.3, T6.5, T6.6	D6.5, D6.7	Informs awareness, training coverage, compliance, and certification KPIs (KPI3.3, KPI8.1, KPI8.2, KPI9.1, KPI9.2, removal of KPI9.3).
WP8	T8.1-T8.4	D8.2, D8.4	Use case pilot results and exercise data for KPI2.1–KPI2.4, KPI3.3, KPI4.2, KPI4.5, KPI8.1.
WP9	T9.1, T9.2, T9.3	D9.1, D9.5, D9.6, D9.7	Exploitation, dissemination, and stakeholder engagement KPIs (KPI9.4, KPI9.5, KPI9.6).

2.3 Deliverable Structure

This deliverable is structured as follows:

Chapter 1 – Executive Summary: Provides a concise overview of M24 KPIs progress, key achievements, and changes from D1.3.

Chapter 2 – Introduction: Defines purpose, scope, and GA mapping; provides linkage to other deliverables and the structural overview.

Chapter 3 – KPIs Progress Assessment: M24 Results: Details the updated and consolidated KPIS set by project objective, including refined measurement methodologies, KPIS ownership, and verification deliverables.

Chapter 4 – Use Case KPIs M24 Status: Reports the Use Case KPIs with M24 status updates from AMC (healthcare), EGL (public administration), and UPRC (higher education).

Chapter 5 – Key Exploitable Results (KERs): Update: Provides an updated summary of KERs and their market readiness status.

Chapter 6 – KPIs Dashboard Summary: Consolidates all 25 Objective KPIs with target, M24 status and trend assessment.

Chapter 7 – M12-M24 KPIs Comparison (D1.3 vs D1.4): Presents a systematic comparison of KPIs definitions, targets and progress

Chapter 8 – Deviations and Mitigation Measures: Documents confirmed deviations from original targets, applied mitigations, and revised outlook.

Chapter 9 – Conclusions: Summarises key contributions and the path forward to D1.5.

© CYberSynchrony, 2026

3 KPIs Progress Assessment: M24 Status

This chapter presents the consolidated and updated KPIs framework for CYberSynchrony at M24. The report now reflects the agreed KPIs verification approach, including common KPIs verification tables in upcoming deliverables, explicit evidence types, revised feasibility assumptions for penetration testing, use of incident and vulnerability registers, and revised measurement methods. The previous version contained 39 entries, but the final Objective KPIs set is expected to include 25 Objective KPIs, since we have same duplicate entries. The Consortium agreed that a common KPIs verification table will be inserted in all upcoming deliverables to document target, methodology, owner, partners/tools, evidence, measurement date, result and deviations. All KPIs results, evidence and final achievement status will be consolidated and formally reported in **D1.5 – Final Annual Report on KPIs Assessment**, which will serve as the final version of the project KPIs assessment framework.

The tables below update the KPIs set by project objective.

3.1 Objective 1

Enhance the threat assessment and risk monitoring services, enabling quicker identification of threats and attacks by leveraging state-of-the-art threat intelligence platform (e.g. MISP, STIX/TAXI, ThreatConnect) and attackers' profiles models that utilizes artificial intelligence to gather and analyses real-time information about emerging cyber threats and attackers' behavior.

Related modules: CYRESCUE, CYBERRA, CYBRITE

Verification: D3.3, D4.3, D4.4, D7.4, D8.2, D1.5 final KPIs consolidation

Table 3 : KPIs for Objective 1

KPI ID / name	Description	KPI Owner	Verification means	Target	Measurement Methodology
KPI1.1 Number of Threat Assessments Carried Out	Measure the quantity of threat assessments conducted using the state-of-the-art threat intelligence platform gathering real-time information about emerging cyber threats and attack potential, analysing their potential impact and vulnerability severity, on critical infrastructure, essential entities, and digital services aiming to improve the threat assessment capabilities and	IANUS	D4.3	>36 threat assessments	Use a **Threat Assessment Register (excel)**. Each valid row counts as one threat assessment when it documents a concrete threat affecting a pilot/use case asset, based on tool output or scenario evidence. Minimum evidence should include date, pilot/use case, partner, tool used, threat type, affected asset, severity, likelihood/impact, recommended action, and evidence link. Sources may include MISP IoC analysis, Wazuh/Suricata alerts, Kitsune intelligence, Anomaly Detector outputs, or validated pilot scenarios. Evidence can be a screenshot, MISP export, alert ID, tool report, PDF, JSON output, or short analyst note. The Anomaly Detector contributes one threat

© CYberSynchrony, 2026

	enhance the early detection and response to potential cyber threats				assessment row per validated anomaly. The detector consumes Suricata flow features from eve.json through the shared Kafka broker and flags flow windows whose reconstruction error exceeds the configured threshold, indicating deviation from the learned traffic baseline. The responsible analyst reviews each flagged window, inspects the contributing flow features (protocol, ports, byte and packet counts, flow duration, peer pairs), correlates with concurrent Suricata signatures, Wazuh events, or MISP IoCs where present, and decides whether the deviation represents a real threat. Confirmed cases are recorded with anomaly score, reconstruction error, the contributing flow features, affected asset, severity, likelihood/impact, and recommended action. Evidence link points to the AD alert payload plus any correlated Suricata/Wazuh alert IDs. **Partners - Tools: IANUS - MISP, Wazuh, Suricata; MAG - Anomaly Detector; MER - Kitsune Search / Monitoring**
KPI1.2 Number of Risk Scenario Analyses Carried Out	Track the number of risk scenario analyses performed using the advanced threat intelligence platform for risk management and incident response strategies.	MER	D8.2	>=13 risk assessments/ risk scenarios	Use a **Risk Scenario Register (excel)**. Each valid row counts as one risk scenario analysis when it includes asset, threat, vulnerability, likelihood, impact, initial risk score, mitigation action, residual risk score, responsible partner, and evidence. Scenarios should be linked to pilot contexts such as data breach, service unavailability, device compromise, software vulnerability, insider threat,

© CYberSynchrony, 2026

					phishing, or supply-chain exposure. **Partners - Tools: FP - ASA/PTA, MER - Kitsune, TRUST - trustSense and/or phishing results, UC Leaders UPRC, AMC, EGL**
KPI1.3 Threat Intelligence Platform Effectiveness	Measure the platform's ability to detect and mitigate threats successfully.	IANUS	D3.3	Achieve threat detection & mitigation rate >85% out of 100	Use a **Threat Effectiveness Test Log.** Define a set of simulated or confirmed threat events, inject or observe them during pilot/testing activities, and record whether the platform correctly detected, enriched, classified, and routed each threat to a recommendation or playbook. The platform effectiveness rate will be calculated as: correctly handled threat events / total injected or confirmed threat events x 100. Given that the platform follows a recommendation-based response philosophy, “mitigation” is understood as the generation of a valid recommendation or playbook, followed by analyst acknowledgement, rather than automatic blocking or autonomous remediation. The Anomaly Detector contributes to the overall effectiveness rate through its anomaly-recall performance on validation events. During pilot validation, a predefined set of anomalous traffic conditions will be exercised against the monitored segment. These conditions will generate flow features in Suricata’s eve.json that deviate from the trained baseline in terms of traffic volume, timing, protocol distribution, or peer-pair behaviour. For each tested anomalous condition, the following will be recorded:

© CYberSynchrony, 2026

					(i) whether the Anomaly Detector raised an alert through reconstruction error above the defined threshold within the expected time window; (ii) whether the alert reached the analyst console together with its anomaly score and contributing flow features; and (iii) whether the analyst was able to interpret the alert and route it to the appropriate recommendation or playbook. The Anomaly Detector's contribution will be calculated as the number of correctly flagged anomalous conditions divided by the total number of tested anomalous conditions, multiplied by 100. This result will then be aggregated with the performance of the other detection components to assess achievement of the platform-level effectiveness target of **>85%**. Attack-type classification is performed by the analyst based on the contributing flow features and contextual evidence, not automatically by the model. **Partners - Tools**: **IANUS - MISP, Wazuh, Suricata; MAG - Anomaly Detector; MER - Kitsune Monitoring / Search; FP - DCO; UC leaders UPRC, AMC, EGL**
KPI1.4 **CYberSynchrony Platform Usability**	User Satisfaction Rating measures the satisfaction of security analysts and incident responders with the platform's usability and features.	EBOS	D7.4, D8.2	SUS > 70%	The System Usability Scale **(SUS)** will be used to assess the usability of the CYberSynchrony Platform. A **10-item standardized questionnaire** will be administered to pilot users & Beneficiaries on a 5-point Likert scale (Strongly Disagree to Strongly Agree). Responses will be scored using the

© CYberSynchrony, 2026

					standard SUS method, where positive items will be adjusted by subtracting 1 and negative items by subtracting the response from 5. The total score will then be multiplied by 2.5 to produce a usability score ranging from 0 to 100. The resulting SUS score will be used as the indicator of their satisfaction and their perceived usability. The questionnaires will be distributed to pilot users (Use Cases & FSTP Beneficiaries) by the end of their use cycle.
KPI1.5 Threat Intelligence Platform Security	Platform Vulnerability Remediation Time – time taken to identify and remediate vulnerabilities in the Threat Intelligence platform.	MAG	D3.3	Reduce vulnerability remediation time to ≤15 days aiming for faster remediation of vulnerabilities enhancing the platform's security posture	Use a **Platform Vulnerability Register (excel)** for vulnerabilities affecting CYberSynchrony platform components or deployed tools. Each row should include vulnerability ID, component, owner, tool/method used to detect it, severity, date identified, remediation action, date fixed, date validated, and evidence link. Calculate remediation time as the number of days between identification and validated closure, then report the average remediation time. **Partners-Tools: IANUS – MISP, Wazuh, Suricata, TRUST - Snyk; FP - ASA; UC leaders UPRC, AMC, EGL**
KPI1.6 Threat Intelligence Platform Security Incident Response Time	Measures time taken to respond to security incidents with emphasis on zero-day threats within the Threat Intelligence platform.	MAG	D4.4	Reduce response time: 4h(zero-days)/ 8h (other threats) in the current year compared to last year,	Use an **Incident / Response Register** based on simulated platform security incidents or real incidents if they occur. For each event, record detection time, alert validation time, response start time, response type, responsible partner, tool involved, and evidence. Response start can be defined as analyst acknowledgement, escalation, containment

© CYberSynchrony, 2026

				ensuring expedited containment and mitigation of incidents.	recommendation, or DCO playbook generation. Calculate response time as response start time minus detection time, separated where relevant into zero-day-type scenarios and other threats. **Partners-Tools: IANUS - MISP, FP - DCO Playbooks; BYTE - Secure Exchange / Integrity layer**

3.2 Objective 2

Minimize the duration and impact of cyber incidents with timely and coordinated incident response by integrating automation and orchestration capabilities in incident response coordination tools by automating repetitive tasks and orchestrating incident response workflows, the efficiency of response efforts can be significantly increased, leading to faster containment and mitigation of cyber incidents enabling faster and more effective response efforts.

Related modules: CROSS-CORE, CYBRITE

Verification: D8.2, D8.4, D1.5 final KPIs consolidation

Table 4 Objective 2 KPIs

KPI ID / name	Description	KPI Owner	Verification means	Target	Measurement Methodology
KPI2.1 Number of Penetration Tests Provided	Measure the quantity of penetration tests provided to assess the security of systems, networks, and applications by simulating real-world cyberattacks.	FP	D8.2, D8.4	6 penetration tests (consortium use cases and/or open calls)	Penetration testing evidence will be collected through a **Threat Assessment Register**. Each aspect represents one assessed threat, vulnerability, or how effective can be in the use case environment. The main technical inputs will come from Security Breach Simulation (**SBS**) and, where applicable, Purple Team Assessment (**PTA**). SBS will be used to execute controlled adversary-emulation activities and generate technical evidence, such as executed techniques, affected assets, Wazuh alerts, DCO incidents, and Caldera operation reports. PTA may be used to structure selected results into MITRE ATT&CK-mapped test cases, record whether the behaviour was prevented, alerted, logged, or missed, and attach supporting evidence. The final risk value will be calculated manually by the analyst using the following formula: Risk = Likelihood × Impact In this context, likelihood may be estimated by considering both the threat evidence and the vulnerability exposure of the affected asset. In many

					modern methodologies, the probability of an event occurring can be understood as a combination of threat and vulnerability, while impact represents the resulting technical, operational, or financial damage if the event occurs. Indicatively: Likelihood = Threat × Vulnerability Therefore, the assessment may be interpreted as: Risk = (Threat × Vulnerability) × Impact The vulnerability score may be derived from the SBS/PTA results, observed exploitability, affected asset exposure, missing controls, detection gaps, or known weaknesses identified during the test. The final score should be reviewed and validated by the responsible analyst. For each pilot, the following minimum information should be collected in order to produce a penetration testing report: • Use case name • Assessment date • Scope of the test • Target asset or system • Tool or method used, e.g. SBS, PTA, or manual testing • Executed scenario or tested technique • Vulnerability or weakness identified • Evidence produced, e.g. SBS report, Caldera output, Wazuh alert, DCO incident, PTA test case, screenshot, log, or analyst note • Vulnerability score or severity • Likelihood score • Impact score • Calculated risk value • Recommended mitigation or corrective action **Partners/Tools:** FP/SBS - penetration testing evidence; WP7/FSTP applicants where relevant; use case leaders; technical partners supporting tested environments.
KPI2.2 Incident Detection Time	Measure the average time taken to detect and identify cyber incidents, including the initial breach or suspicious activity.	IANUS	D8.2 (primary), D8.4	Reduce average incident detection time to 3 days	Use the **Incident Detection Time Register** For each simulated or real incident, record incident start/injection time, detection timestamp, source tool/alert, validation timestamp, and evidence. Calculate detection time as detection timestamp minus incident start/injection timestamp and report the average across validated incidents. **Partners/Tools: IANUS - Wazuh/Suricata/MISP; MAG - Anomaly Detector; FP-ASA/playbooks; BYTE - platform/routing; MER and use case leaders.**
KPI2.3 Incident	Track the average time	FP	D8.2 (primary);	Reduce average	Use the **Incident / Response Register**. For each incident, record the validated detection time and

© CYberSynchrony, 2026

Response Time	taken to respond and initiate incident response actions after detection of a cyber incident.		D8.4	incident response time to 15 days	the first response initiation time. Response initiation can be DCO playbook generation, analyst acknowledgement, escalation ticket creation, containment recommendation, or documented mitigation proposal. Calculate response time as first response initiation time minus detection time, and report the average. **Partners/Tools:** FP - DCO Playbooks; pilot SOC analysts / pilot owners
KPI2.4 Incident Resolution Rate	Measure the percentage of cyber incidents successfully resolved and mitigated without further impact.	FP	D8.2 (primary); D8.4	Achieve ≥80% incident resolution rate within 24 hours	Use the **Incident / Response Register.** For each incident or exercise scenario, record whether it was resolved, mitigated, or closed without further impact within the defined timeframe. Evidence may include playbook closure, analyst confirmation, pilot owner validation, or mitigation report. Calculate resolution rate as incidents resolved within target timeframe / total incidents tested x 100. **Partners/Tools:** FP - DCO Playbooks; pilot SOC analysts / pilot owners

3.3 Objective 3

Strengthen the risk monitoring services and early detection of cyber incidents by deploying advanced **cybersecurity analytics tools** to analyze network traffic, software security, user behavior, and system activity identifying anomalous activities and insider threats

Related modules: CYBERRA, CYBRITE

Verification: D3.4, D5.4, D6.5, D1.5 final KPIs consolidation

Table 5 Objective 3 KPIs

KPI ID / name	Description	KPI Owner	Verification means	Target	Measurement Methodology
KPI3.1 Number of Threat Assessments Carried Out	***This KPI is a duplication of KPI 1.1***				
KPI3.2 Number of Risk Scenario Analyses Carried Out	***This KPI is a duplication of KPI 1.2***				
KPI3.3 Number of Potential Users Covered per Test/Exercise	Measure coverage of potential users (employees) in cybersecurity tests and exercises assessing	TRUST	D6.5;	Average of 150 potential users per test/exercise ***Results of the Phishing Campaign in JUNE 2026:***	**Use of Phishing Campaign / Exercise Register** Count participants per completed cybersecurity test, phishing campaign or exercise and calculate the average number of potential users covered per test/exercise. Evidence should include invitation list, participation logs,

	organisational readiness.			***Ianus: 29*** ***MAGGIOLI: 53*** ***UPRC: 117*** ***participants***	campaign export, attendance list Campaigns that occur after D6.5 can be consolidated in D1.4/D1.5. **Partners/Tools: TRUST - phishing campaigns/; FP: ASA, , PTA, SBS, CSPA, END USERS: UPRC; MAG, IANUS: Wazuh, Suricata, MER: Kitsune, WP8/use case leaders.**
KPI3.4 Number and Nature of Vulnerabilities Discovered	Track vulnerabilities discovered using advanced analytics tools, evaluating severity and criticality to prioritize remediation.	TRUST	D6.5 if results are available in time;	Reduce high-severity vulnerabilities by 15% vs. other approaches	**Use a Vulnerability Register** Record each validated vulnerability with severity, nature, source tool/campaign, date, affected system, owner and remediation status. For the 15% reduction target, compare the number of high-severity vulnerabilities identified after CYberSynchrony-supported assessment/remediation against the selected baseline or alternative approach, while documenting the overall discovery rate. **Partners/Tools: TRUST - trustPhish; FP - ASA/PTA, SBS,; IANUS - Wazuh /MAG/MER - Kitsune, technical evidence; use case leaders.**
KPI3.5 Threat Intelligence Platform Security	***This KPI is a duplication of KPI 1.5***				
KPI3.6 **Risk Scenarios Analysed**	Track the number of customised risk scenarios analysed to assess the impact of potential cyber threats on critical sectors.	MER	D5.4	Increase analysed risk scenarios by 15%; ≥12 customised scenarios	**Use Risk Scenario Register** Use the risk scenario register to record customised scenarios and compare year-over-year changes in number and complexity. Count each scenario only when it contains asset, threat, likelihood, impact and mitigation . **Partners/Tools:** MER - Kitsune/risk monitoring; pilots and use case leaders.
KPI3.7 Risk Mitigation Index	Measure the effectiveness of risk mitigation strategies based on the reduction of	MAG	D3.4	Achieve 20% reduction in identified risks	**Use the Risk Mitigation / Risk Scenario Register as in KPIS3.6,** with addition of before/after risk scoring fields. Calculate reduction in identified risks as (initial risk score - residual risk score) / initial risk score x 100, aggregated across scenarios.

© CYberSynchrony, 2026

	identified risks.				**Partners/Tools: MER - Kitsune Monitoring / Kitsune Search; FP - DCO, CSPA, ASA, PTA, SBS; TRUST -trustSense; UC leaders: AMC, EGL, UPRC for validation.**

3.4 Objective 4

Enhance mutual assistance among MS and facilitate more frequent and realistic cross-border cyber exercises and behavioural change interventions by leveraging virtual cyber range platforms to simulate complex cyber scenarios across borders, critical infrastructure, and digital services enabling more realistic and frequent joint cybersecurity exercises, to bolster mutual assistance efforts and ensure better preparedness for large-scale cross-border cyber incidents.

Related modules: CYRESCUE, CROSS-CORE

Verification: D5.3, D5.4, D8.2, D8.4, **D1.5 final KPIs consolidation**

Table 6 Objective 4 KPIs

KPI ID / name	Description	KPI Owner	Verification means	Target	Measurement Methodology
KPI4.1 Number of Penetration Tests Provided	***This KPI is a duplication of KPI2.1***				
KPI4.2 Number of Cross-Border Actions/Exercises	Quantify cross-border actions and joint cybersecurity exercises facilitated by virtual cyber range platforms. (WP5)	BYTE	D5.3	10 cross-border actions/exercises	Use a **Cross-border Exercise / Collaboration Register** where each valid row represents one completed cross-border action or exercise mediated by the Cross-CORE module, when it involves at least two organisations operating in different Member-State perimeters, produces a concrete joint result, and leaves auditable evidence through the Cross-CORE infrastructure. Evidence will include Hyperledger Fabric anchors, SHA-256 fingerprints, transaction IDs, MISP event IDs, API logs, screenshots or exercise reports. The register records scenario ID, partners involved, action type, date, Cross-CORE primitive, evidence link and validation outcome. Partners/Tools: BYTE - blockchain; WP8/use case leaders; FP, IANUS -

© CYberSynchrony, 2026

					Wazuh/Suricata, Pilot PARTNERS, DSA, KETYAK
KPI4.3 Vulnerabilities Addressed	Track the number of identified vulnerabilities addressed and remediated by critical infrastructure operators.	TRUST	D8.2	Address and remediate ≥80 vulnerabilities	**Use ASA / Vulnerability Remediation Register**: Track identified vulnerabilities and their remediation status. Count vulnerabilities moved from open/identified to addressed/ remediated/accepted based on documented action or validated non-critical status. Evidence should include ASA export, remediation note, closure date, responsible partner and affected asset. **Partners/Tools:** FP - ASA/PTA and remediation tracking; TRUST - complementary vulnerability inputs; pilot owners; IANUS - MISP, UPRC.
KPI4.4 Number and Nature of Vulnerabilities Discovered	***This KPI is a duplication of KPI3.4.***				
KPI4.5 Incident Collaboration Index	Measure the effectiveness of cross-border incident response coordination based on successful collaborative efforts.	BYTE	D5.4	Increase Incident Collaboration Index to 70%	**Use an Incident Collaboration Survey:** After each cross-border or joint incident exercise, we will collect and analyse cross-border incident response collaborations, through a short participant survey. **Partners/Tools:** BYTE - blockchain; MER technical tools; WP8/use case leaders.

3.5 Objective 5

Ensure data privacy and security during information exchange by establishing a secure and standardized communication infrastructure for sharing incident data, threat intelligence, and best practices among MS and relevant stakeholders utilizing encrypted communication channels

Related modules: CYRESCUE, CROSS-CORE

Verification: D5.3, D5.4; final KPIs consolidation in D1.5

Table 7 Objective 5 KPIs

KPI ID / name	Description	KPI Owner	Verification means	Target	Measurement Methodology
KPI5.1 Number of Risk	Measure the quantity of risk monitoring	MER	D5.4	Activate 25 risk monitoring services; ≥95% achieve 4/5	**Use a User Satisfaction Questionnaire:** We count each active monitoring setup as one

© CYberSynchrony, 2026

Monitoring Services Provided	services offered as part of the secure communication and information sharing infrastructure.			user satisfaction; false positive rate <5%	risk monitoring service. For example, one Wazuh monitored endpoint group, one Suricata monitored network segment, one Kitsune monitoring profile, one MISP feed/correlation setup, one Anomaly Detector deployment, one scheduled ASA scan, or one risk monitoring dashboard. For each service, we record tool, partner, pilot, monitored asset/scope, start date and evidence that it was active. Satisfaction and false positives can be measured separately through user surveys and alert review. **Partners/Tools:** MER - Kitsune; IANUS - Wazuh/Suricata; MAG - Anomaly Detector; pilots.
KPI5.2 Information Sharing Frequency	Measure the frequency of information sharing among Member States during cyber incidents and crises.	BYTE	D5.3	Increase information sharing frequency to 75% of cyber incidents/crises	**Use Information Sharing Log:** For each incident, exercise or threat intelligence event, we record whether information was shared with another partner, pilot, stakeholder or Member State actor. Shared information can include IoCs, reports, recommendations, evidence references, incident notes or secure exchange artefacts. The KPIS is calculated as: number of events where information was shared divided by total relevant events, multiplied by 100. **Partners/Tools: BYTE - blockchain; IANUS- MISP, MAG (Anomaly Detector) /pilot/use case leaders.**

3.6 Objective 6

Foster greater collaboration and knowledge sharing among stakeholders in the cybersecurity ecosystem utilizing advanced technologies by enabling real-time information exchange and joint exercises, aiming the MS to learn from each other's experiences and collectively improve their cybersecurity capabilities.

Related modules: CYRESCUE, CYBERRA, CROSS-CORE

Verification: D3.3, D3.4, D4.3, D8.2, D8.4, final KPIs consolidation in D1.5

© CYberSynchrony, 2026

Table 8 Objective 6 KPIs

KPI ID / name	Description	KPI Owner	Verification means	Target	Measurement Methodology
KPI6.1 Number of Penetration Tests Provided	***This KPI is a duplication of KPI2.1***				
KPI6.2 Number of Threat Assessments Carried Out	***This KPI is a duplication of KPI1.1***				
KPI6.3 Number of Risk Scenario Analyses Carried Out	***This KPI is a duplication of KPI1.2***				
KPI6.4 Vulnerabilities Addressed	***This KPS is a duplication of KPI4.3***				
KPI6.5 Threat Intelligence Platform Security	***This KPI is a duplication of KPI 1.5***				

3.7 Objective 7

Enhance early detection and response to cyber incidents by leveraging Advanced threat intelligence and analytics while reducing the impact of potential cyber threats on critical infrastructure and essential entities.

Related modules: CYBERRA, CYBRITE, CROSS-CORE

Verification: D6.5, D8.2 , final KPIs consolidation in D1.5

Table 9 Objective 7 KPIs

KPI ID / name	Description	KPI Owner	Verification means	Target	Measurement Methodology
KPI7.1 Number and Nature of Vulnerabilities Discovered	***This KPI is treated as a duplicate of KPI3.4/KP4.4***				
KPI7.2 Vulnerabilities Addressed	***This KPI is treated as a duplicate of KPI4.3/KP6.4***				

3.8 Objective 8

Implement cybersecurity awareness campaigns and educational programs targeting citizens, businesses, and organizations while fostering a culture of cybersecurity awareness and best practices across all levels of society.

Related modules: CYBERWISE

Verification: D8.2 , D1.5 final KPIs consolidation

© CYberSynchrony, 2026

Table 10 Objective 8 KPIs

KPI ID / name	Description	KPI Owner	Verification means	Target	Measurement Methodology
KPI8.1 Cybersecurity Training Coverage	Measure the proportion of in-scope entities that have completed and recorded participation in cybersecurity awareness training programs.	MER	D8.2 (EGL)	cybersecurity training coverage minimum 85%	**Use Training Attendance Register and Post-training Questionnaire/Test:** The Cybersecurity Awareness Rate will be measured as the percentage of in-scope entities that have successfully completed an approved cybersecurity awareness training program within a defined reporting period. It is calculated by dividing the number of entities with recorded completion of CYberSynchrony awareness training by the total number of eligible entities required to complete the training, and multiplying the result by 100. Completion is determined based on validated training records by MER. To do so, eBOS will collect from each Use Case the eligibility numbers prior to the trainings and calculate after the trainings the awareness rate of each pilot organization. Evidence should include attendance lists, training exports, participant categories, completion status . **Partners/Tools:** Use Case Planning Leader (eBOS) provided guidance on the KPIS approach. Leader on Training (MER) collected the number of eligible participants required to complete CYberSynchrony training by each in-scope entity (AMC, EGL, UPRC) and will track the participation

© CYberSynchrony, 2026

					numbers (keep training records) of each provided training.
KPI8.2 Cybersecurity Awareness Index	Measure the level of cybersecurity awareness among citizens and organisations based on surveys and assessments.	EBOS	D8.2 (EGL)	Achieve a cybersecurity awareness index of 75	Use the **Cybersecurity Awareness Index** that will measure the level of cybersecurity awareness among CyberSynchrony training participants in healthcare, public administration, and university sectors by using a risk-based questionnaire administered **before and after training**. Each response is converted into a numerical risk score, where higher scores indicate more insecure behaviour and therefore lower awareness. Individual risk scores are aggregated and normalised on a 0–100 scale, and the CAI is derived as the inverse of the risk score (CAI = 100 − R), meaning that lower risk corresponds to higher awareness. The change between pre- and post-training results (ΔCAI = CAI_post − CAI_pre) is used to evaluate training effectiveness, while sectoral and overall results are calculated as average CAI values across participants. The KPIS

© CYberSynchrony, 2026

					target is defined as achieving a post-training CAI of at least 75 (means 25% reduction of risk), indicating a satisfactory level of cybersecurity awareness and reduced risk behaviour across the programme. CAI < 50 → Low awareness / high-risk behaviour CAI 50–74 → Moderate awareness CAI ≥ 75 → Target awareness level achieved CAI ≥ 85 → Advanced cybersecurity awareness maturity. **Partners/Tools:** Use Case Planning Leader (**eBOS**) provided guidance to the Use Case Leaders on the questionnaire initiation, and monitors the progress from design to execution of the KPIS. Use Case Leaders (A**MC, UPRC, EGL**) designed the questionnaires and shared with consortium partners for review and feedback. TRUST provided specific feedback and guidance to the use case leaders for final refinement. Pre-training questionnaires are planned to distributed within May-June 2026. Once the gaps identified through Training Needs Analysis by MER, **MER** will proceed with the design of the training programs tailored to the needs of each participant organisation. On the completion of the trainings a post-evaluation questionnaire will be distributed again to the participants.

3.9 Objective 9

© CYberSynchrony, 2026

Ensure a consistent and high level of security across all MS by applying comprehensive cybersecurity policies and regulations while actively disseminate and communicate these standards and practices to ensure widespread adoption, foster collaboration with key stakeholders for effective policy contribution, exploitation, and standardization efforts and leverage the latest technologies and platforms to facilitate information exchange, knowledge sharing, and cybersecurity training across all sectors, enhancing the overall resilience and governance in cybersecurity throughout the MS.

Related modules: CYBERGOPLUS

Verification: D6.7, D6.8, D8.3, D9.5, D9.6, D9.7, final KPIs consolidation in D1.5

Table 11 Objective 9 KPIs

KPI ID / name	Description	KPI Owner	Verification means	Target	Measurement Methodology
KPI9.1 Policy Awareness and Compliance Readiness Rate	Measure stakeholder awareness of compliance and readiness to align with EU cybersecurity policies, regulations and standards through CYberSynchrony policy guidance.	KETYAK	D9.7	Increase policy awareness of compliance rate by: 30 completed feedback surveys on the Policy Toolkit, 1 policy workshop/webinar organised, and 100 downloads/views of D6.7 Cybersecurity Policy Toolkit.	The KPI will be considered achieved when: (a) 30 completed **feedback surveys on the Policy Toolkit** (linked to pr. Website); (b) 1 dedicated **workshop/webinar or awareness session** is organised; and (c) **100 downloads/views of the Policy Toolkit** are recorded **(analytics from pr. Website)**. Evidence will include survey responses, event agenda, attendance list, dissemination records, download statistics and website analytics. INDICATIVE QUESTIONNAIRE: e.g Q1. Have you viewed the CYberSynchrony Cybersecurity Policy Toolkit (D6.7)? • Yes • No Q2. Does your organisation intend to adopt or align at least one cybersecurity policy, practice or recommendation described in the

					CYberSynchrony Policy Toolkit? • Yes • No Partners involved: **KETYAK (methodology and policy guidance), EBOS (dissemination and communication activities, toolkit access and analytics & event organisation), MAG (stakeholder engagement and policy contribution activities), IANUS (contribution to Cybersecurity Policy Toolkit and assessment of operationalization of adopted policies)**
KPI9.2 Industry-specific Standard Adoption	Track adoption of industry-specific cybersecurity standards and best practices by participating critical sectors.	IANUS	D6.8, D8.3	≥65% adoption rate	**Survey and assess adoption rate of cybersecurity standards in various industries.** An assessment will be conducted at per the adoption of industry specific standards and best practices (NIS2 covered critical sectors in the EU). This will provide the baseline of the KPIS. Regarding the "increase rate to 65%", this will depend on the UC participants and their adoption of our platform; inasmuch, if we can achieve adoption of the platform of 2 out of 3 UC participants, we will ensure and justify the adoption of best practices and standards at 66.6%
KPI9.3 Cybersecurity Certification Awareness Rate	KPI9.3 has been removed from the active KPIs framework because formal cybersecurity certification attainment is outside the direct scope and control of the project. CYberSynchrony does not provide certification services, conduct certification audits, or				

	control external certification timelines and decisions. The related objective is partially addressed through KPI9.2, which focuses on adoption of cybersecurity standards, best practices and CYberSynchrony recommendations.				
KPI9.4 Engagement in Dissemination and Communication Activities	Track participation and engagement in dissemination and communication activities.	EBOS	D9.1, D9.3, D9.5	≥30% annual increase in events	Count dissemination and communication activities annually and compare against the previous year. KPIs= ((Events current year − Events previous year) ÷ Events previous year) × 100.
KPI9.5 Stakeholder Engagement in Policy Contribution	Track stakeholder participation in policy contribution and policy recommendation activities.	MAG	D9.5, D9.7	≥50 new stakeholders for policy input within 3 years	Use a **Stakeholder Registry** to track policy engagement. **Policy white papers, briefs and 3–5 evidence-based recommendations will be shared with at least 50 stakeholders** through outreach emails, posts, project events, workshops, webinars, roundtables and policy sessions. Evidence will include the registry, distribution records, attendance lists, event reports and copies/links of policy outputs.. **Partners: MAG,EBOS with the assistance of KETYAK (Policies)**
KPI9.6 Exploitation of CYberSynchrony Best Practices	Track exploitation and adoption of CYberSynchrony best practices.	BYTE	D9.6	Reach 60% adoption of CYberSynchrony best practices within 3 years	**Final-year exploitation questionnaire** distributed to pilots, FSTPs and stakeholders. KPIS = (Number of respondents reporting adoption or planned adoption ÷ Total respondents) × 100.

Duplicated indicators are now monitored through their primary KPIs, while their contribution to the relevant objectives remains cross-referenced.

© CYberSynchrony, 2026

4 Use Case KPIs: M24 Status

Each pilot use case is led by a pilot organisation and supported by consortium technical partners. By M24, all use cases have defined their KPIs scenarios, aligned measurement methodologies with technical partners, and commenced baseline data collection in preparation for the full pilot deployment phase beginning at M26.

4.1 UC1 – Digital Healthcare: KPIs Status

Use Case 1 is led by Apostolos Loukas Medical Center (AMC) and focuses on demonstrating comprehensive cybersecurity for digital healthcare environments, including EHR/EMR systems, medical devices (IoMT), and clinical communications infrastructure.

Table 12 UC1 – Healthcare KPIs

KPI #	KPI Name	Target	CYberSynchrony Modules	Status M24
UC1.KPI1	**Data Encryption**	100% of successful data encryption implementation to 80% of outgoing exported patient sensitive data.	CROSS-CORE, CYBERGOPLUS	AMC has identified and classified the patient data into sensitive and non-sensitive. Also, has identified the current, specific outgoing exported datasets and performed a baseline counting of those. Target was, then redefined in order to reflect the AMC infrastructure needs and internal proceduresto 100% encryption of all outgoing exported data (Target updated from its original formulation in D1.3).
UC1.KPI2	**Training in Cybersecurity Best Practices**	30 healthcare staff trained in cybersecurity best practices compared to current staff with no training	CYBERWISE	A pre- and post- training questionnaire was prepared by UC lead and reviewed by TRUST as a peer-reviewer, and by eBOS as the QA reviewer. The email repository of the participants has been completed by the organisation, so CYberSynchrony technical team will proceed in July 2026 sharing the questionnaires with the training participants (staff). The IT department of AMC also completed the cybersecurity readiness

© CYberSynchrony, 2026

				assessment of CYBERWISE module named trustSense, collected and evaluated the responses for the appropriate design of the trainings, which will be developed by MER
UC1.KPI3	**Audit Frequency & Critical Findings**	Increase audit frequency to annually with a 50% reduction in critical findings during the Pilot implementation using CYberSynchrony platform	CYBERRA, CYBERGOPLUS	The status of the performed audits has been identified which defined the baseline. Specifically, no annual or bi-annual audits are in place for AMC, which means that CYberSynchrony will enhance the posture of audits execution with a sustainability plan onwards. FP will conduct a penetration test before and after CYberSynchrony module implementation to measure reduction in critical findings.
UC1.KPI4	**Detection and Response Time**	Achieve a 60% reduction in detection and response time compared to average time taken in past incidents	CYBRITE, CYRESCUE, CYBERRA	Baseline establishment in progress. No prior documentation of incidents exists at AMC; historical baseline being constructed.

4.2 UC2 – Public Administration: KPIs Status

Use Case 2 is led by the Municipality of Egaleo (EGL) and focuses on securing public administration digital services, including the MAESTRO e-government platform, citizen data registries, and internal communications infrastructure.

Table 13 UC2 - Public Administration KPIs

KPI #	KPI Name	Target	CYberSynchrony Modules	Status M24
UC2.KPI1	**Number of Incidents**	Decrease the number of cybersecurity incidents detected and resolved by 20%	CYRESCUE, CYBRITE	Scenario definition agreed and aligned with technical partners. Scenario includes Controlled phishing attack leading to account compromise and suspicious activity within the MAESTRO environment. Baseline and

© CYberSynchrony, 2026

		compared to the past situation		pilot measurement methodologies defined, well as the exact scenarios/ Experiments. Required tools and responsibilities identified.[1]
UC2.KPI2	**Response Time**	Decrease the time taken to respond to a cybersecurity incident by 20% compared to the current average time	CYBRITE, CYBERWISE	Same as UC2.KPIS1
UC2.KPI3	**Staff Compliance Rates**	Staff compliance rates with new cybersecurity protocols increased to 95% compared to the current rate of compliance	CYBERWISE	A pre- and post- training questionnaire was prepared by UC lead and reviewed by TRUST as a peer-reviewer, and by eBOS as the QA reviewer. The email repository of the participants has been completed by the organisation, so CYberSynchrony technical team will proceed in July 2026 sharing the questionnaires with the training participants (municipality policy officers). The IT department of EGL also completed the cybersecurity readiness assessment of CYBERWISE module named trustSense. eBOS collected the outcomes and MER evaluated them for the appropriate design of the trainings
UC2.KPI4	**Integrity Protection and Monitoring of Municipal Incident Records**	Increase the proportion of municipal incident records whose integrity can be verified and monitored by 30% compared to baseline conditions.	CYRESCUE, CYBERRA, CROSS-CORE	The UC2.KPI4[1] was renamed and target redefined based on the exact capacities and functionalities of the MAESTRO platform, as well as the needs EGL infrastructure for sustainable cybersecurity tools adoption. Then, Scenario definition agreed and aligned with technical partners, which includes a Controlled account compromise scenario leading to unauthorized modification or deletion of incident records within the MAESTRO environment. Baseline and pilot measurement methodologies

[1] Referenced in 8.1 - Confirmed Deviations

© CYberSynchrony, 2026

				defined. Required tools, modules and partner responsibilities identified.

4.3 UC3 – Higher Education: KPIs Status

Use Case 3 is led by the University of Piraeus Research Center (UPRC) and focuses on strengthening cybersecurity across university IT infrastructure, research networks, and learning management systems through deployment and testing of CYberSynchrony security modules in a real academic environment.

Table 14 : UC3 – Higher Education KPIs

KPI #	KPI Name	Target	CYberSynchrony Modules	Status M24
UC3.KPI1	**Number of Incidents**	Number of cybersecurity incidents detected and resolved decreased by 20% post-implementation	CYBERWISE	Extracting historical incident data to formalize pre-pilot baselines for KPIs UC3.KPI1 and UC3.KPI4. A voluntary opt-in campaign for the Phishing Simulation Scenario has been finalized, 117 participants from the University of Pireus. The phishing campaign has concluded, collected the outcomes of the exercise and TRUST performed hands-on training for cybersecurity topics focusing on phishing campaigns awareness and cyber hygiene practices.
UC3.KPI2	**Faculty Compliance Rates**	Faculty compliance rates with new cybersecurity protocols achieve 90% compliance post-training and awareness campaigns	CYBERWISE, CYBERGOPLUS	A pre- and post- training questionnaire was prepared by UC lead and reviewed by TRUST as a peer-reviewer, and by eBOS as the QA reviewer. The email repository of the participants is under development (it is an opt-in-based collection of emails for this scenario for data protection reasons). The IT department of UPRC also completed the cybersecurity readiness assessment of CYBERWISE module named trustSense. eBOS collected the outcomes and MER evaluated them for

© CYberSynchrony, 2026

				the appropriate design of the trainings. The training aim to focus on policy and cybersecurity infrastructure enhancement of UPRC. Post implementation of CYBERGOPLUS Policy Tool kit the defined cohort of faculty members will be evaluated for their compliance.
UC3.KPI3	**Student Cybersecurity Satisfaction**	Student satisfaction rates with new security of online services achieve 90% satisfaction post-enhancements	CYBERWISE	A pre- and post- training questionnaire was prepared by UC lead and reviewed by TRUST as a peer-reviewer, and by eBOS as the QA reviewer. The email repository of the participants is under development (it is an opt-in-based collection of emails for this scenario for data protection reasons). The questionnaires will be distributed to the students opted-in for training, then training will be developed based on the identified gaps and outcomes of UC3.KPI2. Finally, post-training evaluation will be performed, including questions on students' satisfaction after the UPRC enhancements supported by CYberSynchrony module.
UC3.KPI4	**Response Time**	Time taken to respond to cybersecurity incident reduced by 30% post SOAR platform deployment	CYBRITE CYRESCUE	The Isolated NOC Simulation Lab has been configured by the UPRC Network Administrator. Scenario definition agreed and aligned with technical partners, which includes extracting historical incident data to formalize pre-pilot baselines for Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). Methodologies and pilot execution plan has been defined.

© CYberSynchrony, 2026

4.4 Open Call KPIs

The Open Calls are expected to contribute to selected project KPIs, including

- Number of penetration tests provided
- Number of essential entities supported
- Number of threat assessments / risk scenario analyses carried out
- Number of risk monitoring services provided
- Number of potential users covered per test / exercise
- Number and nature of vulnerabilities discovered
- Number of cross-border actions / exercises

Some Open Calls have identified additional KPIs that will be also further explored.

To ensure consistent verification, Open Call beneficiaries will use a dedicated KPIs evidence template, reporting the activity performed, tool/method used, measured result, evidence provided, date of evidence, issues/deviations and next planned action. This Template will be included in D1.5 together with the consolidated results.

© CYberSynchrony, 2026

5 Key Exploitable Results (KERs): Update

This section presents the updated portfolio of Key Exploitable Results (KERs) for the CYberSynchrony project as of M24. Three new KERs have been added compared to the D1.3 baseline: the Open Call Methodology, the CYberSynchrony Architecture/Framework, and the Training Needs Analysis (TNA) Methodology. The consortium has adopted a tiered exploitation strategy: the original knowledge creator retains rights to their findings while sharing software execution capabilities with the full consortium. KERs are made accessible as open-source community versions for academic and research communities, while other outcomes provide commercial opportunities for consortium members.

Table 15 below provides an overview of all 16 KERs. Table 15 details the exploitation plans and benefits by partner. Final KER development and updates will be provided in D9.6 Final report on exploitation and sustainability in M36.

Table 15 KER Overview

KER	Module	Consortium Members	Type	Lic.	Svc. Type	Time to Market
Core Platform						
CYberSynchrony Platform	Full Platform	All	S	CO	S, C, E	1–2 yrs post-project
CYRESCUE						
CYRESCUE – Advanced Penetration Testing Tools	CYRESCUE	MAG, EBOS, FP, BYTE, MER	S	CO	S, T, C, E	1–2 yrs post-project
CYRESCUE – SOAR Platforms	CYRESCUE	MAG, EBOS, FP, BYTE, MER	PR	SaaS	S, T, C, E	1–2 yrs post-project
CYBERRA						
CYBERRA – Immutable Forensic Analysis Techniques	CYBERRA	MAG, EBOS, IANUS, FP, BYTE, MER	PR	OA	S, T, C, E	1–2 yrs post-project
CYBERRA – Customized Risk Assessment Software	CYBERRA	MAG, EBOS, IANUS, FP, BYTE, MER	P	C	S, T, C, E	1–2 yrs post-project
CYBRITE						
CYBRITE – Advanced Cybersecurity Analytics Tools	CYBRITE	MAG, IANUS, TRUST, UPRC, FP, BYTE	P	C	S, T, C, E	1–2 yrs post-project
CYBRITE – SIEM Systems and Network Traffic Analysis Tools	CYBRITE	MAG, IANUS, TRUST, UPRC, FP, BYTE	P	CO	S, T, C, E	1–2 yrs post-project
CROSS-CORE						

© CYberSynchrony, 2026

CROSS-CORE – Standardized Data Sharing Formats	CROSS-CORE	MAG, IANUS, TRUST, BYTE, MER	S	S	S, T, C, E	1–2 yrs post-project
CYBERWISE						
CYBERWISE – Awareness Platforms with Gamification	CYBERWISE	All, FP	S	SaaS	T, C	1–2 yrs post-project
CYBERWISE – Awareness Training Initiatives	CYBERWISE	All	T	OA	T, C	1–2 yrs post-project
CYBERGOPLUS						
CYBERGOPLUS – Compliance Monitoring and Auditing Tools	CYBERGOPLUS	All	P	C	S, T, C, E	1–2 yrs post-project
Cross-cutting						
Cross-border Cyber Exercise Programs	CYRESCUE, CROSS-CORE	All	S	SaaS	S, T, C, E	1–2 yrs post-project
Customized Cybersecurity Solutions	Multiple	IANUS, TRUST, DSA, KETYAK, FP, BYTE, EGL, MER	S	SaaS	S, T, C, E	1–2 yrs post-project
Open Call Methodology	Multiple	All	PR	OA	S, T, C, E	During/after project
CYberSynchrony Architecture / Framework	Full Platform	All	S	OA	S, C, E	During/after project
Training Need Analysis (TNA) Methodology	CYBERWISE	EBOS, TRUST, IANUS	PR	OA	T, C	During/after project

Table 16 KER Exploitation Plans and Benefits by Partner

KER	Key Exploitation Plans and Benefits (by Partner)
Core Platform	
CYberSynchrony Platform	MAG: public sector service offer. EBOS: hosted on EBOS GitLab/Kubernetes. FP: modular cybersecurity portfolio for critical entities. KETYAK: CYBERGOPLUS Policy Toolkit integrated. EGL: municipal cybersecurity framework. DSA: centralised national CII oversight platform.
CYRESCUE	

© CYberSynchrony, 2026

CYRESCUE – Advanced Penetration Testing Tools	FP: offensive security and red-team services; incorporated into cyber range attack-chain simulations. UPRC: undergraduate penetration testing courses. DSA/CSIRT-CY: national red-teaming and vulnerability assessments on critical infrastructures.
CYRESCUE – SOAR Platforms	FP: SOC workflow automation (alert triage, escalation, post-incident analysis) in cyber range. UPRC: undergraduate and cybersecurity graduate programmes. DSA/CSIRT-CY: automate national incident response and threat containment.
CYBERRA	
CYBERRA – Immutable Forensic Analysis Techniques	IANUS: MISP as forensic repository with blockchain integrity layer for traceable post-incident reporting. FP: evidence integrity in incident investigation and exercise debriefing. BYTE: strengthen e-government and smart-border trusted-exchange offers. DSA: national risk assessment frameworks and early warning advisories.
CYBERRA – Customized Risk Assessment Software	IANUS: MISP-based sector-tailored risk assessment for SMEs, public admins, and critical infrastructure; future integration with OpenVAS, TheHive, Cortex. FP: cybersecurity consulting for SMEs and critical entities. UPRC: undergraduate and graduate training. DSA: national threat advisory dissemination.
CYBRITE	
CYBRITE – Advanced Cybersecurity Analytics Tools	MAG: AI Anomaly Detector for critical infrastructure clients. IANUS: AI-augmented SOC services (Wazuh/Suricata + OpenAI reasoning module). FP: cyber range anomaly detection and UBA exercises. BYTE: AI-enhanced detection in security projects. UPRC/TRUST: telecom security and risk management training. DSA: national monitoring for zero-day and systemic threats.
CYBRITE – SIEM Systems and Network Traffic Analysis Tools	IANUS: Wazuh/Suricata hybrid SIEM/IDS with OpenAI event interpretation; affordable managed security service. FP: SOC-oriented training, threat hunting, blue-team exercises. BYTE: enhanced IDS/IPS and SIEM services. UPRC: telecom security and graduate programmes.
CROSS-CORE	
CROSS-CORE – Standardized Data Sharing Formats	BYTE: reusable interoperability assets; increased market potential of BYTE products. DSA: encrypted cross-border threat intelligence sharing; mutual assistance with EU Member States and CSIRTs Network.
CYBERWISE	
CYBERWISE – Awareness Platforms with Gamification	IANUS: translate MISP/Wazuh/Suricata results into NIS2 and cyber hygiene awareness content (ENISA ECSF, CyberHot 2025/2026). FP: expand training for non-technical users and SME staff. EGL: municipal awareness initiatives. DSA: national cybersecurity education campaigns across public sector and general public.
CYBERWISE – Awareness Training Initiatives	EBOS: TNA methodology published as open best practice. FP: incorporate into training portfolio for SMEs, public bodies, and critical-sector personnel. TRUST: SME training advancement. EGL: staff training programmes. KETYAK: policy-maker training.
CYBERGOPLUS	
CYBERGOPLUS – Compliance	IANUS: NIS2/GDPR/DORA compliance services for SMEs and critical infrastructure, supported by Wazuh/Suricata/MISP evidence. FP: compliance consulting and audit

© CYberSynchrony, 2026

Monitoring and Auditing Tools	preparation for clients. KETYAK: integrates Policy Toolkit; facilitates EU regulatory alignment. EGL: municipal compliance monitoring. DSA: NIS2 regulatory audits and enforcement across Cyprus essential entities.
Cross-cutting	
Cross-border Cyber Exercise Programs	FP: extend cyber range offer to multi-actor, multi-country preparedness scenarios. UPRC: cybersecurity labs. KETYAK: policy-maker training exercises. EGL: improve municipal preparedness and coordination with external stakeholders.
Customized Cybersecurity Solutions	FP: tailored assessments, training packages, and resilience-building services for SMEs and critical entities. TRUST: maritime and health sector cybersecurity solutions. EGL: sector-specific solutions for municipal operations.
Open Call Methodology	Replicable evaluation framework for FSTP beneficiaries. TRUST: applied to maritime and health sector open call outcomes. Consortium-wide: model for future EU innovation ecosystems.
CYberSynchrony Architecture / Framework	Overarching interoperability blueprint (APIs, data models, deployment patterns) enabling third parties and FSTP beneficiaries to replicate or extend the platform. Reference implementation for modular, scalable cybersecurity platforms across sectors and Member States.
TNA Methodology	EBOS: publicly shared as best-practice TNA resource for cybersecurity awareness programmes. TRUST: applied to maritime and health sector training. IANUS: align CYBERWISE content with Wazuh/Suricata/MISP threat intelligence findings.

© CYberSynchrony, 2026

6 KPIs Summary Table

The following table consolidates all 25 Objective KPIs with their targets and M24 status. Duplicate KPIs entries (KPI3.1, KPI3.2, KPI3.5, KPI4.1, KPI4.4, KPI6.1–KPI6.5, KPI7.1, KPI7.2) are tracked under their primary entries and are not repeated here.

Table 17 KPIs Dashboard Summary

KPI ID	KPI Name	Target	M24 Status
KPI1.1	Number of Threat Assessments Carried Out	>36 threat assessments	In progress – pilot deployments commencing M25/M26 (June/July 2026). Data collection via Threat Assessment Register. Partial contributions expected from Open Call 1.
KPI1.2	Number of Risk Scenario Analyses Carried Out	>=13 risk scenario analyses	In progress – 4–5 scenarios per use case being defined. Risk Scenario Register established. Expected evidence via D8.2 and D3.4.
KPI1.3	Threat Intelligence Platform Effectiveness	>85% detection & mitigation rate	Methodology finalised. Threat Effectiveness Test Log defined. Validation exercises planned with pilot environments during M25–M30.
KPI1.4	CYberSynchrony Platform Usability (SUS)	SUS > 70%	SUS questionnaire drafted by EBOS. Distribution planned for end of use cycle (approx. December 2026). Applicable to UC participants and FSTP beneficiaries.
KPI1.5	Threat Intelligence Platform Security	Avg. remediation time ≤15 days	Platform Vulnerability Register established. Tools (ASA, Wazuh, Suricata, Snyk) actively monitoring. Measurement to be consolidated in D3.3.
KPI1.6	Platform Security Incident Response Time	Zero-day ≤4h; Others ≤8h	Incident/Response Register methodology defined. Simulated incident exercises to be conducted during pilot phase (M25–M30).
KPI2.1	Number of Penetration Tests Provided	6 penetration tests	In progress – SBS and PTA toolset deployed. Target revised from original 60 to 6 (3 consortium use cases). FP leading with AMC (×2), EGL (×1) planned.
KPI2.2	Incident Detection Time	Average ≤3 days	Incident Detection Time Register established. Detection tool stack active (Wazuh, Suricata, Anomaly Detector, Kitsune). Results expected during pilot exercises M25–M30.
KPI2.3	Incident Response Time	Average ≤15 days	Incident/Response Register methodology defined. DCO Playbooks being integrated with pilot environments. Results expected M25–M30.
KPI2.4	Incident Resolution Rate	≥80% within 24 hours	Methodology aligned with Incident/Response Register. Evidence collection framework in place. Measurement during pilot exercises.

© CYberSynchrony, 2026

KPI3.3	Potential Users Covered per Test/Exercise	Average 150 users/exercise	Partial results available: IANUS – 29 participants; MAG – 53 participants; UPRC 117 participants. Total 199. Full results in D6.5/D1.5.
KPI3.4	Number and Nature of Vulnerabilities Discovered	15% reduction in high-severity vulns.	Vulnerability Register structure established. ASA, PTA, SBS, Wazuh, trustPhish contributing findings. Baseline comparison methodology defined.
KPI3.6	Risk Scenarios Analysed	≥12 customised scenarios; +15% YoY	Risk Scenario Register established by MER/Kitsune. Scenario planning in progress across pilots. Results expected in D5.4.
KPI3.7	Risk Mitigation Index	≥20% reduction in identified risks	Before/after risk scoring methodology defined. Initial scores being established during pilot risk assessments. Results expected in D3.4.
KPI4.2	Number of Cross-Border Actions/Exercises	10 cross-border actions/exercises	Cross-Border Exercise Register established by BYTE. Hyperledger Fabric infrastructure operational. Joint exercises being planned with DSA, KETYAK, and pilot partners.
KPI4.3	Vulnerabilities Addressed	≥80 vulnerabilities addressed	Vulnerability Remediation Register in use. ASA (FP) primary tool for tracking. Remediation activities progressing across use cases.
KPI4.5	Incident Collaboration Index	≥70% collaboration index	Survey instrument designed. Cross-border exercises to feed this KPIS. Results expected post-exercise analysis in D5.4.
KPI5.1	Number of Risk Monitoring Services Provided	25 services; ≥95% satisfaction; <5% FP rate	Monitoring setups active: Wazuh endpoint groups, Suricata segments, Kitsune profiles, MISP feeds, Anomaly Detector deployments. Service inventory being maintained by MER.
KPI5.2	Information Sharing Frequency	≥75% of incidents with info sharing	Information Sharing Log established. BYTE blockchain infrastructure operational for secure exchange. MISP IoC sharing active via IANUS.
KPI8.1	Cybersecurity Training Coverage	≥85% training coverage	Training Needs Analysis by MER in progress. Eligibility numbers being collected from AMC, EGL, UPRC. Training programmes being designed by MER. Results expected in D8.2.
KPI8.2	Cybersecurity Awareness Index (CAI)	Post-training CAI ≥75	Pre-training questionnaires designed by AMC, UPRC, EGL (reviewed by TRUST). Distribution planned May–June 2026. Post-training questionnaires to follow completion of MER-designed training sessions.
KPI9.1	Policy Awareness and Compliance Readiness Rate	Increase policy awareness of compliance rate	D6.7 Cybersecurity Policy Toolkit (v2) methodology published. KPI9.1 will be measured through 30 completed Policy Toolkit feedback surveys, 1 policy

© CYberSynchrony, 2026

		by: 30 completed feedback surveys on the Policy Toolkit, 1 policy workshop/webinar organised, and 100 downloads/views of D6.7 Cybersecurity Policy Toolkit.	awareness webinar/workshop, and 100 recorded Toolkit downloads/views using project website/platform analytics.
KPI9.2	Industry-specific Standard Adoption	≥65% adoption rate	Assessment methodology defined in D6.8. Target achievable at 2/3 UC adoption (66.6%). Assessment activities ongoing.
KPI9.3	**KPIS9.3 – Removed from active KPIS framework** Certification attainment is outside project scope; objective partially covered by KPIS9.2.		
KPI9.4	Engagement in D&C Activities	30% annual increase in events	ACHIEVED – 56% increase from M12 to M24. D&C Tracker maintained by EBOS. Target set for Year 3: additional 30% increase.
KPI9.5	Stakeholder Engagement in Policy Contribution	≥50 new stakeholders in 3 years	Stakeholder Registry operational. Policy engagement activities ongoing. White paper with best practice recommendations in development. ENISA policy workshop planned.
KPI9.6	Exploitation of CYberSynchrony Best Practices	60% adoption within 3 years	Exploitation questionnaire under development. Distribution planned for final project year to pilots, FSTPs, and associated stakeholders.

Communication and Dissemination KPIs

The table below presents the Communication and Dissemination KPIs performance comparing M12 vs M24 status.

Table 18 Communication and Dissemination KPIs – M12 vs M24

KPI ID	KPI Name	Target	Status M12	Status M24
C.1.1	Project website (M03–6 years)	Published by M03	1.7K Objective users	3.6K Objective users
C.2.1	Social Media Followers by M36	>1,000	176	321
C.2.2	Average Monthly Impressions	>500	618	2,406
C.3.1	Newsletters	>10	1	5

© CYberSynchrony, 2026

C.3.2	Total Contacts on Mailing List	>1,000	52	249
C.4.1	Press Releases	≥12	4	39
C.4.2	Published Articles (newspapers/online)	≥10	0	4
C.5.1	Objective Blog Publications	>10	0	12
C.5.2	Different Platforms for Posting	>4	0	8
C.6.1	Printed Materials (brochures, flyers)	>3,000	0	550
C.6.2	Display Banners	>3	1 roll-up	4 (1 poster, 1 roll-up, 1 fact sheet, 1 leaflet)
C.7.1	Produced Videoclips	3	0	5
C.7.2	Video Views	>10,000	0	766
C.7.3	Conducted Interviews	>6	0	7
C.8.1	Public Events at Universities	>3 (>60 participants)	4	5 (>100 each)
C.8.2	University Open Days	>3	1	2
C.8.3	Events by Local Entities/Stakeholders	>4 (>120 participants)	2	4 (>150 each)
D.1.1	Use Case-based Workshops	3	0	0 (planned H2 2026)
D.1.2	Training Program	1	0	3
D.1.3	Showcases	>2	1	0 (additional planned)
D.1.4	Webinars	>6 (>40 participants each)	1	6 (25–50 participants each)
D.1.5	Exhibitions/Trade Fairs/Symposiums	>3	0	4
D.2.1	Scientific Papers	>6	3	10
D.2.2	Presentations at Scientific Conferences	>6	2	8
D.3.1	High-Impact Communities to Push Results	>2	0	4
D.4.1	Standardisation Contributions to SDOs	>1	0	2

© CYberSynchrony, 2026

7 M12 vs M24 Comparison (D1.3 vs D1.4)

This chapter provides a systematic comparison between the KPIS framework established in D1.3 (M12 baseline) and the updated framework presented in D1.4 (M24). It documents changes to targets, measurement methodologies, and progress status, enabling the consortium to assess the trajectory of KPIs achievement.

Table 19 M12 vs M24 KPIs Comparison

KPI ID	KPI Name	D1.3 Target (M12)	D1.4 Status (M24)	Change / Notes
KPI1.1	Threat Assessments	>36 (methodology defined, no data)	In progress – pilots commencing M25/M26	Target unchanged. Measurement methodology significantly enhanced with Threat Assessment Register and Anomaly Detector integration.
KPI1.2	Risk Scenario Analyses	≥13 (methodology defined)	In progress – 4–5 scenarios per UC being defined	Target unchanged. Evidence requirements and scenario structure formalized.
KPI1.3	Platform Effectiveness	>85% (no data yet)	Methodology finalized; validation planned M25–M30	Methodology enhanced with Anomaly Detector contribution calculation.
KPI1.4	Platform Usability	≥4.5/5 MOS	Revised to SUS >70% (industry standard)	Measurement method changed from MOS to standardized SUS scale. More robust and comparable.
KPI1.5	Vulnerability Remediation Time	≤15 days (methodology defined)	Platform Vulnerability Register established; monitoring active	Target unchanged. Detailed toolchain and workflow defined.
KPI1.6	Incident Response Time	Zero-day ≤4h; Others ≤8h	Incident/Response Register defined; simulations planned	Target unchanged. Blockchain-based evidence preservation (BYTE) added.
KPI2.1	Penetration Tests Provided	≥60 (over-ambitious)	Revised to 6 targeted penetration tests	Target significantly revised downward to reflect feasible scope (3 use cases × 2 tests). Original 60 was infeasible.
KPI2.2	Incident Detection Time	Reduce to 3 days avg.	Register defined; detection tools active	Target unchanged. Measurement methodology formalized with tool stack.
KPI2.3	Incident Response Time	Reduce to 15 days avg.	Methodology defined; DCO Playbooks integrating	Target unchanged. Response initiation criteria clearly defined.
KPI2.4	Incident Resolution Rate	≥80% within 24h	Methodology defined; evidence framework in place	Target unchanged. Evidence types clarified.
KPI3.3	Users Covered per Exercise	150 users/exercise avg.	IANUS: 29; MAG: 53; UPRC: 117 TOTAL: 199	Partial results available. Additional campaigns planned. Full count in D6.5/D1.5.
KPI3.4	Vulnerabilities Discovered	15% reduction vs. others	Vulnerability Register active; baseline being set	Target unchanged. TRUST trustPhish added as tool contribution.
KPI3.6	Risk Scenarios Analysed	≥12; +15% YoY	Register established; scenario planning in progress	Target unchanged. Year-over-year tracking methodology formalized.

© CYberSynchrony, 2026

KPI3.7	Risk Mitigation Index	≥20% risk reduction	Scoring methodology defined; initial scores in progress	Target unchanged. Likelihood × Impact formula standardized (1–5 scale).
KPI4.2	Cross-Border Actions/Exercises	10 exercises	Register established; exercises being planned	Target unchanged. Blockchain evidence layer (BYTE) added to evidence requirements.
KPI4.3	Vulnerabilities Addressed	≥80 vulnerabilities	Remediation Register active	Target unchanged. Criteria for 'addressed' status formally defined.
KPI4.5	Incident Collaboration Index	≥70% index	Survey instrument designed	Target unchanged. Survey methodology formalized.
KPI5.1	Risk Monitoring Services	25 services; 95% satisfaction; <5% FP	Multiple services active across pilots	Target unchanged. Service definition clarified (one setup per tool/pilot = one service).
KPI5.2	Information Sharing Frequency	≥75% of incidents	Log established; blockchain infrastructure operational	Target unchanged. BYTE blockchain added as evidence layer.
KPI8.1	Cybersecurity Training Coverage	≥85% coverage	Training Needs Analysis in progress; eligibility data collected	Target unchanged. Measurement approach formalized with eBOS tracking.
KPI8.2	Cybersecurity Awareness Index	Awareness index of 75	Questionnaires designed; distribution planned May–Jun 2026	Measurement method enhanced with before/after CAI methodology. More rigorous than original.
KPI9.1	**New name** Policy Awareness and Compliance Readiness Rate	Policy Compliance Rate Increase policy compliance rate to 65%	Increase policy awareness of compliance rate by: 30 completed feedback surveys on the Policy Toolkit, 1 policy workshop/webinar organised, and 100 downloads/views of D6.7 Cybersecurity Policy Toolkit. D6.7 Toolkit published; baseline being aligned	KPIS renamed and methodology refined from policy compliance measurement to policy awareness and compliance readiness. Evidence will be based on Policy Toolkit feedback surveys, one policy awareness event, and recorded Toolkit downloads/views.
KPI9.2	Industry-specific Standard Adoption	Increase industry-specific standard adoption to 65%.	Track the adoption rate of industry-specific cybersecurity standards and best practices by critical sectors. Increase industry-specific standard adoption to 65%.	Target unchanged. Measurement approach refined above.
KPI9.3	Cybersecurity Certification Rate	20 certified entities	Removed from active KPIs framework	Certification attainment is outside project scope and partially covered by KPI9.2.
KPI9.4	D&C Engagement	+30% annually	ACHIEVED: +56% M12→M24	Target exceeded. M24 baseline established for M36 target.

© CYberSynchrony, 2026

KPI9.5	Stakeholder Engagement	≥50 stakeholders in 3 yrs.	Stakeholder Registry operational; policy outreach ongoing	Target unchanged. Policy white paper in development.
KPI9.6	Best Practices Exploitation	60% adoption in 3 yrs.	Questionnaire under development	Target unchanged. Measurement planned for final project year.

© CYberSynchrony, 2026

8 Deviations and Mitigation Measures

This chapter documents confirmed deviations from the KPIS targets and approaches established in D1.3, the mitigation measures applied during M24, and the revised outlook for M36 and the final reporting period.

8.1 Confirmed Deviations

The following confirmed deviations from the original D1.3 framework have been identified and addressed:

- **KPI2.1 - Penetration Test Target Revision:** The original target of ≥60 penetration tests was confirmed infeasible within the project scope and resources. Following consortium review, the target has been revised to 6 targeted penetration tests aligned with the three use case environments (AMC ×2, EGL ×1, UPRC ×1, plus potential Open Call contributions). This revision better reflects the operational reality of conducting controlled adversary-emulation activities in pilot environments.
- **KPI1.4 - Usability Measurement Methodology:** The original MOS (Mean Opinion Score) measurement approach for platform usability has been replaced by the System Usability Scale (SUS), a standardised and widely validated 10-item questionnaire yielding a score from 0–100. The revised target of SUS >70% (equivalent to 'Good' usability) replaces the original target of 4.5/5 MOS. This change improves comparability with industry benchmarks and provides more actionable data.
- **KPI9.1 - Policy Compliance Measurement Refinement:** The original KPIs referred to measuring compliance with EU-wide cybersecurity policies and standards across Member States. During the M24 review, this was considered difficult to measure directly within the project lifetime and not fully controllable by the consortium. The KPIs has therefore been refined as **Policy Awareness and Compliance Readiness Rate**, focusing on stakeholder engagement with the CYberSynchrony Policy Toolkit and related policy guidance. This keeps the policy ambition of the original indicator, while making the evidence more realistic, attributable and verifiable.
- **KPI9.3 – Cybersecurity Certification Rate Removal:** During the M24 KPIs review, the consortium concluded that KPI9.3 is outside the realistic scope of the project. The original KPIs aimed to measure the number of entities obtaining cybersecurity certifications in alignment with EU-wide standards, with a target of 20 certified entities. However, formal cybersecurity certification depends on external certification bodies, audit processes, organisational decisions, available resources and timelines that cannot be controlled by the CYberSynchrony consortium. The project does not provide certification services or conduct formal certification audits. Therefore, KPI9.3 has been removed from the active KPIs framework. Its underlying objective is considered partially covered by KPI9.2 – Industry-specific Standard Adoption, which measures adoption of cybersecurity standards, best practices and CYberSynchrony recommendations by participating critical entities in a more realistic, measurable and verifiable manner.
- **KPIs Framework - Duplicate Resolution:** The original D1.3 framework contained 39 objective KPIs entries with significant duplication across objectives. M24 review confirmed 12 instances of full duplication (KPI3.1, KPI3.2, KPI3.5, KPI4.1, KPI4.4, KPI6.1–KPI6.5, KPI7.1, KPI7.2) which are now formally cross-referenced to their primary entries. The active Objective KPIs count is 25. The duplicated KPIs remain relevant to their respective objectives, but their evidence will be collected once under the primary KPIs to avoid double-counting.
- **Use Case KPIs Updates**: During M24 review, the use case KPIs tables were updated to reflect the latest inputs from AMC, EGL and UPRC. These updates clarify the pilot-specific baseline status, scenarios, tools and measurement approaches.
- **UC1.KPI1 – Data Encryption Target Refinement:** UC1.KPI1 has been refined from a general “100% data encryption implementation” target to a more specific focus on the encryption of outgoing exported patient-sensitive data. Target reflects the AMC infrastructure needs and internal procedures.
- **UC1.KPI3 – Audit Frequency Target Refinement:** UC1.KPI3 has been refined from increasing audit frequency to bi-annually to increasing it to annually, as AMC currently has no annual or bi-annual audit process in place. The revised target is more realistic and supports the establishment of a sustainable audit posture.

© CYberSynchrony, 2026

- **UC1.KPI4 – Detection and Response Baseline Refinement:** UC1.KPI4 remains focused on achieving a 60% reduction in detection and response time, but the baseline is being reconstructed because AMC has no prior documented incident-response records. This refinement ensures that the KPIs can be measured against a realistic and evidence-based baseline during pilot validation.
- **UC2.KPI4 – Use Case KPIs Description Update:** UC2.KPI4 has been renamed and redefined from increasing the number of citizens using digital IDs to increasing the proportion of municipal incident records whose integrity can be verified and monitored. The updated KPIs better reflects the MAESTRO platform capabilities and EGL's infrastructure needs for sustainable cybersecurity adoption.
- **UC3 KPIs Clarification:** The UPRC use case KPIS descriptions have been refined to better reflect the latest pilot planning inputs.The KPIs names and targets remain aligned with the original formulation. UC3.KPIS1 is linked to a phishing simulation and historical incident baseline collection, UC3.KPI2 is connected to faculty compliance assessment supported by training and policy-related activities, UC3.KPI3 focuses on pre-pilot satisfaction and perceived security baseline collection, and UC3.KPIS4 is linked to the isolated NOC simulation lab and response-time baseline establishment. These are clarifications of scope and measurement approach, not changes to the overall KPIs targets.
- **Delayed Quantitative Data – Technical KPIs:** Pilot deployment commenced at M25/M26 (June/July 2026), which is at the boundary of this reporting period. Consequently, quantitative measurement results for technical KPIs (KPI1.1–KPI1.3, KPI1.5–KPI1.6, KPI2.2–KPI2.4, KPI3.6–KPI3.7, KPI4.2–KPI4.3, KPI4.5, KPI5.1–KPI5.2, KPI8.1–KPI8.2) are not yet available. These results will be consolidated in D1.5 (final KPIs report).

8.2 Mitigation Measures Applied

- **Structured Register Framework:** Standardised Excel-based registers (Threat Assessment Register, Risk Scenario Register, Vulnerability Register, Incident/Response Register, Cross-Border Exercise Register, Information Sharing Log, Platform Vulnerability Register) have been designed and distributed to all responsible partners, ensuring consistent evidence collection when pilots commence.
- **KPIs Ownership Assignment:** Each Objective KPIs now has a formally assigned owner responsible for data collection, evidence validation, and reporting. This resolves the Year 1 ambiguity where multiple partners contributed to the same KPIs without a single point of accountability.
- **Open Call Integration:** Open Call 1 activities will contribute to multiple KPIs (particularly KPI1.1, KPI1.2, KPI2.1, KPI3.4, KPI4.2, KPI4.3, KPI4.5, KPI5.1), providing additional data points to support target achievement.
- **Proactive Baseline Establishment:** Use case leaders (AMC, EGL, UPRC) have all initiated baseline data collection and scenario definition prior to the formal pilot deployment phase, reducing the risk of delays in comparative measurement.

Continuous KPIs Dashboard Monitoring: The KPIs Dashboard (Chapter 6) provides project-wide visibility and enables early identification of at-risk KPIs through regular consortium review at WP8 coordination meetings

8.3 Revised Targets and Outlook

With the exception of KPI2.1 (revised from 60 to 6 penetration tests) and KPI1.4 (measurement method updated to SUS), KPI9.1 and KPI9.3, all other KPIs targets remain as defined in D1.3. The consortium is confident in the achievability of the remaining targets based on the tool deployments, pilot readiness, and evidence collection infrastructure now in place.

The final consolidated KPIs report (D1.5) will provide quantitative results for all 25 Objective objective KPIs, based on pilot data collected during M25–M33, Use Case KPIs and Communication & Dissemination KPIs. The present report establishes the complete methodological and governance foundation required to deliver those results with full traceability and evidence integrity.

© CYberSynchrony, 2026

8.4 KPIs TEMPLATE

To ensure consistent reporting across all deliverables and partners, the consortium will use a common KPIs verification template for the collection of evidence and reporting of results. This template will support the final consolidation of KPIs achievements in D1.5 and will ensure that each KPIs is assessed using the same evidence logic, regardless of the responsible partner or technical module involved.

This common template will be used by KPIs owners during Year 3 to support structured evidence collection and to ensure that the final KPIs assessment in D1.5 is complete, traceable and auditable. The template is provided in Annex I.

© CYberSynchrony, 2026

9 Conclusions

D1.4 marks a critical maturation point for the CYberSynchrony KPIs framework. Building on the conceptual baseline established in D1.3, this report delivers a fully operationalised, governance-aligned, and evidence-ready KPIS monitoring system that will support the final measurement and reporting phase of the project. The M24 review identified duplicated KPIs entries across objectives and introduced a more practical monitoring framework, where each active KPIs is linked to a responsible owner, verification deliverable, evidence source and measurement methodology.

Key contributions of this report include:

- Rationalisation of the KPIs set from 39 entries to 25 Objective indicators, eliminating ambiguity and ensuring each KPIs has a clear owner, verification deliverable, and evidence framework.
- Substantially enhanced measurement methodologies for all Objective KPIs, with partner/tool assignments, register structures, and evidence type specifications.
- First partial quantitative results demonstrating tangible progress (KPI3.3: 199 phishing campaign participants; KPI9.4: 56% D&C engagement growth).
- Formal documentation of confirmed target revisions including (KPI2.1, KPI1.4) with full justification, and additional clarifications for Objective 9 indicators including KPI9.1 refinement and KPI9.3 removal, as well as clarification of KPI7.1 as a duplicate indicator.
- Removal of KPI9.3, as cybersecurity certification attainment falls outside the direct scope and control of the project, with related objectives partially addressed through KPI9.2.
- Strong Communication and Dissemination performance, with multiple targets already exceeded or on track at M24
- Three pilot use cases (healthcare, public administration, higher education) with defined KPIs scenarios, aligned methodologies, and baseline collection underway.

The project now transitions into the critical measurement and validation phase. Pilot use case initiation, starting from M26 onwards, will generate the quantitative evidence base required for the final consolidated KPIs report in D1.5. The KPIs governance structures, registers, and dashboard mechanisms established in this report will ensure that data collection is consistent, evidence-linked, and audit-ready for both the consortium and the European Commission.

CYberSynchrony remains committed to delivering measurable, evidence-based impact across the European cybersecurity landscape, with KPIs serving as the primary instrument for demonstrating that the platform's technical capabilities, training outputs, and cross-border collaboration activities translate into concrete security improvements for, but not limited to, the healthcare, public administration, and higher education sectors.

© CYberSynchrony, 2026

Annex I - KPIs Template for Cybersynchrony KPIs Mapping

KPI ID	**KPI Name**	**Owner**
Target		
Measurement Methodology		
Components involved	**Participating partners & Role in KPI Measurement**	**Evidence collection process & validation approach**
Methodology Description		
KPI Progress Status		

Current Value/Target	**Date of Measurement**	**Status**	**Next Actions** (if required)
		On Track / Under Review/ Finalised	

Challenges, Deviations and Corrective Actions

© CYberSynchrony, 2026