Framework Mapping: Cisco Secure Workload + NIS2 and ISO 27001:2022

Overview of the NIS2 Directive

The EU Network and Information Security (NIS2) Directive came into effect on January 16, 2023, with Member States required to transpose its measures into national law by October 2024. While implementation timelines and specific requirements may vary slightly by country, the directive sets a unified baseline for cybersecurity across the EU.

Purpose of the Framework

NIS2 aims to strengthen cybersecurity across the EU by:

- Strengthening cybersecurity across critical and essential sectors.
- Expanding scope to include more entities and industries.
- Mandating incident reporting and robust security practices.
- Increasing accountability through governance and risk management requirements.

Key Requirements

To achieve compliance, organisations must implement a comprehensive set of technical, operational, and organisational controls. Key requirements include:

- **Incident Reporting:** Essential entities must report incidents within 24 hours. Important entities have up to 72 hours to report incidents. These shorter timeframes place pressure on organisations to have rapid detection and response capabilities to meet these deadlines and avoid potential penalties.

- **Corporate Accountability:** Emphasizes management oversight and training on cybersecurity measures.

- **Risk Management:** Requires regular risk assessments and implementation of security measures

- **Business Continuity Planning:** Mandates plans for system recovery and emergency procedures.

- **Supply Chain Security:** NIS2 requires organisations to ensure cybersecurity measures extend to the supply chain.
- **Security Policies and Audits:** Implementation of comprehensive security policies, regular security audits, and vulnerability handling.
- **Access Control:** Enforces role-based access control, multi-factor authentication, and monitoring of access to critical systems.
- **Cryptography:** Establishes policies for cryptography and encryption to protect data.
- **Information Sharing:** Encourages coordinated vulnerability disclosure and sharing of threat intelligence with relevant authorities.
- **Supervisory Measures:** Essential entities face comprehensive ex-ante and ex-post controls, including onsite inspections and audits; important entities are subject to lighter ex-post supervision.

The Role of ISO 27001:2022 in NIS2 Compliance

With the NIS2 directive now in effect, organisations across Europe are looking to sustain and demonstrate ongoing compliance. While ISO 27001:2022 certification is not an explicit requirement under NIS2, it is strongly encouraged in the directive's preamble as a relevant international standard. The European Union Agency for Cybersecurity (ENISA) further supports this approach, having mapped ISO 27001 clauses directly to NIS2 requirements, highlighting the synergy between them.

However, it is critical to recognize that ISO 27001 compliance does not equal automatic NIS2 compliance. While ISO 27001 focuses on a risk-based management system (ISMS), NIS2 is a prescriptive legal directive. Key differences include:

- **Reporting Timelines:** NIS2 mandates an "early warning" within 24 hours of incident detection, a requirement not found in ISO 27001.
- **Management Liability:** NIS2 introduces personal accountability for corporate management regarding cybersecurity failures.
- **Supply Chain Rigor:** While ISO 27001 addresses third-party risk, NIS2 requires specific security assessments of the supply chain and the vulnerabilities of each direct supplier.

By aligning with ISO 27001, organisations can address NIS2's risk management and governance expectations with confidence. This internationally recognized standard provides a structured methodology for implementing security controls and managing incident response, ensuring a consistent and robust approach to information security. Adopting ISO 27001 not only helps strengthen cyber resilience but also enhances regulatory readiness, positioning organisations to proactively meet evolving compliance demands.

Understanding Cisco Secure Workload

Cisco Secure Workload, formerly known as Cisco Tetration, is a comprehensive workload protection platform designed to provide visibility, security, and compliance across hybrid, multi-cloud, and on-premises environments. It enables organisations to monitor application behaviours, map application dependencies, and enforce microsegmentation policies to limit lateral movement and reduce the attack surface.

By leveraging advanced analytics and machine learning, Cisco Secure Workload detects anomalies, identifies unauthorised activities, and simplifies policy creation and enforcement. Its capabilities help enhance the organisation's security posture, meet compliance requirements, and protect workloads throughout the lifecycle.

Deployment Options

Cisco Secure Workload offers flexible deployment options to address the diverse needs of organisations, whether they operate in on-premises data centers, public or hybrid clouds, or containerized environments. Its ability to integrate seamlessly with existing infrastructure and adapt to evolving IT environments makes it a powerful solution for securing workloads across the enterprise. By tailoring the deployment to the unique requirements, organisations can maximize security, reduce risks, and maintain a consistent security posture across all environments.

On-Premises Option

Cisco Secure Workload can be deployed in an organisation’s on-premises data center, providing full workload visibility and security within private infrastructure.

Use Case: Ideal for organisations with strict data sovereignty, compliance, or security requirements that mandate keeping workloads on-premises.

Deployment Details:

- Requires physical and virtual infrastructure to run the Cisco Secure Workload platform.
- Sensors (agents) are deployed on workloads (e.g., servers, virtual machines) to collect telemetry and enforce security policies.
- For workloads where it is not possible to install an agent, telemetry and discovery can be done using common network telemetry protocols such as NetFlow, IPFIX, ERSPAN and NSEL.
- Integration with existing on-premises tools such as firewalls, network management solutions, and SIEMs is supported.

Benefits:

- Full control over data and infrastructure.
- Enhanced security for workloads operating within private data centers.

Software-as-a-Service (SaaS) Option

Cisco Secure Workload can also be delivered as a SaaS offering, reducing the operational overhead of managing the platform infrastructure.

Use Case: Ideal for organisations seeking a fully managed solution that simplifies deployment and maintenance.

Deployment Details:

- Cisco hosts and manages the platform infrastructure, while organisations deploy sensors on their workloads or consume network telemetry for workload discovery.
- SaaS deployment supports hybrid, multi-cloud, and on-premises workloads. Updates, scaling, and availability are handled by Cisco.

Benefits:

- Faster time to value with minimal operational burden.
- Fully managed by Cisco, ensuring the latest features and security updates.
- Scales to meet the needs of dynamic environments.

Workload Form-Factors Support

Cisco Secure Workload provides holistic coverage of workload form-factors such as bare-metals, virtualised workloads (regardless of hypervisor), public cloud workloads and modern cloud-native workloads. It also has extensive support for multiple operating systems such as Windows OS, Linux and Unix.

Bare-Metal and Virtualised Workloads

Cisco Secure Workload supports deployment on both bare-metal servers and virtualised infrastructure.

Use Case: Provides flexibility for organisations using traditional IT environments or virtualised platforms.

Deployment Details:

- Sensors (agents) can be installed on bare-metal servers and virtual machines.
- Additionally, Workload without sensors (agentless) can be discovered and onboarded with network telemetry.
- Virtualised environments, such as VMware vSphere, Microsoft Hyper-V, or KVM-based are fully supported.
- Granular telemetry and policy enforcement extend to both bare-metal and virtualised workloads.

Benefits:

- Versatility across diverse IT environments.
- Protects legacy systems and modern virtualised infrastructures.

Public Cloud Workloads

Cisco Secure Workload supports cloud workloads regardless of the cloud service provider. Examples of cloud service providers include AWS, Microsoft Azure, and Google Cloud Platform.

Use Case: Suitable for organisations adopting public cloud infrastructure or operating cloud-native workloads.

Deployment Details:

- Sensors (agents) are deployed on cloud workloads (e.g., instances, virtual machines) to monitor application behaviors and enforce security policies.
- Additionally, workloads without sensors (agentless) can be discovered and onboarded using cloud flow logs.
- Enforcement can be done with the host-native firewall of the workloads or using cloud built-in controls, such as security groups.
- Visibility extends to workload communication within and across cloud environments.

Benefits:

- Supports cloud scalability and dynamic workload environments.
- Simplifies security for distributed and containerized workloads.
- Provides consistent security policies across hybrid infrastructures.

Cloud-Native: Containerized and Kubernetes Workloads

Cisco Secure Workload supports modern application architectures, including containerized workloads and Kubernetes-based deployments.

Use Case: Designed for organizations using microservices and containers in the development and production environments

Deployment Details:

- Sensors (agents) are deployed within Kubernetes clusters.
- Integrates with Kubernetes-native tools for workload orchestration and management.
- Integrates with cloud-managed Kubernetes services, such as Amazon EKS, Azure AKS, Google GKE.
- Provides visibility into container-to-container communication and enforces security policies at the container level.

Benefits:

- Provides granular visibility into containerized workloads.
- Security is aligned with DevSecOps practices.
- Helps ensure compliance and reduces risk in containerized environments.

Technical Features

Cisco Secure Workload delivers a robust set of technical features designed to secure workloads in complex and dynamic environments. Its ability to integrate with diverse infrastructure, automate security policy enforcement, and provide deep visibility makes it a key solution for organizations aiming to strengthen their workload security posture.

Visibility and Inventory Features

Comprehensive Workload Visibility

- Feature: Provides deep visibility into workload behaviors, application dependencies, and network communications across on-premises, hybrid, and multicloud environments.
- Benefit: Enables organisations to understand how workloads interact, identify vulnerabilities, and gain insights into their IT environment for better decision-making and security posture.

Application Dependency Mapping

- Feature: Automatically maps application dependencies by analyzing communication patterns between workloads and applications.
- Benefit: Simplifies the creation of security policies, supports troubleshooting, and helps ensure secure application behavior by understanding interdependencies.

Supply Chain Visibility and External Dependency Mapping

- Feature: Provides a continuous inventory of external communications between internal workloads and third-party APIs, SaaS providers, or vendor services.
- Benefit: Allows organisations to identify, validate, and restrict third-party dependencies to only authorised interactions.

Software Inventory and Exposure Monitoring

- Feature: Maintains a continuous, granular inventory of installed software packages, versions, and libraries across all bare-metal, virtualised, and containerized workloads.
- Benefit: Supports asset management and simplifies compliance audits by rapidly identifying workloads affected by newly discovered software vulnerabilities.

Zero Trust and Microsegmentation Features

Microsegmentation (Zero Trust Enforcement)

- Feature: Enables granular policy enforcement to segment workloads and limit lateral movement of threats within the environment.
- Benefit: Reduces the attack surface by implementing a Zero Trust "deny-all" model, restricting unauthorized communications between workloads and ensuring adherence to the principle of least privilege.

Policy Automation

- Feature: Automates the generation and enforcement of security policies based on observed workload behaviours and application dependencies.
- Benefit: Simplifies security management, reduces the risk of human error, and helps ensure consistent application of policies across diverse environments, improving operational efficiency.

Risk Management and Compliance Features

Risk-Based Vulnerability Management

- Feature: Integrates continuous workload telemetry with Cisco Vulnerability Management (part of the Cisco Security Cloud) to prioritize software vulnerabilities based on active risk and exploitability.
- Benefit: Meets requirements for vulnerability handling by allowing teams to focus on the most critical threats and automatically tighten segmentation for high-risk, unpatched workloads.

Executive Compliance Dashboards and Posture Scoring

- Feature: Provides high-level dashboards and "Security Posture Scores" that aggregate compliance data and policy adherence across the entire estate.
- Benefit: Addresses "Corporate Accountability" mandates by providing management with clear oversight of security health and simplifying "due diligence" reporting for auditors.

Compliance and Audit Support

- Feature: Tracks workload behaviours and generates detailed audit trails that demonstrate compliance with security frameworks and regulations (e.g., NIST, GDPR, PCI-DSS).
- Benefit: Simplifies compliance reporting and enhances transparency for internal and external audits, helping organisations meet regulatory requirements.

Threat Detection and Forensics Features

Near Real-Time Anomaly Detection

- Feature: Leverages advanced machine learning and analytics to identify deviations from baseline workload behaviors and detect suspicious activities.
- Benefit: Provides early warning of potential threats, essential for meeting the 24-hour "early warning" incident reporting requirements.

Process-Level Forensics and Hash Visibility

- Feature: Captures deep forensic details, including process IDs, user context, and process hashes for every network interaction.
- Benefit: Accelerates incident response and forensic investigations by identifying exactly which executable or script initiated a suspicious connection.

Behavioral Baselines

- Feature: Builds baseline profiles of normal workload and application behaviours over time.
- Benefit: Helps detect "living off the land" attacks and suspicious activity by identifying deviations from established norms.

Threat Intelligence Integration

- Feature: Supports integration with external threat intelligence platforms to enhance detection and response to known threats.
- Benefit: Improves situational awareness and strengthens defenses by correlating workload activity with global threat data.

Platform and Operations Features

Multicloud and Hybrid Cloud Support

- Feature: Offers seamless integration with public cloud platforms (AWS, Azure, GCP), private cloud, and on-premises environments.
- Benefit: Provides a unified security approach regardless of where workloads are deployed.

Integration with Kubernetes and Container Environments

- Feature: Supports containerised workloads and integrates with Kubernetes clusters (EKS, AKS, GKE) at the pod level.
- Benefit: Secures modern microservices-based applications and aligns with DevSecOps practices.

Secure API Integration

- Feature: Provides APIs for integration with third-party tools such as SIEM (e.g., Splunk®), SOAR, and EDR.
- Benefit: Enhances interoperability and allows organisations to build a cohesive security ecosystem.

Centralised Management

- Feature: Offers a single management console for policy configuration, monitoring, and reporting.
- Benefit: Simplifies operations and provides a unified view of workloads across the entire IT environment.

Role-Based Access Control (RBAC)

- Feature: Provides role-based access control for administrators and users of the platform.
- Benefit: Protects sensitive security configurations and reduces insider threats.

Infrastructure and Deployment Features

Enforcement Via Agents (Sensors)

- Feature: Lightweight sensors are deployed on workloads to collect telemetry and enforce security policies in real time.
- Benefit: Provides continuous monitoring and ensures policies are applied directly at the workload level.

Enforcement Via Network (Agentless)

- Feature: Collection of telemetry via network protocols (NetFlow, IPFIX, ERSPAN) and cloud flow logs for workloads where agents cannot be installed.
- Benefit: Ensures 100% visibility across the environment, including legacy systems and IoT devices.

Support for Legacy, Modern, and Cloud-Native Environments

- Feature: Works across bare-metal servers, virtual machines, and containerised environments.
- Benefit: Provides consistent security across traditional IT systems and modern hybrid architectures.

Encrypted Communications

- Feature: Supports encrypted communications between workloads and the Secure Workload platform.
- Benefit: Protects sensitive telemetry data and ensures secure interactions between platform components.

Scalability and Performance

- Feature: Designed to scale from small deployments to large enterprises with hundreds of thousands of workloads.
- Benefit: Provides consistent security and visibility as organisations expand their IT infrastructure.

Mapping Cisco Secure Workload to NIS2 and ISO 27001:2022

NIS2 Article/Sub-Article	NIS2 Mapping (Meets)	NIS2 Mapping (Supports)	ISO 27001:2022 Mapping (Meets)	ISO 27001:2022 Mapping (Supports)
Article 10: Computer security incident response teams (CSIRTs)		10(3), 10(7), 10(8)	A.5.36	6.1, 8.1, A.5.35
Article 11: Requirements, technical capabilities and tasks of CSIRTs		11(4), 11(5)	9.1, A.8.20	6.1, A.5.26
Article 12: Coordinated vulnerability disclosure and a European vulnerability database		12(4), 12(5)	A.5.25	6.1, 8.2, A.5.7, A.5.24, A.5.26
Article 18: Report on the state of cybersecurity in the Union		18(3)		
Article 19: Peer reviews		19(1)(a), 19(1)(c), 19(1)(e)	A.5.25, A.5.27, A.8.20	6.1, 6.2, A.5.24, A.5.26, A.5.28
Article 21: Cybersecurity risk-management measures		21(2)(c), 21(2)(e), 21(2)(h), 21(2)(i), 21(2)(j)	A.5.25, A.5.27, A.8.1, A.8.2, A.8.7, A.8.9, A.8.15	
Article 23: Reporting obligations		23(4)(a), 23(4)(b)	A.5.25	6.1, A.5.24
Article 24: Use of European cybersecurity certification schemes	24(1)		A.5.27	6.1, A.5.24
Article 25: Standardisation		25(2)	A.5.27	6.1, A.5.24
Article 29: Cybersecurity information-sharing arrangements		29(1), 29(3)	A.5.25, A.5.27, A.8.20, A.8.21	A.5.24, A.5.26, A.5.28

Conclusion

Achieving NIS2 compliance is more than just a regulatory hurdle; it is an opportunity to build a sustainable, risk-based security culture. While ISO 27001 provides the foundational "how-to" for managing information security, NIS2 introduces the "must-do" legal obligations necessary for regional resilience. By leveraging ISO 27001:2022 as a strategic framework to satisfy NIS2 requirements, organisations can bridge the gap between operational best practices and strict legal accountability, transforming a compliance mandate into a robust competitive advantage.

Cisco Secure Workload plays a role in supporting this alignment by delivering advanced technical controls that directly address key NIS2 and ISO 27001 requirements. Its comprehensive visibility, application dependency mapping, and microsegmentation capabilities enable organisations to understand and control workload interactions, helping to reduce the attack surface and limiting lateral movement of threats.

Cisco Secure Workload fills the "reporting gap" created by NIS2. By providing near real-time detection and granular telemetry, it allows organisations to help meet the 24-hour and 72-hour notification windows that ISO 27001 processes might not be tuned for. This proactive approach not only supports compliance but also fortifies an organisation's security posture in an increasingly complex threat landscape.

Resources

Cisco Secure Workload

Cisco Secure Workload At-a-Glance

Cisco Secure Workload Datasheet