# Understanding the EU NIS2 Directive:

## Enhancing Cybersecurity for Pulp & Paper Companies

### What is the NIS2 Directive?

The NIS2 Directive is a legislative framework established by the EU to enhance the cybersecurity and resilience of critical infrastructure sectors. It replaces and extends the first NIS Directive from 2016, that was established to ensure a high level of security across the Member States. The NIS2 Directive addresses the following objectives:

- Strengthen the security requirements
- Secure the supply chains
- Streamline reporting obligations
- More stringent supervisory measures
- Stricter enforcement requirements
- Harmonized sanctions across the EU

EU Member States will have to transpose NIS2 into their national legislation by October 17, 2024.

### Who is affected by NIS2 and how?

The NIS2 Directive distinguishes between Essential and Important entities:

- **Essential entities -** include several sectors such as Energy, Transport, Water, and more, or any enterprise with a headcount over 250 or more than 50 million in revenue.
- **Important entities -** include Manufacturing, Chemicals, Gas, Food, and more, or enterprises with a headcount over 50 or more than 10 million in revenue.

Essential entities will be required to meet supervisory requirements, while the Important entities will be subject to supervision only if authorities receive evidence of non-compliance. Fines for Essential entities amount to €10,000,000 or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, and up to € 7,000,000 or at least 1,4% of the total worldwide annual turnover of the preceding financial year for Important entities.

> *"Our partnership with Andritz and OTORIO helped us to define our operations security policies, and provided the needed tools for continuous governance of their implementation. With the RAM² platform we have comprehensive visibility into the OT/ ICS and Operations Supporting Systems networks. The platform enables us to get a clear view regarding the risk level of different regions, and allocate proper resources while focusing on the most critical risks. OTORIO's solution is an important enabler for increased operational efficiency through automation and connectivity"*
>
> **CISO, global Pulp & Paper company**

## What are the implications for the Pulp & Paper industry?

The NIS2 Directive is becoming the baseline for cybersecurity regulations in the EU. It also applies to non-EU organizations that provide services within Member States. The Pulp & Paper industry provides essential products and services, such as paper, packaging, and tissue. It is also a major employer, providing jobs for hundreds of thousands of mill workers around the world. A disruption to the pulp & paper industry would significantly impact the economy and society, as well as potential environmental implications. Therefore, the Pulp & Paper industry now falls under the regulatory obligations set forth by the NIS2 directive.

## How can I prepare for NIS2?

To ensure operational resilience based on the NIS2 guidelines, and avoid significant financial impact due to lack of compliance, it is important to start implementing the needed measures before the NIS2 Directive takes effect on your business. Pulp & Paper mill operators should adhere to compliance with the NIS2 Directive requirements, by implementing a cybersecurity strategy that addresses the following areas:

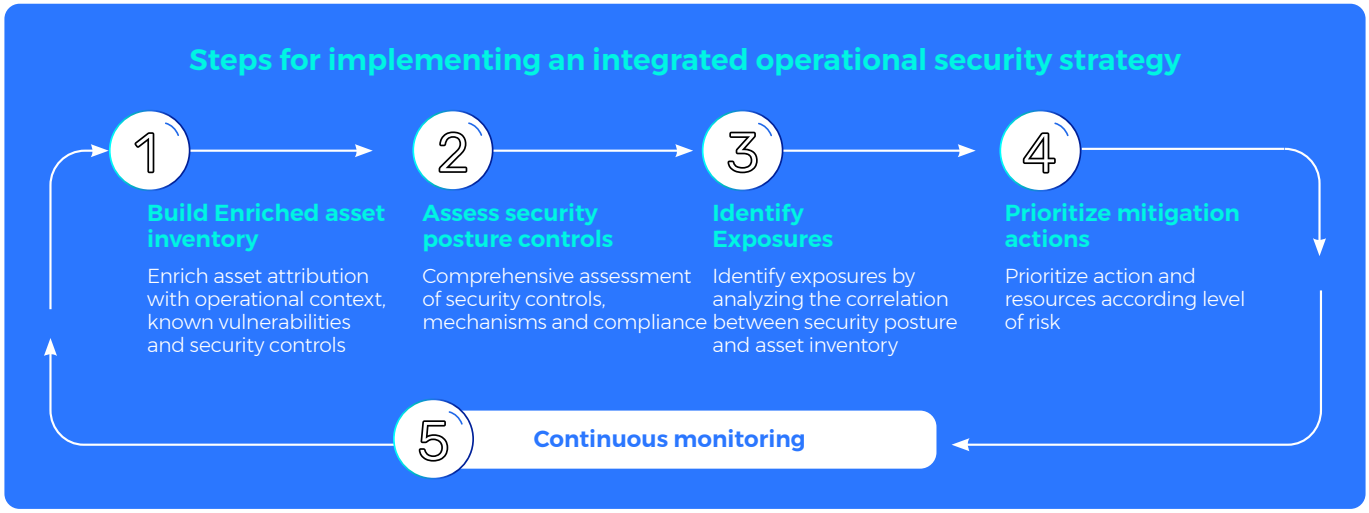
- Asset and network visibility
- Operational risk management
- Supply chain security and access management
- Protection against cyber-attack
- Incident and crisis management
- Response and recovery planning

> *"With OTORIO's solution we gained full transparency into our asset inventory and network. We are using OTORIO as an overlay on existing controls to create a single source of truth and improve our ROI. OTORIO's RAM² improves our team's efficiency, supports our preparation for compliance, and enables governance and policy enforcement. With OTORIO and Andritz we can scale the solution to additional sites, without compromising on safety, efficiency and reliability."*
>
> **OT security global manager, global Pulp & Paper company**

# How Andritz and OTORIO can support your NIS2 compliance?

## The journey toward operational security

Implementing the needed security controls and processes can be highly challenging in complex, multi-vendor, multi-generation, geographically spread Mills, where accelerated digitization, connectivity, and third party access are essential for efficiency and competitiveness. Pulp & Paper operations risk management leaders need to establish an integrated OT security strategy that involves establishing suitable processes, using technological tools that support the security strategy, and collaboration between cross-domain stakeholders.




Implementing the needed measures will ensure operations resilience and avoid significant financial impact due to lack of compliance before the NIS2 Directive comes into effect for your business.

## Andritz and OTORIO provide a platform that ensures your NIS2 compliance

Andritz and OTORIO's solution for OT cyber risk management supports your efforts for compliance with the NIS2 Directive. Our automation and cybersecurity experts can help you take the next steps towards OT security and compliance, wherever you are in your journey.

OTORIO's industrial native platform empowers OT security practitioners to proactively mitigate risks, and collaborate with stakeholders from different disciplines for maximum efficiency.

# How we help you turn your strategy into actions

## 1 Build Enriched asset inventory

- Full visibility and transparency into IT-OT-IoT asset inventory and network
- Leveraging cross-domain data sources for maximum accuracy and coverage (down to level 0)
- Detailed asset configurations
- Enrich asset attribution with operational context, known vulnerabilities and security controls

## 2 Assess security posture controls

- Out-of-the-box compliance and policy assessment from a single asset to entire site level
- Security posture assessment
- Attack surface analysis
- Offline and online compliance and security assessment of vendor equipment

## 3 Identify exposures

- Exposures identifications based on correlation between security posture and asset inventory
- Segmentation assessment and hardening
- Empowering proactive risk mitigation with prescriptive mitigation playbooks
- Security remote access control, monitoring and governance for the supply chain

## 4 Prioritize mitigation actions

- Impact-driven operational Risk prioritization
- Vulnerability management
- Security configurations hardening
- Actionable mitigation guidance that are tailored to the operational environment constraints

## 5 Continuous monitoring and response

- Continuous monitoring of the network.
- Automatic correlation of events from multiple sources for early detection of potential attacks
- Case and Incident management for collaborative response.

**Our solution improves preparedness for the NIS2 Directive, safely, efficiently, and effectively.**
**Contact us to learn how Andritz and OTORIO can help you reduce compliance costs and expedite the adoption of an integrated OT cyber security strategy.**

**For more detailed information, please visit: www.otorio.com**

## About ANDRITZ

ANDRITZ is an international technology group providing plants, systems, equipment, and services for various industries. The company is one of the technology and global market leaders in the hydropower business, the pulp and paper industry, the metal working and steel industries, and in solid/liquid separation in the municipal and industrial segments. The listed Group is headquartered in Graz, Austria. Since its foundation 170 years ago, ANDRITZ has developed into a Group with approximately 27,400 employees, and more than 280 locations in over 40 countries worldwide. As a reliable and competent partner, ANDRITZ supports its customers in achieving corporate and sustainability goals.
**www.andritz.com**

## About OTORIO

OTORIO's industrial-native OT security platform enables industrial organizations to achieve an integrated, holistic security strategy. Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. OTORIO's global team brings the extensive mission-critical experience of top nation-state cyber security experts combined with deep operational and industrial domain expertise.

**www.otorio.com**

CN120723