Harmonizing People, Processes, and Technology for Robust Cybersecurity

D6.4 Compliance Monitoring

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	D6.4 Compliance Monitoring		
Work Package	WP6 – CYBERWISE-CYBERGOPLUS		
Contractual due date	31/12/2025	**Actual submission date**	15/12/2025
Type	Report	**Dissemination Level**	PU
Lead Beneficiary	IANUS		
Responsible Author	Demetris Antoniou (IANUS)		
Contributions from	BYTE, MAG, DSA		

Funded by the European Union

Funded by the European Union under Grant Agreement no. 101158555. 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	Issue Date	Changes	Contributor(s)
0.1	01.09.2025	Initial Deliverable structure	Demetris Antoniou (IANUS)
0.2	30.09.2025	Draft text version	Demetris Antoniou (IANUS)
0.3	13.10.2025	Contribution on Real-Time compliance oversight	BYTE (George Karavokiros)
0.4	20.10.2025	Contribution in integration logic	MAG (Kostas Andrikos)
0.5	10.11.2025	Implementation of DSA requirements	DSA (George Achilleos)
0.6	02.12.2025	90% of the deliverable ready for peer-review	Demetris Antoniou (IANUS)
0.7	10.12.2025	Peer-Review	Vasilis Rousakis (KETYAK)
0.8	10.12.2025	Addressed Peer-review comments and delivered for 2nd peer-review and QA.	Demetris Antoniou (IANUS)
0.9	12.12.2025	Peer & QA review	Eleni Keliri (eBOS)
1.0	15.12.2025	Deliverable 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

© CYberSynchorny, 2025

Table of Contents

1 Executive Summary 9
2 Introduction 11
2.1 Purpose of the Deliverable 11
2.2 Mapping CYberSynchrony Outputs 11
2.3 Linkage to other project outputs 12
2.4 Deliverable Structure 13
3 Overview of WP6 and Task 6.7 14
3.1 WP6 Scope and Cross-Sector Orientation 14
3.2 Role of Task 6.7 – Real-Time Compliance Oversight 14
3.3 Dependencies with Tasks 6.1–6.6 15
3.4 Key Outputs Expected from D6.4 15
3.4.1 Compliance Monitoring v1 (Definition & Architecture) 15
3.4.2 Compliance Monitoring v2 (Implementation & Validation) 16
4 Compliance Framework Foundations 17
4.1.1 NIS2 Directive and National Implementation Frameworks 17
4.2 Sector-Specific Requirements (Healthcare, Governance, Research) 19
4.2.1 Healthcare Sector Requirements 19
4.2.2 Public Administration Sector Requirements 20
4.2.3 Research and Academia Sector Requirements 21
4.3 Harmonised Cross-Sector Principles 23
4.3.1 Principle 1: Risk-Driven Governance 24
4.3.2 Principle 2: Asset-Centric Protection 24
4.3.3 Principle 3: Continuous Threat Detection 25
4.3.4 Principle 4: Resilience and Recovery 25
4.4 Mapping of Principles to CYberSynchrony Responsibilities 26
5 CYberSynchrony Compliance Monitoring Approach (High-Level) 28
5.1 Objectives of Compliance Monitoring 28
5.2 Pipelines Compliance Domains and Assessment Areas 28
5.3 Indicators, Metrics and Maturity Levels 29
5.3.1 Operational Compliance Indicators (KCIs) 29
5.3.2 Mapping Controls to KPIs 29
5.3.3 Maturity Levels 30
5.4 Evidence Bases: Policy, Implementation, and Operational Artefacts 31
5.4.1 Policy and Governance Evidence 31
5.4.2 Implementation and Configuration Evidence 31
5.4.3 Operational and Runtime Evidence 32
6 System Specifications and Integration Requirements 34
6.1 Functional Requirements 34
6.1.1 Policy and Governance Management Functions 34
6.1.2 Automated Auditing and Assessment Functions 34
6.1.3 Findings Management and Reporting Functions 35
6.2 Technical Specifications 35
6.2.1 Architecture Pattern 35
6.2.2 Technology Stack 35
6.2.3 Data Storage Strategy 35
6.2.4 Security Standards 36
6.3 Integration Specifications 36
6.3.1 Integration with Data Sources (Northbound/Southbound) 36

© CYberSynchorny, 2025

6.3.2 Integration with Identity Services 37
6.3.3 Integration with Presentation Layer 37
7 Conclusions and Roadmap to v2 38
7.1 Summary of v1 Achievements (Definition Phase) 38
7.2 Immediate Next Steps (Development Phase M19–M30) 38
7.3 Cycle Objectives for D6.8 Compliance Monitoring v2 (Validation Phase) 38
8 References 40
Annex I: Technical Interface Specifications 41

List of Figures

Figure 1: Harmonised Cross-Sector Compliance Principles mapping regulatory concepts to CYberSynchrony platform responsibilities 24

Figure 2: Functional Compliance Monitoring Architecture detailing the flow from raw telemetry to stakeholder reporting. 33

Figure 3: CYBERGOPLUS Technical Architecture. This diagram illustrates the module's microservices deployment within Kubernetes, detailing data ingestion from external sources (CYBRITE, CROSS-CORE), internal processing via the Compliance Engine, and integration with Keycloak for identity and polyglot storage for data persistence. 37

List of Tables

Table 1: Adherence to CYberSynchrony's GA 11

Table 2: Links to other Project Outputs/Work 12

Table 3: Mapping of Platform Functionality to Regulatory Evidence 17

Table 4: Healthcare-Specific Compliance Indicators 20

Table 5: Public Administration-Specific Compliance Indicators 21

Table 6: Research and Academia-Specific Compliance Indicators 22

Table 7: Mapping of Harmonised Principles to Platform Responsibilities 26

Table 8: Comprehensive Compliance Indicator Map 29

© CYberSynchorny, 2025

Acronyms and abbreviations

Abbreviation / Term	Description
AM	Asset Management
API	Application Programming Interface
BFF	Backend for Frontend
BIA	Business Impact Analysis
BYOD	Bring Your Own Device
CAPA	Corrective and Preventive Action
CISO	Chief Information Security Officer
CNI	Container Network Interface
CVE	Common Vulnerabilities and Exposures
CYBERRA	Cyber Threat Intelligence and Customized Risk Analysis
CYBRITE	Proactive Cyber Risk Monitoring and Incident Response
CROSS-CORE	Cross-Border Cyber Incident Cooperation & Response
CYBERGOPLUS	Cybersecurity Governance and Compliance
CYBERWISE	Cybersecurity Consciousness: Empowering Society Through Awareness
CYRESCUE	Cybersecurity Resilience and Incident Response Enhancement
DCO	Defensive Cyber Operations
DDoS	Distributed Denial of Service
DPO	Data Protection Officer
DSA	Digital Security Authority (Cyprus)
EDR	Endpoint Detection and Response
EHR	Electronic Health Records
EIM	Event and Incident Management
FIM	File Integrity Monitoring
GDPR	General Data Protection Regulation
GOV	Governance
GRC	Governance, Risk, and Compliance
gRPC	gRPC Remote Procedure Calls
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

© CYberSynchorny, 2025

IaC	Infrastructure as Code
IAM	Identity and Access Management
IDS	Intrusion Detection System
IoMT	Internet of Medical Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
JWT	JSON Web Token
K8s	Kubernetes
KCI	Key Compliance Indicator
KPI	Key Performance Indicator
LMS	Learning Management System
MFA	Multi-Factor Authentication
MTTR	Mean Time to Remediate / Respond
NIS2	Network and Information Security Directive 2
NIST	National Institute of Standards and Technology
NS	Network Security
OIDC	OpenID Connect
OS	Operating System
PHI	Protected Health Information
PII	Personally Identifiable Information
RBAC	Role-Based Access Control
REST	Representational State Transfer
RM	Risk Management
SAST	Static Application Security Testing
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SNYK	Security tool for vulnerability scanning
SOC	Security Operations Center
SS	System Security
SSO	Single Sign-On

© CYberSynchorny, 2025

SQL	Structured Query Language
TA	Training and Awareness
TLS	Transport Layer Security
TLP	Traffic Light Protocol
UI	User Interface
URL	Uniform Resource Locator
VM	Vulnerability Management
WP	Work Package
XML	Extensible Markup Language

© CYberSynchorny, 2025

1 Executive Summary

Task 6.7 *Real-Time Compliance Oversight* plays a crucial role within CYberSynchrony by establishing the mechanisms, indicators and monitoring pipelines required to ensure that organizations adopting the CYberSynchrony ecosystem can demonstrate continuous alignment with cybersecurity and data protection regulations. As regulatory frameworks such as **NIS2**, **GDPR** and technical standards such as **NIST 800** and **ISO 27001** shift towards evidence-driven compliance, task 6.7 introduces a structured methodology for real-time compliance oversight. The digital transformation of critical sectors across Europe has introduced unprecedented efficiencies but also significant vulnerabilities. As organizations in Healthcare, Public Administration, and Academia digitize their operations, they become subject to an increasingly complex web of regulatory requirements, most notably the **NIS2 Directive** and **GDPR**. However, a persistent challenge in cybersecurity governance is the gap between *written policy* and *technical reality*. Organizations often possess comprehensive security policies on paper yet lack the visibility to verify if these policies are enforced across their IT infrastructure in real-time.

Deliverable 6.4 Compliance Monitoring v1 addresses this critical gap within the **CYberSynchrony** project. Developed under **Work Package 6 (WP6)**, this document establishes the foundational framework for **Task 6.7 (Real-time Compliance Oversight)**. Its primary objective is to define the methodology, requirements, and architecture for the **CYBERGOPLUS** module; a dedicated component designed to continuously monitor, audit, and visualize an organization's compliance posture.

This deliverable serves three distinct but interconnected purposes:

1. **Defining the "To-Be" Technical State:** It translates the 15 static Policy Tools developed in **D6.3 (Cybersecurity Policy Toolkit)** into measurable technical requirements. By mapping policy clauses (e.g., "Passwords must expire every 90 days") to digital indicators (e.g., Active Directory configuration parameters), this document creates the blueprint for the automated monitoring tools currently under development.
2. **Establishing the "As-Is" Baseline**: Leveraging the extensive end-user requirements analysis from **D2.2** and supplementary surveys conducted in M18, this report provides a detailed **Initial Baseline Assessment** of the project's pilot use cases. This assessment reveals a mixed maturity landscape: while sectors like Healthcare demonstrate high adherence to Data Protection standards (driven by existing regulations), broader compliance with Asset Management and Vulnerability Management remains inconsistent and largely manual.
3. **Architecting the Solution:** It outlines the technical architecture of the CYBERGOPLUS module, ensuring seamless integration with the **Cyber Awareness Platform (D6.1)**. The architecture leverages open-source components (such as **Wazuh** for telemetry and **Keycloak** for identity management) to provide a scalable, cost-effective compliance solution for European SMEs and public entities.

Key Findings from the Baseline Assessment:

- **Policy Adoption is High:** 85% of pilot organizations have formally adopted the governance policies defined in D6.3.
- **Technical Enforcement is Low:** Only 35% of organizations have automated tools to verify that these policies are enforced on endpoints.
- **Reporting is a Burden:** 71% of respondents in the D2.2 survey identified "Compliance Reporting" as a critical need, citing the manual effort required to generate audit evidence as a major resource drain.

Conclusion and Next Steps: This v1 deliverable successfully defines the *scope* and *design* of the compliance monitoring system. It confirms that the "Real-Time Oversight" capability is not just a technical luxury but a regulatory necessity under NIS2. The roadmap presented in Chapter 8 outlines the transition from this design

© CYberSynchorny, 2025

phase to the active development and deployment of the automated tools, culminating in the final validation report (**D6.8 Compliance Monitoring v2**) due in Month 36.

© CYberSynchorny, 2025

2 Introduction

2.1 Purpose of the Deliverable

In the rapidly evolving landscape of European cybersecurity, regulatory frameworks such as the **NIS2 Directive** [1] and **GDPR** [2] have shifted the focus from voluntary best practices to mandatory compliance. Organizations operating critical infrastructure or providing essential services must now demonstrate not only that they have security policies in place, but that these policies are actively enforced and effective.

The primary purpose of **Deliverable 6.4 Compliance Monitoring v1** is to establish the operational framework for **Task 6.7 (Real-time Compliance Oversight)**. This task aims to bridge the gap between governance documentation and technical reality by deploying automated tools that continuously verify the security posture of an organization.

This deliverable serves as the foundational blueprint for the **CYBERGOPLUS** compliance module. It defines:

- **The "What":** The specific regulatory requirements and internal policies (from **D6.3**) that must be monitored.
- **The "How":** The technical architecture and indicators (KCIs) required to translate static policy documents into dynamic, real-time alerts.
- **The "Current State":** A baseline assessment of the project's pilot users, identifying the current maturity gaps that the automated system must address in its final release (v2).

2.2 Mapping CYberSynchrony Outputs

This deliverable is a key output of **Work Package 6 (WP6)**, which focuses on "Cybersecurity Consciousness: Empowering Society Through Awareness." Specifically, it addresses the requirements of **Task 6.7**, led by **BYTE**, which mandates the development of "tools that monitor and audit in real-time" to ensure industry-wide compliance.

The following table maps the specific Grant Agreement (GA) commitments addressed in this document:

Table 1: Adherence to CYberSynchrony's GA

Component no	Component title	Respective Document Chapter(s)	Justification
DELIVERABLE			
D6.4	**Compliance Monitoring v1**	All	Defines the methodology and initial findings for compliance oversight.
TASKS			
Task 6.7	**Real-time Compliance Oversight**	Chapters 3, 4, 5	Describes the technical framework for real-time auditing tools.

© CYberSynchorny, 2025

2.3 Linkage to other project outputs

The Compliance Monitoring framework leverages and integrates results from multiple Work Packages across the project. This deliverable is related to other project outputs as it translates the requirements, policies, and technical capabilities defined elsewhere into a structured oversight mechanism.

Table 2 outlines the specific deliverables and tasks that contribute to or interface with the compliance monitoring activities described in D6.4.

Table 2: Links to other Project Outputs/Work

WP Number	Task Number	Deliverable Number related	Content
WP2	T2.2, T2.4	D2.2 [7]	Provides the cybersecurity landscape analysis, end-user requirements (including reporting needs), and the overarching framework design used to define the compliance baseline.
WP3	T3.2	D3.2[8]	Provides the Risk Scenario Analysis Toolkit and Risk Register structure used for the "Risk-Driven Governance" principle.
WP4	T4.1	D4.1[9]	Provides the Integrated Cybersecurity Monitoring Suite (Wazuh, Suricata, Sysmon) which generates the raw technical evidence for asset, network, and vulnerability compliance.
WP4	T4.3	D4.2[10]	Provides the Automated Response Toolkit (DCO Playbooks), used to verify incident response and resilience capabilities.
WP5	T5.2	D5.2[11]	Provides the Evidence Integrity System (Hyperledger), used to verify the immutability of logs and audit trails.
WP6	T6.1	D6.1[12]	Provides the Cyber Awareness Platform and Keycloak Identity Manager, used as the source of truth for Role-Based Access Control (RBAC) and MFA verification.
WP6	T6.4	D6.2[13]	Provides the Cybergate gamified training environment, generating the user performance metrics required to verify staff awareness training compliance.
WP6	T6.5	D6.3[14]	Provides the Cybersecurity Policy Toolkit, containing the 15 static policy templates (e.g., Access Control, Asset Management) that this monitoring module digitizes.
WP8	T8.1	D8.1[15]	Provides the Integration Blueprint and Kubernetes architecture standards that dictate how the compliance module is deployed and connected to the ecosystem.

© CYberSynchorny, 2025

2.4 Deliverable Structure

This document is organized into the following chapters:

- **Chapter 1: Executive Summary:** Provides an overview of the document, summarizing the context, objectives, and main findings regarding compliance monitoring within the CYberSynchrony project.
- **Chapter 2: Introduction:** Outlines the purpose of the deliverable, maps the content to project outputs and the Grant Agreement, and details the structure of the document.
- **Chapter 3: Overview of WP6 and Task 6.7:** Describes the scope of Work Package 6, focusing on the role of Task 6.7 in real-time compliance oversight, its dependencies with other tasks, and the expected outputs.
- **Chapter 4: Compliance Framework Foundations:** Establishes the regulatory baselines (including NIS2, GDPR, and ISO 27001), sector-specific requirements for Healthcare, Governance, and Research, and the harmonized principles underpinning the framework.
- **Chapter 5: CYberSynchrony Compliance Monitoring Approach (High-Level):** Details the methodology for monitoring, covering objectives, compliance domains, indicators, metrics, and the evidence bases derived from policy, implementation, and operational layers.
- **Chapter 6: System Specifications and Integration Requirements:** Defines the functional capabilities, technical architecture, and integration interfaces required for the CYBERGOPLUS module, ensuring alignment with the wider CYberSynchrony ecosystem.
- **Chapter 7: Conclusions and Roadmap to v2:** Summarizes the achievements of this definition phase, outlines the immediate next steps for development, and sets the objectives for the final validation release (D6.8).
- **Chapter 8: References:** Lists the bibliographic references used throughout the document.
- **Annex I: Technical Interface Specifications:** Provides the specific data models, JSON schemas, and API payload definitions required for system integration.

© CYberSynchorny, 2025

3 Overview of WP6 and Task 6.7

3.1 WP6 Scope and Cross-Sector Orientation

Work Package 6 (WP6), titled "Cybersecurity Consciousness: Empowering Society Through Awareness (CYBERWISE) and Cybersecurity Standardization and Compliance Reinforcement (CYBERGOPLUS)," is designed to address the human and governance layers of the cybersecurity ecosystem. The scope of this work package extends beyond technical implementation to encompass the behavioral and organizational changes necessary to maintain a secure posture.

The primary objectives of WP6 are to:

- Engage diverse societal segments with cybersecurity awareness.
- Utilize gamification techniques to make learning impactful.
- Measure the effectiveness of awareness campaigns using data analytics.
- Cultivate a culture prioritizing secure online behavior.
- Support comprehensive cybersecurity policy implementation.
- Establish unified standards across various sectors.
- Monitor and audit adherence to established cybersecurity standards.
- Ensure industry-wide compliance with regulations.

A defining characteristic of WP6 is its cross-sector orientation. As identified in the project's landscape analysis, diverse industry sectors often maintain varied cybersecurity practices, which can create inconsistencies and vulnerabilities. To address this, WP6 integrates requirements from three distinct critical sectors: Healthcare, Public Administration (Governance), and Academia/Research.

Through Task 6.6 (Sector-Specific Cybersecurity Harmonization), the project seeks to bridge differences between these domains and advocate for the adoption of a consistent cybersecurity framework. By engaging with multiple industry sectors, this initiative ensures that there is a uniform set of cybersecurity standards and practices. This harmonization reduces vulnerabilities resulting from inconsistent practices and ensures that every sector is fortified against cyber threats.

Consequently, the compliance monitoring activities described in this deliverable are designed to be adaptable. They must support specific sectoral requirements (such as patient data privacy in healthcare or open network security in academia) while enforcing a harmonized baseline of security controls mandated by cross-cutting regulations like NIS2 and GDPR.

3.2 Real-Time Compliance Oversight

Task 6.7, titled "Real-time Compliance Oversight," is led by BYTE with the participation of MAG, IANUS, DSA, and KETYAK. The primary role of this task is to maintain the integrity of established cybersecurity standards by introducing tools that monitor and audit adherence in real time.

Unlike traditional compliance assessments which may be static or periodic, this task focuses on providing instant insights into how organizations are complying with established norms. It is designed to flag any deviations or non-compliance instantly. By providing real-time oversight, Task 6.7 ensures that standards are not just set but are also followed diligently. The capability for prompt detection ensures that deviations are rectified immediately, thereby minimizing potential security risks.

© CYberSynchorny, 2025

This task effectively operationalizes the governance frameworks defined in other tasks by deploying the technical means to verify them. It serves as the foundation for the compliance monitoring and auditing tools within the CYBERGOPLUS module, assessing entities' adherence to cybersecurity standards.

3.3 Dependencies with Tasks 6.1–6.6

Task 6.7, "Real-time Compliance Oversight," does not operate in isolation. It relies heavily on the outputs, frameworks, and data generated by the preceding and concurrent tasks within Work Package 6. While Tasks 6.1 through 6.6 focus on the creation of content, tools, and standards, Task 6.7 focuses on the verification and measurement of their adoption and effectiveness.

The specific dependencies are outlined below:

- **Dependence on Task 6.1 (Cyber Awareness Platform) and Task 6.4 (Immersive Gamified Cybersecurity):** These tasks aim to engage societal segments and utilize gamification for impactful learning. They provide the raw data required to measure "human-centric" compliance. Task 6.7 requires input from the Cyber Awareness Platform (T6.1) and Gamified Training Modules (T6.4) to verify metrics such as training completion rates and user engagement levels, ensuring that the objective of cultivating a secure culture is met.
- **Dependence on Task 6.2 (Proactive Social Engineering Assessments):** Task 6.2 involves targeted campaigns to simulate real-world threats like phishing to evaluate user responses. Task 6.7 relies on the data from these assessments to report on the organization's vulnerability to social engineering and to track improvements in staff resilience over time.
- **Dependence on Task 6.5 (Tailored Cybersecurity Policy Tools):** This task focuses on developing adaptable tools and templates to assist in the creation of cybersecurity policies. These policies form the "ruleset" that Task 6.7 monitors. Without the defined policies and regulations from T6.5 (e.g., Access Control Policy, Data Protection Policy), the compliance monitoring tools in T6.7 would lack the specific criteria against which to audit the organization.
- **Dependence on Task 6.6 (Sector-Specific Cybersecurity Harmonization):** Task 6.6 aims to bridge differences between diverse industry sectors (Healthcare, Public Administration, Academia) to advocate for a consistent cybersecurity framework. Task 6.7 depends on this harmonized framework to apply the correct audit parameters to specific entities. It ensures that the monitoring tools respect the unified standards established in T6.6 while verifying adherence across different sectors.

In summary, Tasks 6.1–6.6 establish the "what" (policies, training content, standards) and the "how" (training delivery, harmonization), while Task 6.7 establishes the "check" (monitoring, auditing, oversight) to ensure these elements are effectively implemented.

3.4 Key Outputs Expected from D6.4

Deliverable 6.4 serves as the initial version of the "Compliance Monitoring" report. It establishes the foundational framework for Task 6.7, defining the mechanisms required to bridge the gap between governance documentation and technical reality. This section outlines the specific outputs delivered in this version (v1) and sets the stage for the subsequent implementation phase (v2).

3.4.1 Compliance Monitoring v1 (Definition & Architecture)

This subsection defines the scope of the current deliverable, which focuses on the definition of tools, architecture, communications, and requirements necessary for real-time oversight. The key outputs provided in v1 include:

© CYberSynchorny, 2025

- **Methodological Framework Definition:** The document establishes the methodology for the CYBERGOPLUS module, detailing how compliance will be monitored, audited, and visualized.
- **Translation of Policy into Technical Requirements:** It translates the 15 static Policy Tools developed in D6.3 (Cybersecurity Policy Toolkit) into measurable technical requirements. This includes mapping policy clauses to specific digital indicators.
- **Technical Architecture Blueprint:** It outlines the technical architecture of the compliance module, specifying the integration with the Cyber Awareness Platform (D6.1) and the use of components such as Wazuh and Keycloak.
- **Initial Baseline Assessment:** Leveraging analysis from D2.2 and supplementary surveys, this output provides an "As-Is" assessment of the pilot use cases, identifying current maturity gaps in compliance enforcement.

3.4.2 Compliance Monitoring v2 (Implementation & Validation)

This subsection outlines the expected outputs for the final release, Deliverable 6.8, which represents the actual implementation and validation of the systems defined in v1. The key outputs expected in v2 include:

- **Deployment of Automated Tools:** The transition from the design phase to the active development and deployment of the automated monitoring tools described in the v1 blueprint.
- **Mature Monitoring Outcomes:** Presentation of data derived from the "Real-Time Oversight" capability, moving beyond baseline assessments to provide evidence of continuous compliance.
- **Final Validation Report:** A comprehensive report detailing the validation of the compliance monitoring system within the pilot environments, confirming its effectiveness in addressing the gaps identified in v1.
- **Refined Compliance Indicators:** Updated indicators and metrics based on the lessons learned and cross-sector challenges identified during the initial monitoring cycles.

© CYberSynchorny, 2025

4 Compliance Framework Foundations

This chapter establishes the regulatory and theoretical foundations upon which the CYberSynchrony compliance monitoring mechanism is built. To ensure that the "Real-Time Oversight" capability defined in Task 6.7 is effective, it must be grounded in specific legal obligations, industry standards, and organizational policies rather than abstract metrics. This section outlines the regulatory baselines, primarily the NIS2 Directive and GDPR, that dictate the mandatory security controls for European essential entities.

Furthermore, this framework integrates the outputs of D6.3 (Cybersecurity Policy Toolkit), ensuring that the automated monitoring tools are configured to verify specific policy clauses defined in the project's standardized templates. The following sections detail how these regulatory requirements are harmonized with sector-specific needs for Healthcare, Public Administration, and Research, creating a unified basis for the technical indicators described later in this document.

4.1.1 NIS2 Directive and National Implementation Frameworks

The NIS2 Directive (Directive (EU) 2022/2555) establishes cybersecurity risk management measures and reporting obligations for essential entities. To operationalize real-time compliance monitoring within the CYberSynchrony ecosystem, the project utilizes the security measures framework established by the Digital Security Authority (DSA) of Cyprus in Decision 389/2020. This framework structures the high-level requirements of NIS2 into measurable domains, including Governance, Protection, Defence, and Resilience. It is further aligned with the overall European approach for NIS2 implementation as defined by ENISA and the Member State national authorities[6].

The compliance monitoring approach translates these regulatory obligations into verifiable digital evidence. The CYBERGOPLUS module ingests specific data points from the platform's active components to verify that specific controls are operational, rather than relying on manual self-assessments.

Regulatory Control Mapping Operational Compliance Flow

To ensure traceability, the framework establishes a clear lineage from platform functionality to collected evidence, and finally to the satisfied regulatory requirement. The following table reconciles the CYberSynchrony platform capabilities with the specific evidence artifacts generated and the corresponding NIS2-aligned controls defined in the national framework and international standards.

Table 3: Mapping of Platform Functionality to Regulatory Evidence

CYberSynchrony Functionality	Evidence Collected (Digital Artifact)	Source Deliverable	Regulatory Requirement Satisfied (DSA 389/2020 / ISO 27001 / NIST) [3][4][5]
Automated Asset Discovery (Wazuh)	Real-time inventory logs listing active IP addresses, hostnames, and OS versions.	D4.1	Asset Management (AM2) Inventory of assets (ISO A.8.1.1 / NIST CM-8)
Identity Management (Keycloak)	Configuration logs verifying MFA enforcement and Single Sign-On (SSO) usage.	D6.1	Identity & Access (IAM4) Strong authentication (ISO A.9.1.2 / NIST AC-3)

© CYberSynchorny, 2025

Network Traffic Analysis (Suricata)	EVE JSON logs confirming use of secure protocols (TLS 1.2/1.3) and absence of cleartext.	D4.1	Network Security (NS4) Secure communication protocols (ISO A.13 / NIST SC-8)
Vulnerability Detection (Wazuh)	CVE Reports detailing open Critical/High severity vulnerabilities on endpoints.	D4.1	Vulnerability Management (VM1) Vulnerability scanning (ISO A.12.6 / NIST RA-5)
Software Security Scanning (SNYK)	SAST reports identifying code-level vulnerabilities and dependency risks.	D6.1	Vulnerability Management (VM1) Vulnerability scanning (ISO A.12.6 / NIST RA-5)
Gamified Training (Cybergate)	User participation records and simulation outcome scores (e.g., Phishing defense).	D6.2	Awareness & Training (TA2) Information Security training (ISO A.7.2.2 / NIST AT-1)
Immutable Logging (Hyperledger)	Blockchain hash records proving logs and backups have not been altered.	D5.2, D4.1	Data Integrity (DS) Information integrity (NIS2 Art 21 / ISO A.8)
Policy Management (CYBERGOPLUS)	Digital policy versions and user acknowledgment timestamps.	D6.3	Governance (GOV3) Policies and procedures (ISO A.5.1 / NIST PL-1)

Evidence Requirements for Compliance Monitoring

The following subsections detail the evidence required to validate compliance for the core NIS2 domains. The monitoring engine relies on specific data streams to validate the controls listed above.

1. Asset and Configuration Evidence To satisfy Asset Management (AM) requirements, the system ingests dynamic data regarding the infrastructure state.

- **Functionality:** The Wazuh agent collects system-level telemetry including process executions and installed applications.
- **Evidence:** Automated inventory scans provided by D4.1 are reconciled against the authorized asset register defined in D2.2 requirements. This verifies control AM2 (Inventory of Assets).

2. Identity and Access Evidence Monitoring compliance with Identity and Access Management (IAM) focuses on authentication mechanisms.

- **Functionality:** Keycloak manages user identities and enforces Multi-Factor Authentication (MFA).
- **Evidence:** Authentication logs (success/failure) and configuration exports from D6.1 provide proof that strong authentication (IAM4) is active and that privileged access is restricted.

3. Technical Security Evidence To validate Network (NS) and System Security (SS), the platform ingests traffic and configuration data.

© CYberSynchorny, 2025

- **Functionality:** Suricata performs deep packet inspection to detect insecure protocols.
- **Evidence:** EVE JSON logs from D4.1 serve as evidence for Secure Communication Protocols (NS4), confirming that data in transit is encrypted.

4. Resilience and Awareness Evidence Verifying Resilience (BCR) and Awareness (TA) requires evidence of testing and human engagement.

- **Functionality:** The Cybergate platform simulates attack scenarios (e.g., Ransomware) to test staff response.
- **Evidence:** Training completion records and simulation scores from D6.2 provide objective evidence for Information Security Awareness (TA2) and verify that staff are prepared for incident response.

4.2 Sector-Specific Requirements (Healthcare, Governance, Research)

While the CYberSynchrony platform applies a harmonized compliance framework, distinct sectors possess unique operational risks, asset types, and regulatory nuances that require tailored monitoring configurations. This section details the specific requirements for the Healthcare sector, as identified during the end-user analysis and pilot definition phases.

4.2.1 Healthcare Sector Requirements

The healthcare sector represents a critical domain within the NIS2 Directive scope, characterized by the processing of sensitive personal data and the reliance on life-critical systems. The digitization of health services, including Electronic Health Records (EHR) and Remote Patient Monitoring (RPM), has expanded the attack surface, making data privacy and system availability paramount.

Regulatory and Operational Context

Healthcare entities are classified as essential entities under NIS2 and must adhere to strict data protection standards defined by the GDPR, particularly regarding special category data (health data). The primary security objectives identified for this sector are Confidentiality (preventing unauthorized access to patient records), Integrity (ensuring medical data accuracy), and Availability (ensuring systems function during emergencies).

Specific Compliance Monitoring Requirements

To address the specific threats facing healthcare, such as ransomware and data breaches involved in IoMT (Internet of Medical Things), the compliance monitoring module must verify the following sector-specific controls:

- **Patient Data Confidentiality and Encryption:** Given the sensitivity of Protected Health Information (PHI), the monitoring system must verify that strong encryption is applied to patient databases and data in transit.
    - *Required Evidence:* Logs from the Data Integrity and Encryption module confirming that patient records stored or transferred via the Secure Data Exchange Platform utilise validated encryption protocols.
- **IoMT and Medical Device Security:** The proliferation of connected medical devices (pacemakers, insulin pumps) introduces vulnerabilities that traditional IT monitoring may miss.
    - *Required Evidence:* Network traffic analysis logs (Suricata) identifying communication patterns of IoMT devices to detect anomalies indicative of compromise, such as unauthorized external connections.
- **Availability and Ransomware Resilience:** Healthcare operations require continuous up time. Ransomware poses a direct threat to patient safety by locking critical systems.

© CYberSynchorny, 2025

- *Required Evidence:* Backup verification logs (from the Asset Management Policy requirements) confirming that critical medical data is backed up regularly and that restoration tests are successful.

- **Access Control for Medical Personnel:** Access to health records must be restricted based on clinical roles (e.g., doctors, nurses, administrators).
  - *Required Evidence:* Identity Management logs (Keycloak) verifying that Multi-Factor Authentication (MFA) is enforced for all staff accessing EHR systems and that Role-Based Access Control (RBAC) policies are active.

Table 4: Healthcare-Specific Compliance Indicators

Specific Risk / Asset	Monitoring Requirement	Evidence Source	Regulatory Alignment
Electronic Health Records (EHR)	Verify encryption at rest and strict RBAC enforcement.	D4.1 (Wazuh/Sysmon), D6.1 (Keycloak)	GDPR Art. 32, NIS2 Art. 21
Internet of Medical Things (IoMT)	Monitor for unauthorized firmware changes or traffic anomalies.	D4.1 (Suricata/Anomaly Detector)	NIS2 Supply Chain Security
Telehealth Services	Ensure secure communication channels (TLS 1.3) for remote consultations.	D4.1 (Suricata EVE JSON)	HIPAA (Reference), GDPR
Medical Staff Access	Audit logs for unauthorized access attempts to high-profile patient data.	D6.1 (Keycloak), D4.1 (Wazuh)	ISO 27001 A.9, GDPR

These specific requirements inform the configuration of the CYBERGOPLUS module for the Healthcare pilot (Use Case 1), ensuring that the generic technical controls are applied with the necessary rigor for medical environments.

4.2.2 Public Administration Sector Requirements

The Public Administration sector, encompassing local government and municipalities, faces distinct challenges related to the provision of essential services, the management of public records, and the protection of citizen data. As identified in the CyberSynchrony use case analysis, this sector is characterized by a high reliance on legacy systems, a broad attack surface due to e-governance platforms, and strict accountability requirements.

Regulatory and Operational Context

Public administration entities are classified as essential under the NIS2 Directive, necessitating robust measures to ensure service continuity and data integrity. The primary security objectives for this sector include preventing the disruption of critical services (e.g., water supply, emergency response), safeguarding sensitive citizen information against data breaches, and maintaining trust in digital public infrastructure.

Specific Compliance Monitoring Requirements

To address threats such as ransomware, DDoS attacks, and supply chain compromises, the compliance monitoring module must verify the following sector-specific controls:

- **Service Availability and Resilience:** Given the critical nature of municipal services, the monitoring system must verify that e-governance platforms and utility control systems maintain high availability.

© CYberSynchorny, 2025

- *Required Evidence:* Availability logs from the CYBRITE module (Wazuh/Suricata) detecting DDoS attempts and confirming the uptime of critical public-facing portals.

- **Integrity of Public Records:** The unauthorized alteration of public records (e.g., land registry, vital statistics) undermines governance. Monitoring must ensure data immutability.
  - *Required Evidence:* Validation logs from the CROSS-CORE Evidence Integrity System (Blockchain), providing cryptographic proof that stored public records have not been tampered with.
- **Secure Digital Identity Management:** With the shift to digital IDs for citizen services, the system must verify robust authentication mechanisms to prevent identity theft and unauthorized access.
  - *Required Evidence:* Identity Management logs (Keycloak) confirming the enforcement of strong authentication protocols for accessing digital service portals.
- **Supply Chain Security:** Public administrations often rely on numerous third-party vendors for software and infrastructure. Monitoring must track the security posture of these dependencies.
  - *Required Evidence:* Supply chain risk assessment reports (from CYBERRA/SNYK) identifying vulnerabilities in third-party software components integrated into municipal systems.

Table 5: Public Administration-Specific Compliance Indicators

Specific Risk / Asset	Monitoring Requirement	Evidence Source	Regulatory Alignment
E-Governance Portals	Monitor for DDoS signatures and service uptime.	D4.1 (Suricata), D4.1 (Wazuh)	NIS2 Art. 21 (Business Continuity)
Public Records Databases	Verify data integrity via blockchain hashing.	D5.2 (Evidence Integrity System)	GDPR (Integrity), NIS2
Digital Citizen IDs	Audit authentication logs for anomaly detection.	D6.1 (Keycloak), D4.1 (Anomaly Detector)	eIDAS, GDPR
Utility Control Systems (OT)	Monitor traffic at IT/OT boundaries for unauthorized access.	D4.1 (Suricata/Wazuh)	NIS2 (Supply Chain & Network Security)

These requirements guide the configuration of the CYBERGOPLUS module for the Public Administration pilot (Use Case 2), ensuring that compliance monitoring addresses the specific needs of local governance and digital public services. Specifically, in alignment with the European digital identity framework, the monitoring module validates compliance with the **eIDAS Regulation**, specifically regarding trust services and electronic identification. For Public Administration (UC2) and Academia (UC3), the system monitors the integrity of digital signatures and authentication timestamps. This ensures that the "Continuous Threat Detection" principle extends to the validity of digital transactions, a critical requirement for cross-border services within the Digital Single Market.

4.2.3 Research and Academia Sector Requirements

The Research and Academia sector operates under a unique security paradigm characterized by "open by default" networks, decentralized IT management, and a high volume of Bring Your Own Device (BYOD) usage. As defined in Use Case 3 (Cybersecure University), this sector faces significant threats regarding Intellectual Property (IP) theft, ransomware attacks on research repositories, and the compromise of student personal data.

© CYberSynchorny, 2025

Regulatory and Operational Context

While Academic institutions must comply with GDPR regarding student and staff data, they also face specific requirements related to the protection of research integrity and funding grant stipulations . The security objective here is to balance the academic freedom and open information exchange required for research with the stringent controls needed to protect high-value IP and sensitive personal records.

Specific Compliance Monitoring Requirements

To address the specific vulnerabilities of open campus networks and decentralized research labs, the compliance monitoring module must verify the following sector-specific controls:

- **Research Data Integrity and Protection:** Research institutions must ensure that critical research data is not altered or stolen. Monitoring must verify that access to sensitive research segments is restricted and that data integrity is maintained.
    - *Required Evidence:* Integrity verification logs from the Evidence Integrity System (Blockchain) confirming that critical research datasets remain unaltered, alongside access logs (Wazuh) showing restricted entry to IP repositories.
- **Student Record Privacy:** Universities handle vast amounts of Personally Identifiable Information (PII). Monitoring must ensure these records are encrypted and accessed only by authorized administrative staff.
    - *Required Evidence:* Database encryption status logs and Identity Management audits (Keycloak) verifying that Role-Based Access Control (RBAC) separates student records from general faculty access.
- **E-Learning Platform Availability:** The reliability of online learning platforms is critical for continuity. These platforms are frequent targets for DDoS attacks.
    - *Required Evidence:* Network traffic analysis (Suricata) and server health logs (Sysmon/Wazuh) monitoring the availability and latency of Learning Management Systems (LMS).
- **Open Network Security (BYOD):** Given the prevalence of personal devices, the system must monitor for rogue devices and anomalous traffic patterns originating from within the campus network.
    - *Required Evidence:* Network anomaly detection logs (Anomaly Detector IDS) identifying suspicious lateral movement or unauthorized scanning activities within open campus Wi-Fi segments.

Table 6: Research and Academia-Specific Compliance Indicators

Specific Risk / Asset	Monitoring Requirement	Evidence Source	Regulatory Alignment
Research Repositories	Verify data integrity hashing and access restrictions.	D5.2 (Evidence Integrity), D4.1 (Wazuh)	IP Protection Laws, Funding Agreements
Student Information Systems	Audit access logs for PII and verify encryption.	D4.1 (Wazuh), D6.1 (Keycloak)	GDPR (Confidentiality)
E-Learning/LMS	Monitor platform uptime and DDoS signatures.	D4.1 (Suricata), D4.1 (Sysmon)	NIS2 (Business Continuity)

© CYberSynchorny, 2025

Campus Wi-Fi (BYOD)	Detect anomalous traffic flows and rogue access points.	D4.1 (Anomaly Detector/Suricata)	Network Security Best Practices

These requirements define the configuration of the CYBERGOPLUS module for the University pilot (Use Case 3), ensuring that the monitoring framework accommodates the open nature of academic environments while securing critical assets. The operational validation of the CYBERGOPLUS module will be conducted through the cross-sector Use Cases defined in WP8. The tool will be deployed in three distinct pilot environments to demonstrate its adaptability:

- **Use Case 1 (Healthcare):** The module will be integrated with the Hospital Information System (HIS) to validate the "Asset-Centric Protection" principle, specifically monitoring IoMT devices and patient data access (Tool 10).
- **Use Case 2 (Public Administration):** The pilot will focus on the "Continuous Threat Detection" principle, validating the system's ability to detect threats against e-governance portals (Tool 8).
- **Use Case 3 (Academia):** The deployment will test the "Resilience and Recovery" principle, ensuring that open research networks can maintain continuity during simulated attacks (Tool 15).

4.3 Harmonised Cross-Sector Principles

While the specific operational contexts of Healthcare, Public Administration, and Academia differ, the fundamental requirements for cybersecurity compliance under NIS2 and ISO 27001 share a common logical foundation. To ensure the CYberSynchrony platform can scale across these diverse sectors without requiring bespoke development for every new use case, the compliance monitoring framework is built upon four Harmonised Cross-Sector Principles. These principles distil the regulatory obligations into functional categories that apply universally to all essential entities.

These principles serve as the bridge between the high-level legal text (e.g., NIS2 Article 21) and the low-level technical indicators collected by the platform components. Each principle is mapped to specific controls from the DSA 389/2020 framework to ensure regulatory alignment, and then to specific CYberSynchrony functionalities to ensure technical feasibility.

© CYberSynchorny, 2025

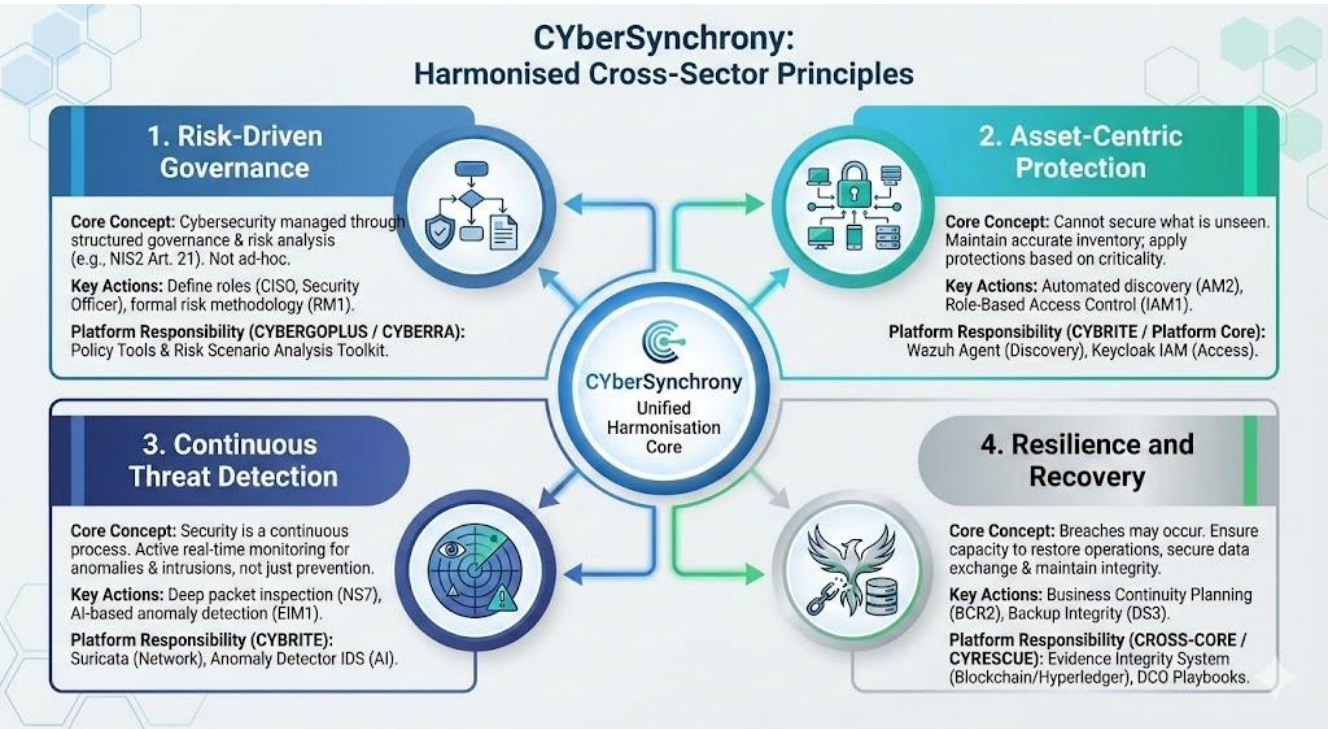

Figure 1: Harmonised Cross-Sector Compliance Principles mapping regulatory concepts to CYberSynchrony platform responsibilities.

4.3.1 Principle 1: Risk-Driven Governance

The first principle mandates that cybersecurity must be managed through a structured governance framework driven by risk analysis rather than ad-hoc decisions. This aligns with the NIS2 requirement for management bodies to approve cybersecurity measures and oversee their implementation.

- **Regulatory Control (DSA 389/2020):**
    - **GOV1 (Roles and Responsibilities):** Defines the obligation to assign specific security roles within the organization.
    - **RM1 (Risk Management Methodology):** Requires a formal methodology for identifying and treating risks.
- **CYberSynchrony Functionality:** The **CYBERGOPLUS** module operationalizes this principle. It provides the "Roles & Responsibilities Matrix" feature described in the requirements analysis, allowing organizations to digitally assign accountability. Furthermore, the **CYBERRA** module supports this by offering the "Risk Scenario Analysis Toolkit," which digitizes the risk assessment process.
- **Monitoring Evidence:** Compliance is verified by checking for the existence of active user accounts with "Admin" or "Security Officer" roles in the Identity Manager and the completion timestamps of digital risk assessment reports.

4.3.2 Principle 2: Asset-Centric Protection

This principle establishes that an organization cannot secure what it cannot see. It mandates the maintenance of an accurate inventory of all digital assets and the application of protective measures such as updates and access controls based on asset criticality.

- **Regulatory Control (DSA 389/2020):**

© CYberSynchorny, 2025

- **AM2 (Inventory of Assets):** Requires the identification and recording of all assets and their ownership.
- **IAM1 (Role-Based Access Control):** Mandates that access to these assets is restricted based on user roles.

- **CYberSynchrony Functionality:** The **CYBRITE** module, specifically through the **Wazuh** component, fulfills this principle by performing automated asset discovery and inventory management. Simultaneously, the **Keycloak Identity Manager** enforces access control policies, ensuring that only authorized users interact with the discovered assets.
- **Monitoring Evidence:** Compliance is monitored by reconciling the list of active endpoints detected by Wazuh agents against the authorized asset list and verifying authentication logs for proper access enforcement.

4.3.3 Principle 3: Continuous Threat Detection

Security is not a static state but a continuous process. This principle requires organizations to implement active monitoring capabilities to detect anomalies, intrusions, and potential incidents in real time, rather than relying solely on preventive measures.

- **Regulatory Control (DSA 389/2020):**
  - **NS7 (Intrusion Detection):** Requires measures to detect and prevent unauthorized access to the network.
  - **EIM1 (Event Readiness and Detection):** Mandates the capability to detect events that could threaten security.
- **CYberSynchrony Functionality:** The platform addresses this through the **Integrated Cybersecurity Monitoring Suite** (D4.1). **Suricata** performs deep packet inspection to identify network threats, whilst the **Anomaly Detector IDS** utilises AI-based logic to flag deviations in traffic patterns that may indicate novel attacks.
- **Monitoring Evidence:** Compliance is evidenced by the continuous stream of EVE JSON logs and alert records generated by these components, proving that the detection mechanisms are active and functioning.

4.3.4 Principle 4: Resilience and Recovery

The final principle acknowledges that breaches may occur and mandates that organizations must have the capacity to restore operations. This covers business continuity planning, backup management, and the integrity of data required for recovery.

- **Regulatory Control (DSA 389/2020):**
  - **BCR2 (Business Continuity Plan):** Requires a plan to maintain critical functions during a crisis.
  - **DS3 (Backup and Recovery):** Mandates regular backups and the ability to restore information.
- **CYberSynchrony Functionality:** The **CROSS-CORE** module supports resilience by facilitating secure data exchange and coordination during incidents . Additionally, the **Evidence Integrity System** (Hyperledger) ensures that the logs and backup hashes required for recovery have not been tampered with, ensuring a trusted restoration point.
- **Monitoring Evidence:** Compliance is verified through the "Evidence Integrity System" logs which validate the immutability of critical records, and through the tracking of incident response activities within the **Defensive Cyber Operations (DCO)** playbooks.

© CYberSynchorny, 2025

4.4 Mapping of Principles to CYberSynchrony Responsibilities

The following table summarizes the harmonization of these principles, mapping the regulatory requirement to the specific technical component within the CYberSynchrony ecosystem that assumes responsibility for fulfilling it.

Table 7: Mapping of Harmonised Principles to Platform Responsibilities

Harmonised Principle	Regulatory Reference (DSA 389/2020)	CYberSynchrony Module Responsibility	Key Component
1. Risk-Driven Governance	GOV1, RM1	CYBERGOPLUS / CYBERRA	Policy Tools, Risk Assessment Toolkit
2. Asset-Centric Protection	GOV1, RM1	CYBRITE / Platform Core	Wazuh Agent, Keycloak IAM
3. Continuous Threat Detection	NS7, EIM1	CYBRITE	Suricata, Anomaly Detector IDS
4. Resilience and Recovery	BCR2, DS3	CROSS-CORE / CYRESCUE	Evidence Integrity System, DCO Playbooks

Specifically, the principles are operationalized through the 15 policy tools defined in the Cybersecurity Policy Toolkit (D6.3). This alignment ensures that every technical principle monitored by the system is backed by a formal governance policy:

- **Principle 1 (Risk-Driven Governance):** Operationalized by **Tool 1** (Information Security Strategy), **Tool 2** (Information Security Governance Policy), and **Tool 3** (Risk Management Policy & Methodology).
- **Principle 2 (Asset-Centric Protection):** Operationalized by **Tool 4** (Asset Management Policy), **Tool 5** (Supplier and Third-Party Management Policy), **Tool 6** (Access Control Policy), **Tool 7** (Vulnerability and Patch Management Policy), **Tool 8** (Network Security Policy), **Tool 9** (Systems & Applications Security Policy), and **Tool 10** (Data Protection Policy).
- **Principle 3 (Continuous Threat Detection):** Operationalized by **Tool 3** (Risk Management Policy & Methodology), **Tool 12** (Human Resources Security, Training & Awareness Policy), **Tool 13** (Physical Security Policy), and **Tool 14** (Incident and Event Management Policy).
- **Principle 4 (Resilience and Recovery):** Operationalized by **Tool 15** (Business Continuity and Disaster Recovery Policy).

The mapping presented above serves as the operational "bridge" between the abstract regulatory requirements of the NIS2 Directive and the concrete technical configurations monitored by the CYBERGOPLUS module. While the Harmonised Principles defined in Section 4.3 provide the high-level logic for compliance, categorizing obligations into Governance, Protection, Detection, and Resilience, it is the **Cybersecurity Policy Toolkit (D6.3)** that translates these concepts into enforceable organizational rules.

This structure ensures a complete chain of custody for compliance evidence. By operationalizing **Principle 1 (Risk-Driven Governance)** through **Tools 1–3**, the framework ensures that security is not treated as an ad-hoc technical task but as a board-level strategic imperative, directly satisfying the "Management Responsibility"

© CYberSynchorny, 2025

requirements of NIS2 Article 20. Similarly, the heavy concentration of tools under **Principle 2 (Asset-Centric Protection** spanning **Tools 4 through 10** reflects the operational reality that the majority of auditable controls are preventive in nature, focusing on the correct configuration of assets, identities, and networks.

Furthermore, the explicit mapping of **Principle 3 (Continuous Threat Detection)** to **Tools 12–14** shifts the focus from purely preventive security to the "active defense" posture required by modern regulations. It mandates that organizations not only possess security policies but also active mechanisms for Incident Management and Assurance Auditing. Finally, **Principle 4 (Resilience and Recovery)**, anchored by **Tool 15**, closes the loop by ensuring that when preventive and detective measures fail, a formally defined Business Continuity plan is available to restore operations.

© CYberSynchorny, 2025

5 CYberSynchrony Compliance Monitoring Approach (High-Level)

This chapter outlines the operational methodology used to implement the "Real-Time Compliance Oversight" capability defined in Task 6.7. Building upon the regulatory foundations and harmonized principles established in the previous chapters, this section defines how the CYberSynchrony platform technically achieves continuous auditing. The approach moves away from static, document-based compliance towards a dynamic model where technical evidence serves as the primary validation mechanism. This methodology is designed to be agnostic of the specific underlying technology of the end-user while remaining rigorous enough to satisfy the requirements of the NIS2 Directive and ISO 27001 standards.

5.1 Objectives of Compliance Monitoring

The primary objective of the compliance monitoring framework is to provide stakeholders with an accurate, real-time view of their cybersecurity posture, minimizing the latency between a non-compliant event and its remediation. Specifically, the monitoring approach aims to achieve the following four operational objectives:

- **Enable Real-Time Visibility:** To transition from periodic audits (annual or quarterly) to continuous monitoring, providing instant alerts when a specific control fails or a policy is violated.
- **Automate Evidence Collection:** To reduce the administrative burden on cybersecurity staff by automating the gathering of technical logs, configurations, and artifacts required for audits, addressing the resource constraints identified in the end-user analysis.
- **Ensure Cross-Sector Consistency:** To apply a unified auditing logic that allows for comparable compliance scoring across different sectors (Healthcare, Public Administration, Academia), facilitating the "Harmonization" objective of Work Package 6.
- **Support Risk-Based Prioritization:** To link compliance findings directly to risk scenarios, ensuring that organizations prioritize the remediation of non-compliance issues that pose the greatest threat to their critical assets.

5.2 Pipelines Compliance Domains and Assessment Areas

The core purpose of defining specific compliance domains within the CYberSynchrony platform is to translate granular technical telemetry into high-level reporting that is understandable to management boards and non-technical decision-makers. As identified in the end-user requirement analysis (D2.2), a critical gap exists in generating "Management/Board Reporting" that provides a clear view of compliance status without requiring manual aggregation of technical logs.

It is important to note that the CYberSynchrony tool produces compliance data specifically derived from the active components integrated into the ecosystem (e.g., Wazuh, Suricata, Keycloak, SNYK). The platform does not promise a "full" audit of every administrative or physical control within an organization; rather, it provides continuous validation for the specific digital controls that can be monitored via the project's technical architecture.

The assessment areas are structured to generate reports like the survey outcomes analyzed in D2.2, specifically addressing the need for standardized content elements such as risk status, initiative progress, and compliance gaps. By mapping the technical evidence described in Section 4.1.1 to the policy domains defined in D6.3, the platform assesses the following specific areas:

- **Governance & Strategy:** Assessments focus on the assignment of security roles and the verification of policy acknowledgments by staff, aligned with the *Information Security Governance Policy* (Tool 2) .
- **Asset Security:** Monitoring focuses on the reconciliation of discovered assets against authorized inventories and the verification of maintenance schedules, aligned with the *Asset Management Policy* (Tool 4).

© CYberSynchorny, 2025

- **Identity Control:** Assessments track the enforcement of Multi-Factor Authentication (MFA) and the management of privileged accounts, aligned with the *Access Control Policy* (Tool 6) .
- **Threat Protection:** Monitoring evaluates the active status of anti-malware agents, firewall configurations, and intrusion detection systems, aligned with the *Systems & Applications Security Policy* (Tool 9) and *Network Security Policy* (Tool 8) .
- **Vulnerability Status:** Assessments report on the presence of unpatched critical vulnerabilities and software dependencies, aligned with the *Vulnerability and Patch Management Policy* (Tool 7).
- **Resilience:** Monitoring verifies the successful execution of backup routines and the completion of business continuity drills, aligned with the *Business Continuity and Disaster Recovery Policy* (Tool 15) .

5.3 Indicators, Metrics and Maturity Levels

To transition compliance from a qualitative assessment to a quantitative science, the CYberSynchrony platform utilizes a hierarchical measurement model. This model aggregates low-level technical signals (Indicators) into operational performance measures (Metrics) and finally into high-level strategic targets (KPIs). This structure ensures that the technical evidence collected by components like Wazuh and Suricata directly supports the validation of the project's Grant Agreement objectives.

5.3.1 Operational Compliance Indicators (KCIs)

Key Compliance Indicators (KCIs) serve as the atomic units of the monitoring framework. A KCI represents a specific, binary check performed against a technical asset to verify a single control requirement from the DSA 389/2020 framework. These indicators are derived directly from the raw telemetry produced by the platform's security tools.

The system utilizes the following logic for KCI generation:

- **Input:** Raw Log (e.g., Suricata EVE JSON, Wazuh Syslog).
- **Logic:** Boolean evaluation against a policy threshold (e.g., tls_version >= 1.2).
- **Output:** Pass/Fail flag with timestamp and Asset ID.

5.3.2 Mapping Controls to KPIs

The following table presents the technical mapping of regulatory controls to specific digital evidence and the associated Key Performance Indicators (KPIs) defined in the CYberSynchrony Description of Action (DoA). This mapping reconciles the operational requirements identified in D2.2 (KPIRs) with the monitoring capabilities established in D4.1.

Table 8: Comprehensive Compliance Indicator Map

Regulatory Control (DSA 389/2020)	CYberSynchrony Evidence Source	Technical Evidence Artifact	Metric / Measurement Logic	Linked DoA KPI / Requirement
AM2: Inventory of Assets	Wazuh (D4.1)	syscollector inventory logs (JSON)	Unmanaged Asset Ratio: Percentage of active IPs detected by Suricata but not registered in Wazuh inventory.	KPI 9.1: Policy Compliance Rate / KPIR3

© CYberSynchorny, 2025

VM1: Vulnerability Scanning	Wazuh / SNYK (D4.1/D6.1)	CVE Vulnerability Reports (Severity: Critical/High)	Mean Time to Remediate (MTTR): Average time between CVE detection timestamp and patch application timestamp.	KPI 1.5 / KPI 3.5: Platform Vulnerability Remediation Time / KPIR4
IAM4: Strong Authentication	Keycloak (D6.1)	Authentication Event Logs (type=LOGIN, mfa=true/false)	MFA Coverage: Percentage of successful logins performed with Multi-Factor Authentication enabled.	KPI 9.1: Policy Compliance Rate / KPIR12
EIM1: Incident Detection	Suricata / Anomaly Detector (D4.1)	Alert Logs (event_type: alert, severity: 1)	Detection Latency: Time delta between packet ingress timestamp and alert generation timestamp.	KPI 2.2: Incident Detection Time / KPIR6
EIM2: Incident Analysis	DCO Playbooks (D4.1)	Incident Ticket Status Changes (Open -> Closed)	Resolution Rate: Percentage of high-severity incidents closed within the SLA window (e.g., 24 hours).	KPI 2.4: Incident Resolution Rate / KPIR8
TA2: Awareness Training	Cybergate (D6.2)	User Mission Completion Logs & Scores	Training Coverage: Percentage of active directory users who have completed mandatory simulation modules.	KPI 8.1: Cybersecurity Training Coverage / KPIR10
DS3: Backup and Recovery	Evidence Integrity System (D5.2)	Blockchain Transaction Hash (Hyperledger)	Integrity Verification Rate: Percentage of backup archives with valid, unaltered blockchain hashes.	KPI 5.1: Number of Risk Monitoring Services Provided

5.3.3 Maturity Levels

To translate these metrics into a management-friendly format, the platform aggregates KCIs into a five-level maturity scale. This scale aligns with the "Cybersecurity Maturity Controls" decision (K.D.P. 245/2024) referenced in the Risk Management Policy .

1. **Initial (0-20% Compliance):** Controls are non-existent or ad-hoc. Evidence shows high rates of unmanaged assets and open critical vulnerabilities.
2. **Managed (21-40% Compliance):** Controls are documented but implementation is partial. MFA is active for administrators but not general staff.
3. **Defined (41-60% Compliance):** Controls are standardized. Automated scanning (VM1) is active, but remediation times (MTTR) exceed targets.
4. **Quantitatively Managed (61-80% Compliance):** Controls are measured and controlled. KPIs such as Incident Detection Time (KPI 2.2) are consistently met.

© CYberSynchorny, 2025

5. **Optimizing (81-100% Compliance):** Focus on continuous improvement. Advanced anomaly detection (EIM1) is active and integrated with automated response playbooks.

5.4 Evidence Bases: Policy, Implementation, and Operational Artefacts

To ensure the compliance monitoring framework is auditable and transparent, the CYberSynchrony platform categorizes evidence into three distinct layers: Policy (Governance), Implementation (Configuration), and Operational (Runtime). This structure ensures that the system validates not only that a rule exists on paper (Policy), but also that technical controls are correctly deployed (Implementation) and functioning continuously under real-world conditions (Operational).

The following subsections detail the specific technical tools and project deliverables that serve as the authoritative sources for each category of evidence.

5.4.1 Policy and Governance Evidence

The foundational layer of compliance consists of the formal rules, risk assessments, and strategic decisions approved by the organization's management. This evidence is primarily static or semi-static, changing only when organizational strategies are reviewed. The CYBERGOPLUS module monitors this layer by verifying the existence, approval status, and currency of specific governance artifacts generated by the CYberSynchrony toolkits.

- **Cybersecurity Policy Definitions:** The primary source of governance evidence is the **Cybersecurity Policy Toolkit (D6.3)**. The monitoring system verifies the adoption of the 15 core policy tools defined in this deliverable, specifically checking for the "Information Security Strategy" (Tool 1) and "Information Security Governance Policy" (Tool 2) . Compliance is measured by the presence of digital signatures or timestamps indicating formal adoption by the Board or CISO.
- **Risk Assessment Records:** Compliance with the "Risk-Driven Governance" principle is evidenced by artifacts from the **Risk Scenario Analysis Toolkit (D3.2)**. The specific evidence required includes the completed "Asset-Based Risk Assessment Workbook" and the "Risk Register". The monitoring system checks the "Last Updated" timestamp of these documents to ensure risk assessments are conducted at least annually as required by the NIS2 methodologies.
- **Data Classification Schemes:** To verify data governance, the system retrieves evidence regarding information labelling protocols. This relies on the **Data Protection Policy (Tool 10)** from D6.3, which mandates the use of classification schemes such as the Traffic Light Protocol (TLP). The evidence collected is the configuration of data tags within the Secure Data Exchange Platform (D5.1), confirming that data streams are actively tagged (e.g., TLP:RED, TLP:AMBER) before transmission.

5.4.2 Implementation and Configuration Evidence

While policy evidence confirms that a rule has been mandated, implementation evidence verifies that the necessary technical controls have been correctly configured and deployed within the IT environment. This layer of the compliance monitoring framework focuses on the "As-Built" state of the infrastructure, auditing configuration files, rule definitions, and system settings to ensure they align with the authorized policies.

The CYBERGOPLUS module ingests this evidence directly from the configuration repositories and management consoles of the platform's security tools.

- **Identity and Access Configurations:** To verify compliance with the *Access Control Policy*, the system audits the active configuration of the **Keycloak Identity Manager (D6.1)**. Specific evidence artifacts include the JSON export of the "Realm Settings," which proves that Multi-Factor Authentication (MFA) is set to "Required" for privileged user groups and that password complexity policies (e.g., minimum length, special characters) are technically enforced at the directory level.
- **Endpoint Security Rulesets:** Implementation evidence for asset protection is derived from the configuration of the **Wazuh Manager (D4.1)**. The monitoring system parses the active ossec.conf and

© CYberSynchorny, 2025

agent.conf files to verify that File Integrity Monitoring (FIM) modules are enabled for critical system paths (e.g., /etc/passwd, System32) and that the vulnerability detector module is active with an up-to-date CVE database.

- **Network Detection Signatures:** Compliance with network security standards is evidenced by the active configuration of the **Suricata IDS (D4.1)**. The system audits the suricata.yaml configuration file and the active rule files to confirm that the "Emerging Threats" (ET Open) ruleset is loaded and that the detection engine is configured to inspect traffic on all relevant network interfaces (e.g., eth0, docker0).
- **Infrastructure-as-Code (IaC) Manifests:** For environments deployed via the **CYberSynchrony Integration Blueprint (D8.1)**, compliance is verified through the audit of Kubernetes manifests. The system checks the kube-apiserver.yaml and Ingress Controller configurations (D6.1) to ensure that "Network Policies" are defined to restrict pod-to-pod communication and that TLS certificates are strictly enforced via cert-manager.

5.4.3 Operational and Runtime Evidence

The final layer of the evidence hierarchy captures the dynamic state of the environment. While configuration evidence proves a control is *set* to function, operational evidence proves it is *actively functioning* at a specific point in time. This data is generated continuously by the platform's detection engines, response agents, and user interaction modules.

The CYBERGOPLUS module ingests these runtime artifacts to calculate the "Operational Compliance Indicators" (KCIs) defined in Section 5.3.1.

- **Real-Time Threat Detection Logs:** To verify the "Continuous Threat Detection" principle, the system requires proof that monitoring engines are actively inspecting traffic and host activity.
    - **Evidence:** The primary artifact is the stream of **Suricata EVE JSON** logs from the CYBRITE module (D4.1), which documents every inspected network flow and alert. Additionally, **Wazuh Alert Logs** provide evidence of active endpoint monitoring, detailing specific security events such as "Authentication Failure" or "File Integrity Change" .
    - **Regulatory Alignment:** This satisfies the NIS2 requirement for "handling incidents" and "security in network and information systems" by proving detection capabilities are operational.
- **Incident Response Execution Records:** Compliance with resilience standards requires evidence that the organization not only detects threats but responds to them according to procedure.
    - **Evidence:** The **Automated Response Toolkit (D4.2)** generates "Playbook Execution Logs" within the Defensive Cyber Operations (DCO) module. These logs timestamp the exact moment an automated mitigation (e.g., isolating a host) was triggered and completed.
    - **Regulatory Alignment:** This provides the necessary audit trail for "Incident Handling" under NIS2 Article 21.
- **Data Integrity and Exchange Verification:** For the "Resilience and Recovery" principle, the system must verify that critical data remains unaltered during operations.
    - **Evidence:** The **Secure Data Exchange Platform (D5.1)** and **Evidence Integrity System (D5.2)** produce immutable transaction records anchored in the Hyperledger blockchain. The specific artifact is the "Blockchain Transaction Hash," which serves as cryptographic proof that a specific log entry or shared intelligence file has maintained its integrity from creation to storage.
    - **Regulatory Alignment:** This addresses the GDPR requirements for data integrity and the NIS2 requirements for secure supply chain and data sharing.

© CYberSynchorny, 2025

- **Human-Centric Security Metrics:** To validate the effectiveness of the "Cybersecurity Education" objective, the system monitors real-time user behavior and training performance.
    - **Evidence:** The **Cybergate (D6.2)** platform generates "Mission Outcome Reports" and "Simulation Scores" (e.g., Phishing Defense Success Rate) for every training session. These runtime metrics demonstrate active staff engagement and skill application, moving beyond simple attendance records.
    - **Regulatory Alignment:** This fulfils the "Basic Cyber Hygiene and Training" requirement of NIS2.

To synthesize the methodology detailed in this chapter, Figure 3 presents the overall functional architecture of the compliance monitoring framework. This diagram illustrates how the CYBERGOPLUS module acts as the central processing engine, ingesting raw evidence from the various CYberSynchrony components, validating it against the governance rules defined in D6.3, and ultimately transforming this technical data into the operational indicators, strategic KPIs, and management reports described in the preceding sections.

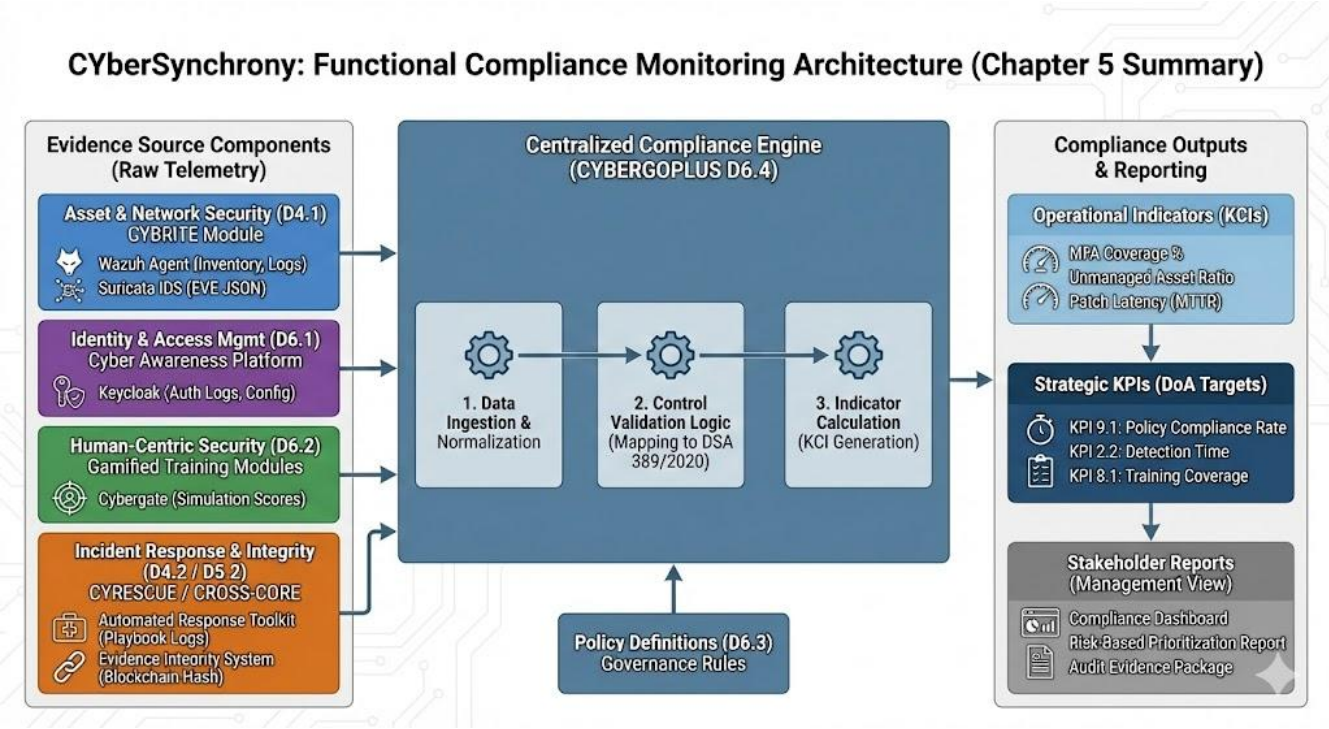

Figure 2: Functional Compliance Monitoring Architecture detailing the flow from raw telemetry to stakeholder reporting.

© CYberSynchorny, 2025

6 System Specifications and Integration Requirements

This chapter translates the high-level compliance methodology into concrete engineering specifications. It defines the functional capabilities the CYBERGOPLUS module must possess, the technical standards it must adhere to, and the integration interfaces required to ingest evidence from the wider CYberSynchrony ecosystem.

6.1 Functional Requirements

The functional specifications for the CYBERGOPLUS module are derived directly from the "Must Have" requirements identified during the End-User Requirements Analysis (D2.2) and the specific governance needs of the NIS2 Directive. The module is designed to fulfill three core functional domains: Policy Governance, Automated Auditing, and Remediation Management.

6.1.1 Policy and Governance Management Functions

To address the end-user requirement for a centralized compliance repository (SQ8), the system must provide digital management for the entire policy lifecycle.

- **REQ-FUNC-01: Policy Registry and Versioning** The system shall provide a digital registry to store, version, and distribute the 15 Cybersecurity Policy Tools defined in D6.3 (e.g., Information Security Strategy, Access Control Policy). The system must maintain a history of policy revisions, recording the timestamp and the identity of the approving officer (e.g., CISO or Board Member) to satisfy audit trails.
- **REQ-FUNC-02: Role Assignment Matrix** The system shall provide an interactive matrix to map regulatory roles (e.g., NIS Officer, DPO, Risk Manager) to specific user identities managed in the Keycloak Identity Manager. This function addresses requirement SQ9 (Roles & Responsibilities Matrix) and ensures accountability for specific compliance domains.
- **REQ-FUNC-03: Framework Mapping** The system shall natively map organizational controls against the specific NIS2 Framework Areas (e.g., Supply Chain Security, Incident Handling) as defined in requirement SQ10. This allows users to view their compliance status filtered by specific NIS2 articles or ISO 27001 domains.

6.1.2 Automated Auditing and Assessment Functions

To reduce the manual workload of gathering audit evidence (SQ1), the system must automate the ingestion and validation of technical telemetry.

- **REQ-FUNC-04: Automated Evidence Ingestion** The system shall automatically retrieve JSON-formatted log data from the CYBRITE (Wazuh/Suricata) and CROSS-CORE modules at user-defined intervals (e.g., hourly, daily). This function replaces manual log collection for controls such as asset inventory and vulnerability status.
- **REQ-FUNC-05: Dynamic Asset Reconciliation** The system shall automatically compare the list of "Active Assets" discovered by Wazuh agents against the "Authorized Inventory" to identify unmanaged devices. This function supports the verification of Asset Management controls (AM1, AM2).
- **REQ-FUNC-06: Vulnerability Risk Mapping** The system shall ingest CVE reports from Wazuh and SNYK and automatically map them against the organization's defined risk appetite (Low, Medium, High, Critical) to calculate the "Unmitigated Vulnerability" score. This fulfills requirement SQ1 (Internal Regulatory Assessments) by providing real-time risk visibility.

© CYberSynchorny, 2025

6.1.3 Findings Management and Reporting Functions

To satisfy the requirement for management-level reporting (SQ5) and issues management (SQ3), the system must process raw data into actionable insights and track remediation.

- **REQ-FUNC-07: Automated Finding Generation** The system shall automatically generate a "Non-Compliance Finding" ticket when a Key Compliance Indicator (KCI) falls below the defined threshold (e.g., if "MFA Coverage" drops below 100% for admins). This ensures that deviations are flagged instantly.
- **REQ-FUNC-08: Remediation Workflow Tracking** The system shall provide a workflow for assigning remediation actions to specific users, tracking due dates, and recording the closure of findings (SQ4). This allows the organization to demonstrate "continuous improvement" to auditors.
- **REQ-FUNC-09: Board-Level Dashboard** The system shall provide a real-time visualization dashboard displaying the current maturity level (1-5) and compliance percentages. This dashboard must be exportable in standard formats (PDF, CSV) to support the "Management/Board Reporting" requirement (SQ5).

6.2 Technical Specifications

The CYBERGOPLUS module is engineered as a cloud-native application, designed to operate within the Kubernetes-based infrastructure defined in the CYberSynchrony Integration Blueprint. This section details the architectural patterns, technology stack, and security standards required for its implementation.

6.2.1 Architecture Pattern

The system adopts a microservices architecture to ensure modularity and scalability.

- **Containerization:** All application components are packaged as Docker containers, ensuring consistency across development, testing, and production environments.
- **Orchestration:** Deployment is managed via Kubernetes (K8s), which handles service discovery, load balancing, and automated failover. This directly addresses the non-functional requirement for "Automated Failover" (NF4) identified in the end-user analysis.
- **Service Mesh:** Inter-service communication is managed through a service mesh (e.g., Istio or Linkerd) to provide traffic management and observability without modifying application code.

6.2.2 Technology Stack

The development stack is selected to ensure compatibility with the existing CYberSynchrony components (Wazuh, Keycloak) and to facilitate high-performance data processing.

- **Backend Framework:** The core logic is developed using **Python** (FastAPI or Django) or **Java** (Spring Boot). Python is preferred for data processing tasks due to its extensive library support for JSON parsing and API integration, aligning with the Wazuh backend structure.
- **Frontend Framework:** The user interface is built using **React** or **Vue.js**. This frontend is designed to be integrated directly into the main CYberSynchrony Platform UI as a micro-frontend, ensuring a unified user experience and "Easy Navigation" (FR14).

6.2.3 Data Storage Strategy

To handle the diverse types of data required for compliance monitoring, the system utilizes a polyglot persistence strategy.

© CYberSynchorny, 2025

- **Relational Database (SQL): PostgreSQL** is used to store structured, relational data such as policy definitions, user role assignments, and finding tickets. This ensures transactional integrity for governance records.
- **Log Storage (NoSQL): Elasticsearch** or **OpenSearch** is utilized for the storage and rapid querying of high-volume log evidence ingested from Wazuh and Suricata. This aligns with the indexing architecture already deployed in the Monitoring Suite (D4.1).

6.2.4 Security Standards

The technical implementation adheres to strict security standards to ensure the integrity and confidentiality of compliance data.

- **Transport Security:** All internal (service-to-service) and external (user-to-service) communications must be encrypted using **TLS 1.2** or higher. This satisfies the requirement for "Secure Communication Protocols" (NS4).
- **Authentication & Authorization:** The module does not manage user credentials locally. Instead, it relies on **OpenID Connect (OIDC)** integration with the **Keycloak Identity Manager** (D6.1) for all authentication requests. Access to specific compliance data is controlled via JWT (JSON Web Token) claims derived from Keycloak roles.

6.3 Integration Specifications

To function as the central oversight engine, CYBERGOPLUS requires standardized interfaces to exchange data with the specialized security modules distributed across the CYberSynchrony ecosystem. These integration specifications define the protocols, authentication methods, and data formats necessary to ingest evidence and export compliance status.

6.3.1 Integration with Data Sources (Northbound/Southbound)

The module ingests technical evidence via RESTful APIs handling JSON payloads, aligning with the "Supported Data Formats" requirement (FR20) defined in the end-user requirements.

- **Input from CYBRITE (Wazuh/Suricata):** The system interfaces with the Wazuh Manager (D4.1) to retrieve asset and vulnerability data.
    - **Protocol:** HTTPS / REST API
    - **Authentication:** JWT (JSON Web Token) via the Wazuh API login endpoint.
    - **Specific Endpoints:**
        - GET /agents: To retrieve the list of active endpoints for inventory reconciliation (AM2).
        - GET /vulnerability/{agent_id}: To retrieve active CVEs for vulnerability compliance (VM1).
        - GET /syscollector: To retrieve hardware and OS details for configuration auditing.
    - **Data Format:** JSON output containing asset IDs, timestamps, and event types.
- **Input from CROSS-CORE (Evidence Integrity):** The system interfaces with the Evidence Integrity System (D5.2) to verify the immutability of logs.
    - **Protocol:** gRPC / HTTPS
    - **Function:** Log Integrity Verification. The compliance module queries the Hyperledger ledger to confirm that the hash of a specific evidence log matches the stored immutable record.

© CYberSynchorny, 2025

6.3.2 Integration with Identity Services

- **Service:** Keycloak Identity Manager (D6.1) .
- **Integration Type:** OpenID Connect (OIDC) / SAML .
- **Data Flow:** The compliance module does not store user credentials. Instead, it queries Keycloak to validate:
    - **MFA Status:** Verifying that the acr (Authentication Context Class Reference) claim in the token indicates strong authentication (IAM4) .
    - **Role Assignment:** Mapping Keycloak roles (e.g., cis_admin, auditor) to the permissions defined in the CYBERGOPLUS Role Assignment Matrix .

6.3.3 Integration with Presentation Layer

- **Target:** CYberSynchrony Platform UI (D8.1).
- **Mechanism:** The compliance module exposes a secure API gateway that allows the main dashboard to fetch real-time KCI metrics (e.g., "Policy Compliance Rate") for visualization in the unified view .
- **Data Object:** ComplianceStatusJSON containing the maturity level, list of open findings, and current KPI scores .

The abovementioned required data models are described in appendix I.

The diagram below indicates the overall architecture of CYBERGOPLUS:

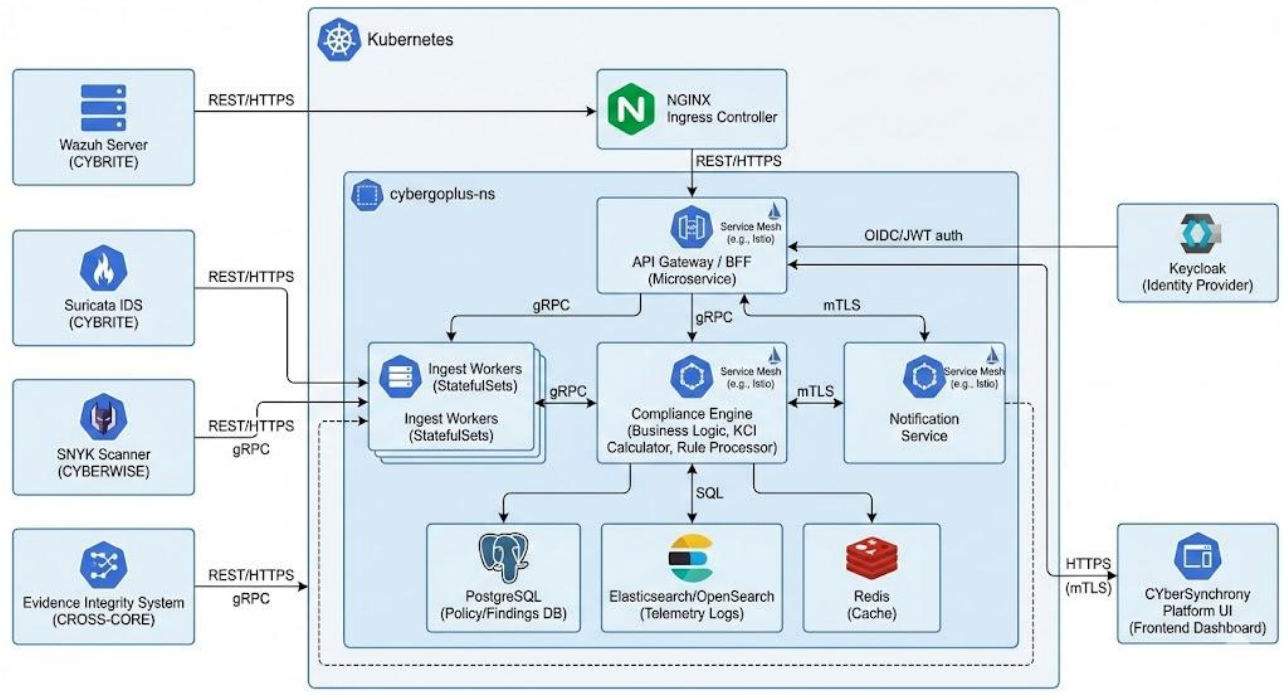

Figure 3: CYBERGOPLUS Technical Architecture. This diagram illustrates the module's microservices deployment within Kubernetes, detailing data ingestion from external sources (CYBRITE, CROSS-CORE), internal processing via the Compliance Engine, and integration with Keycloak for identity and polyglot storage for data persistence.

© CYberSynchorny, 2025

7 Conclusions and Roadmap to v2

This chapter concludes the initial definition phase of the CYBERGOPLUS compliance monitoring module. It summarizes the foundational work established in this deliverable (D6.4) and outlines the concrete steps required to transition from architectural design to active development and pilot validation, culminating in the final v2 release (D6.8).

7.1 Summary of v1 Achievements (Definition Phase)

Deliverable 6.4 has established the necessary theoretical and technical foundations for real-time compliance oversight within the CYberSynchrony ecosystem. By analyzing end-user requirements (D2.2) and regulatory baselines like NIS2, this document has defined a harmonized monitoring approach that balances cross-sector consistency with specific domain needs.

Key achievements of this v1 definition include:

- **Regulatory Mapping:** The translation of high-level legal requirements into measurable technical indicators connected to platform telemetry (e.g., mapping NIS2 Article 21 to Wazuh logs).
- **Functional Architecture:** The definition of the centralized CYBERGOPLUS engine, detailing how it ingests, normalizes, and assesses evidence from diverse sources like CYBRITE and CROSS-CORE.
- **Technical Specifications:** The delivery of a cloud-native, microservices-based blueprint ready for development on the Kubernetes infrastructure defined in WP8.

7.2 Immediate Next Steps (Development Phase M19–M30)

Following the submission of this blueprint, Task 6.7 shifts focus to the active engineering of the defined modules. The immediate next steps involve transforming the architectural specifications into working software components.

Primary activities for the next period include:

- **Environment Setup:** Establishing the dedicated cybergoplus-ns namespace within the development Kubernetes cluster and configuring base services (PostgreSQL, Kafka).
- **Connector Development:** Coding the southbound adapters required to interface with the Wazuh REST API and Keycloak OIDC endpoints.
- **Engine Logic Implementation:** Developing the core business logic in Python to process incoming JSON telemetry and calculate the operational KCIs defined in Chapter 5.
- **Alpha Testing:** Conducting initial integration tests with technical partners (BYTE, IANUS) to validate data ingestion flows before pilot deployment. Capacity-Building Needs

7.3 Cycle Objectives for D6.8 Compliance Monitoring v2 (Validation Phase)

The final output of this task will be Deliverable 6.8, "Compliance Monitoring v2," due in Month 36. While v1 defined the system, v2 will report on its operational validation in real-world scenarios.

The objectives for the final release are to present:

- **Mature Monitoring Data:** Moving beyond baseline assessments to provide longitudinal compliance data collected from the pilot use cases over a sustained period.
- **Validated KPIs:** Reporting on the established project indicators (e.g., KPI 9.1 Policy Compliance Rate) based on actual measurements rather than estimates.
- **Integrated User Experience:** Demonstrating the seamless integration of compliance dashboards within the main CYberSynchrony UI.

© CYberSynchorny, 2025

- **Refined Calibration:** Updating threat detection thresholds and risk scoring logic based on feedback gathered during pilot operations in Healthcare, Governance, and Academic sectors.

© CYberSynchorny, 2025

8 References

[1] Author, Title, Date, URL or page address European Parliament and Council, **Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)**, 14 December 2022. URL: http://data.europa.eu/eli/dir/2022/2555/oj

[2] European Parliament and Council, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (GDPR), 27 April 2016. URL: http://data.europa.eu/eli/reg/2016/679/oj

[3] International Organization for Standardization, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, October 2022. URL: https://www.iso.org/standard/27001

[4] Digital Security Authority (DSA), **The Security of Networks and Information Systems (Security Measures of Operators of Essential Services and Operators of Critical Information Infrastructure) Decision, 2020 (K.D.P. 389/2020)**, August 2020. URL: https://dsa.cy/en/legislation/decisions

[5] National Institute of Standards and Technology (NIST), **Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)**, September 2020. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/final

[6] European Union Agency for Cybersecurity (ENISA), "Cybersecurity Standards and National Authorities". URL: https://www.enisa.europa.eu/audience/national-eu-authorities

[7] CYberSynchrony Deliverable "D2.2 Cybersecurity landscape and threat analysis end-user requirement analysis and use case definition and CYberSynchrony Framework", Submitted M16

[8] CYberSynchrony Deliverable "D3.2 Risk Scenario Analysis Toolkit", Submitted M16

[9] CYberSynchrony Deliverable "D4.1 Integrated Cybersecurity Monitoring Suite", Submitted M16

[10] CYberSynchrony Deliverable "D4.2 Automated Response Toolkit", Submitted M12

[11] CYberSynchrony Deliverable "D5.2 Evidence Integrity System", Submitted M13

[12] CYberSynchrony Deliverable "D6.1 Cyber Awareness Platform", Submitted M19

[13] CYberSynchrony Deliverable "D6.2 Gamified Training Modules", Submitted M19

[14] CYberSynchrony Deliverable "D6.3 Cybersecurity Policy Toolkit", Submitted M19

[15] CYberSynchrony Deliverable "D8.1 CYberSynchrony Integration Blueprint Use Case Portfolio", Submitted M16

© CYberSynchorny, 2025

Annex I: Technical Interface Specifications

Ss This annex provides the specific data models required for the integration of CYBERGOPLUS. *Note: These schemas represent the standard data structures for the open-source components defined in the architecture. Exact field names may require adjustment during the v2 implementation phase based on specific versioning.*

III.1 Vulnerability Ingestion Schema (Wazuh/CYBRITE)

The compliance module ingests vulnerability data from the Wazuh Manager via the REST API.

- **Source:** D4.1 Integrated Cybersecurity Monitoring Suite v1.
- **Endpoint:** GET /vulnerability/{agent_id}

```
JSON
{
 "data": {
  "agent_id": "001",
  "vulnerabilities": [
   {
    "cve": "CVE-2023-44487",
    "title": "HTTP/2 Rapid Reset",
    "severity": "Critical",
    "cvss": {
     "v3": { "base_score": 7.5 }
    },
    "package": {
      "name": "nginx",
      "version": "1.18.0"
    },
    "status": "Active",
    "detection_time": "2025-10-15T08:30:00Z"
   }
  ]
 }
}
```

III.2 Software Composition Analysis Schema (SNYK/CYBERGOPLUS)

Used to verify software dependency safety under the Supply Chain security requirements.

- **Source:** D6.1 Cyber Awareness Platform v1.
- **Context:** Static Application Security Testing (SAST).

© CYberSynchorny, 2025

```
JSON
{
  "projectName": "cybersynchrony-backend",
  "timestamp": "2025-11-01T10:00:00Z",
  "vulnerabilities": [
    {
      "id": "SNYK-PYTHON-REQUESTS-12345",
      "severity": "high",
      "moduleName": "requests",
      "version": "2.24.0",
      "fixedIn": "2.25.0",
      "isUpgradable": true
    }
  ]
}
```

III.3 Integrity Verification Request (CROSS-CORE)

Used to verify that logs used for compliance evidence have not been tampered with.

- **Source:** D5.2 Evidence Integrity System v1.
-
-

```
JSON
{
  "status": "VERIFIED",
  "asset_id": "server-finance-01",
  "log_hash": "sha256:a1b2c3d4...",
  "ledger_block": 10245,
  "anchored_time": "2025-10-15T08:35:15Z",
  "tamper_detected": false
}
```

Context: Blockchain anchoring via Hyperledger.

III.4 Identity Verification Schema (Keycloak/Platform)

Used to verify Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) status for audit logs.

- **Source:** D6.1 Cyber Awareness Platform v1.

© CYberSynchorny, 2025

- **Context:** OIDC Token Introspection.

```
JSON
{
  "sub": "user-12345",
  "email_verified": true,
  "realm_access": {
    "roles": ["ciso", "auditor"]
  },
  "acr": "loa2",
  "authentication_method": ["pwd", "otp"],
  "compliance_meta": {
     "last_login": "2025-11-01T12:00:00Z",
     "mfa_enabled": true
  }
}
```

III.5 Compliance Status Output (Dashboard Feed)

The aggregated data structure sent to the main dashboard.

- **Source:** D8.1 Integration Blueprint.

```
JSON
{
  "organization_id": "org-001",
  "report_period": "Q4-2025",
  "maturity_level": 3,
  "kpi_scores": {
    "policy_compliance_rate": 85.5,
    "mfa_coverage": 98.0,
    "incident_resolution_rate": 92.0
  },
  "critical_findings": 2
}
```

© CYberSynchorny, 2025