

How Cyolo and BearingPoint Help You Achieve Compliance: NIS2 Directive

INTRODUCTION

The NIS2 Directive is a piece of legislation that aims to enhance the cyber resilience of critical infrastructure in the European Union (EU) by establishing a minimum set of cybersecurity requirements that all EU Member States must impose on their respective in-scope entities. NIS2 replaces and builds upon its predecessor, the original NIS Directive, with an expanded scope and additional requirements developed in response to increases in the frequency and impact of cyberattacks against EU critical infrastructure in recent years.

This document details Cyolo and BearingPoint's support for NIS2 compliance and offers related guidance for security and risk practitioners in the EU and beyond.

KEY NIS2 COMPLIANCE REQUIREMENTS

The minimum requirements for NIS2 compliance for in-scope essential and important entities are as follows:

Cybersecurity risk management measures: Entities must implement 10 key measures to manage and mitigate cyber risks posed to any networks, systems, and/or other digital or physical assets involved in delivering essential or important services in the EU.

These measures include:

1. Policies on risk analysis and information system security.
2. Incident handling (prevention, detection, and response to incidents).
3. Crisis management and business continuity, such as backup and recovery management.
4. Supply chain security for relationships between each entity and its suppliers or service providers.

Timelines & Deadlines

- NIS2 entered into force on **16 January 2023**
- Member states must transpose NIS2 into national law by **17 October 2024**
- Member states must identify and register in-scope essential and important entities by **17 April 2025**

5. Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosures.
6. Policies and procedures to assess the effectiveness of cybersecurity risk management.
7. Basic cyber hygiene practices and cybersecurity training.
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption.
9. Human resources security, access control policies, and asset management.
10. The use of multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications, and secured emergency communication systems.

OVERVIEW OF CYOLO PRO

Cyolo PRO (Privileged Remote Operations) is an advanced, infrastructure-agnostic secure access solution built to mitigate the risks of remote access to mission-critical assets. Cyolo PRO’s decentralized architecture provides exceptional flexibility and can seamlessly adapt to all environments (cloud-connected, cloud-averse, and offline) without change management.

Common challenges Cyolo PRO solves include:

- Ensuring rapid, secure, and safe support and maintenance for the factory floor and OT environments
- Safely connecting third parties to OT environments with no agents or end-user downloads required
- Adding multi-factor authentication (MFA) to legacy systems that do not natively support modern identity authentication
- Securing all access points to mission-critical assets, whether remote or on-premises
- Implementing segmentation, supervision, session recording, and other requirements of industry and regional compliance mandates

CYOLO PRO/NIS2 ALIGNMENT

Cyolo PRO addresses the compliance requirements of NIS2 with the following functions and features:

Risk Management Measure	Cyolo PRO Capabilities	Control Type
Policies on risk analysis and information system security	Granular control policies provide user, session, application, and device information to help validate compliance.	SUPPORTS
Incident handling (prevention, detection, and response to incidents)	Features like zero-trust access, MFA to all systems, and session monitoring and recording reduce the likelihood of a security incident. If suspicious activity is detected, access can be restricted or terminated in real-time. Seamless integration with SOAR, SIEM, XDR, and other tools for additional incident response capabilities.	PROVIDES

Measure	Cyolo PRO Capabilities	Control Type
Crisis management and business continuity, such as backup and recovery management	Unique decentralized architecture is built from self-replicating components, ensuring business continuity and uptime and enabling data recovery even from a single component.	PROVIDES
Supply chain security for relationships between each entity and its suppliers or service providers.	<p>Zero-trust architecture shields applications and assets from direct connectivity.</p> <p>Application-level access prohibits lateral movement and limits the damage a potential attacker could cause.</p> <p>Oversight controls like supervised access and session recording ensure security for the full duration of the connection.</p> <p>The solution’s agentless deployment model is ideal for securing third-party access.</p>	SUPPORTS
Policies and procedures to assess the effectiveness of cybersecurity risk management	In-platform analytics demonstrate the effectiveness of cybersecurity and risk management policies.	SUPPORTS
Policies and procedures regarding the use of cryptography and, where appropriate, encryption	<p>TLS connection ensures full end-to-end encryption from user to application.</p> <p>All data, secrets, and encryption keys remain inside the customer’s trusted boundaries and are never stored or decrypted in the Cyolo cloud.</p>	SUPPORTS
Human resources security, access control policies, and asset management	Robust and granular access controls include MFA, password vault, device posture checks, end-to-end encryption, continuous authorization, and identity federation.	SUPPORTS

Measure	Cyolo PRO Capabilities	Control Type
The use of multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications, and secured emergency communication systems	<p>MFA extends all user accounts (service, shared, individual, etc.) in all environments (cloud-connected, cloud-averse, offline).</p> <p>MFA capabilities can be added to legacy systems with no upgrades or change management needed.</p>	PROVIDES

Control Type Description

Provides: Provides information you provide directly to auditor or feeds data into an artifact.

Validates: Can be used to prove whether another control(s) is present and/or working.

Supports: Feeds info into another system or processes which serve the requirements.

ABOUT CYOLO

Cyolo, the access company for the digital enterprise, takes a holistic approach to cybersecurity that aligns closely with the ethos of the NIS2 Directive. The adaptable, infrastructure-agnostic Cyolo solution is purpose-built to secure, monitor and audit privileged remote connections to critical infrastructure and OT systems.

With Cyolo, organizations like yours can proactively implement the steps highlighted here with no operational disruptions and no changes needed to your existing infrastructure. Schedule a demo and begin your path to NIS2 compliance today.

Learn more at Cyolo.io

ABOUT BEARINGPOINT

BearingPoint is an independent management and technology consultancy with European roots and a global reach. The company operates in three business units: Consulting, Products, and Capital. Consulting covers the advisory business with a clear focus on selected business areas. Products provides IP-driven digital assets and managed services for business-critical processes. Capital delivers M&A and transaction services.

BearingPoint's clients include many of the world's leading companies and organizations. The firm has a global consulting network with more than 10,000 people and supports clients in over 70 countries, engaging with them to achieve measurable and sustainable success.

Learn more at BearingPoint.com