



**Rockwell
Automation**

UNDERSTANDING EU'S NIS2 CYBERSECURITY DIRECTIVE



▶ BEGIN

TABLE OF CONTENTS

Introduction

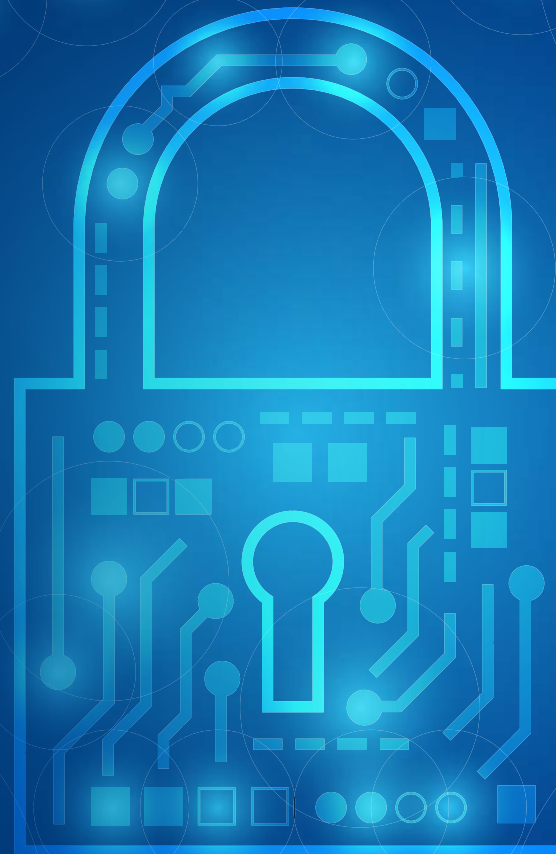
NIS2 directive overview

Entities in scope

NIS2 compliance requirements and security measures

Supervision, enforcement, fines, and penalties

Accelerate compliance with a strategic partner



Introduction

An increasingly digitized world with growing digital connectivity brings enormous opportunities and attack paths for cyber criminals to exploit.

In parallel, the number, complexity, and scale of cybersecurity incidents and their economic and social impact are growing. Supply chains are more interconnected, and a security breach at an entity can impact an entire region or industry. The European Parliament is introducing legislation to enhance the cyber resilience of critical infrastructure within the European Union by establishing a minimum set of cybersecurity requirements.

At the end of 2022, the European Union published the [final version](#) of “Measures for a high common level of cybersecurity across the Union,” also called “NIS2”. This is the successor of the “Network and Information Security Directive” (NISD), which was released in 2016. The directive provides legal measures to improve overall cybersecurity across the EU. This includes obligations for businesses, government authorities, and cooperation between EU member states on security risks and incidents. The differences between the NIS2 draft version (released in 2020) and the final version are significant, and this paper refers to the final version.

This document’s purpose is to provide an overview of the final NIS2 directive. Our second whitepaper provides [practical advice and security measures](#) for incident detection/reporting and OT security based on an EU member state’s recently published methodology update.



NIS2 directive overview

The NIS2 directive will become effective across all EU Member states by 17. October 2024. All requirements apply for entities of specific sectors and business sizes that are active in one or more EU member states. For a business to be in scope, the entity has to engage in economic activities, irrespective of its legal form. Major suppliers for clients in the EU will also be in scope if their clients are in the EU and receive critical services.

Key aspects of NIS2:



A new level of reliability

Significant fines and penalties for repeated non-compliance are proposed, along with accountability for senior management



More industries

Supervision and enforcement by local authorities for medium and large organizations across more than a dozen key sectors



Minimum requirements

Establish mandatory, reviewable, and sanctionable cybersecurity measures for incident reporting and risk management, response/remediation required. EU member states can define stronger requirements for their region



Supply chain included

Requires risk reviews of security practices for major connected third-party services providers; this includes, e.g., Managed Security Services providers



Government support

Entities without adequate security staffing can ask for help in case of a major incident



Maximum fees

Defined by member states but has to be at least 1.4% of global turnover or €7M for important entities, 2% of global turnover or €10M for essential entities

The expected impact

- **Gain in security maturity insights across EU Member states:** Expect government authorities to develop a good understanding of effective measures in your industry and raise the expected security maturity to a common level.
- **Efficient management of risks required:** Adding active risk management measures will add cost/time efficiency pressure to the organization as it requires not only to detect but to continuously assess and respond to risks.
- **NIS2 is not the end:** Cybersecurity maturity is a strategic target of the EU commission, and in parallel to NIS2, additional initiatives are underway. An increase in requirements and fines can be expected.
- Recently published measures from an EU member state indicate that NIS2 compliance will require a significant increase in security maturity (approx. Capability Maturity Model level 3-4), requiring better understanding and actively managing risks, not only covering incident detecting but also taking remediation actions, and measures the outcome and security management efficiency.

Suggested actions

- **Review your compliance:** Assess security risks based on all relevant assets, review your security risk management and incident detection and response management capabilities, and define local/regional (EU)/global responsibilities. There are solutions from Rockwell Automation that can help to evaluate and resolve security issues.
- **Close gaps:** Identify OT-accepted security solutions based on their security coverage, work efficiency, and operational costs. There are OT security solutions for different maturities available; look for a solution that covers regulatory compliance as well as internal requirements. Consider scalable solutions that will grow with your requirements and future compliance and regulatory needs.
- **Prepare for expected security controls:** As of today, the expected measures in detail have not been published. ENISA, the European cybersecurity agency, released a mapping of [NIS2 requirements to global security standards](#). As a guide, we mapped expected NIS2 measures with the 2023 version of the security compendium from German BSI in the whitepaper "[Understanding EU's NIS2 Cybersecurity Directive](#)".
- **Note to CISOs and board members:** Be aware of what's coming, not only because you can be held personally responsible but also because the EU is on its way to building and enforcing a major and rather complex framework of security compliance regulations [across all member states](#). If organizations fail to take the initiative, the initiative could be taken by government authorities.

NIS2 and important related regulations 2023/2024

NIS2 is part of the EU's cybersecurity strategy and complements other directives and laws. Especially relevant for operational environments are the Critical Entity Resilience (CER) directive, which is closely interrelated with NIS2, and the EU Cyber Resilience Act (ECRA). Both have significant consequences for vendors, operators, and service providers of operational equipment; ECRA became effective at the end of 2023.

CER Directive (final):

Finalized and transposed in parallel to the NIS2 Directive, together they address digital cyberattacks (NIS) to physical attacks and natural disasters (CER). CER focuses on physical rather than digital resilience measures for critical entities. National authorities perform reviews and assess the effectiveness and accountability of the risk management process; they can also provide significant support to entities. Both directives become effective by October 2024.

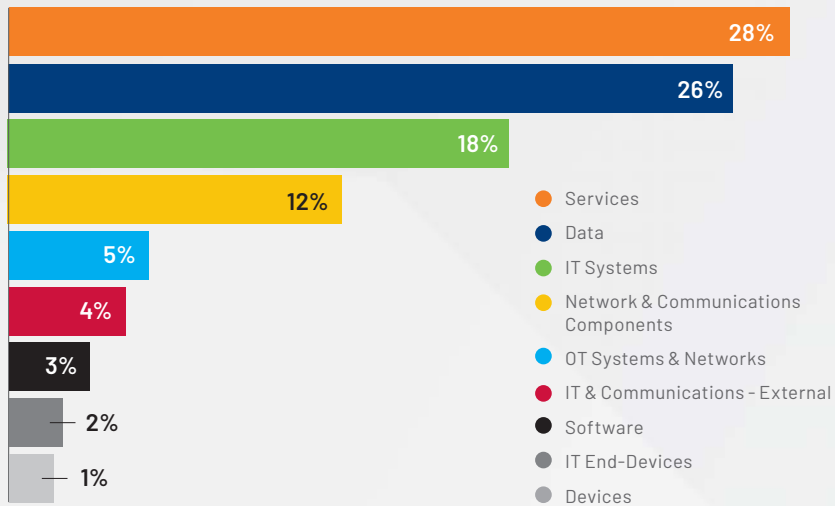
EU Cyber Resilience Act (ECRA):

Became legally effective at the end of 2023 and is focused on regulating a broad range of products with digital elements, their hardware, and solutions with embedded software and applications. It imposes obligations on manufacturers, importers, and distributors of these products across their lifecycles. It also defines essential requirements for the design, development, production, and operation of digital products and adds requirements for vulnerability and incident handling for manufacturers and obligations for operators.

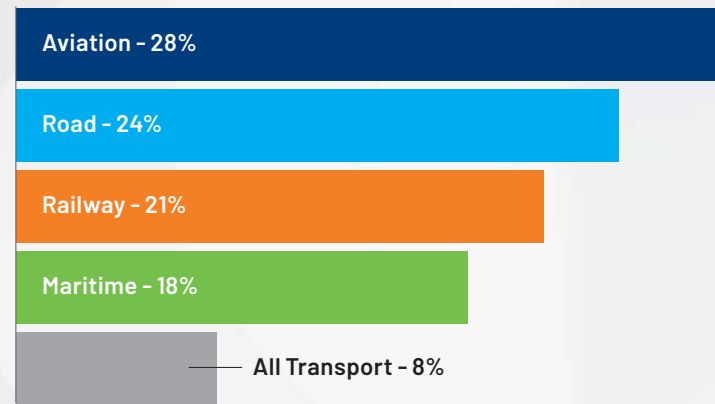
ENISA's 2023 report uses NIS-based reported data

To improve cybersecurity and create risk awareness, ENISA publishes an annual threat landscape report that includes NIS-based incident reporting information and globally gathered incident data. A recently released 2023 report for the transport sector shows a targeted system that includes OT for the first time (left image) and observed incidents across all sectors (right image) and concludes that for 2022, once again, an increase of ransomware is impacting vulnerable and unpatched systems.

Affected assets and services



Observed incidents in each sector



What does the coverage of OT mean for the organizations in scope?

We know that there is already a [skills shortage in cybersecurity](#) and especially for OT, but there is a notorious lack of experts with a combined industrial operational risk understanding and security expertise. Entities and regulators must find ways to identify and evaluate the most efficient, automated, and integrated approaches for continuous and active management of risks, including OT.

NIS2 will require organizations to understand their risks and actively manage their security measures. A one-time, project-based security investment into a single-dimensional technology without proper management integration will not be sufficient to cover the increasing requirements. For operational environments, entities will either acquire new security solutions for each maturity increase step they take or invest in higher maturity solutions they can grow with and into. These two different approaches have their own benefits and constraints. Investing in cybersecurity solutions requires a cost versus risk analysis. Knowing current risk is key to defining the strategy. As some entities are regularly audited, effective and valuable approaches to OT security will quickly become visible to authorities.



A one-time, project-based security investment into a single-dimensional technology without proper management integration will not be sufficient to cover the increasing requirements.

Entities in scope

The last NIS2 update added a new level of flexibility to who is in scope. Added flexibility for regulators allows entities to move between weaker and tougher requirements sets; unfortunately, it also adds complexity for entities to determine if they are in scope.

Scoping elements:

- Medium and large-sized entities that provide or conduct services within the Union and are active within the sectors of NIS2 Annex I or II
- NIS2 Annex I or II type entities of any size when the entity is
 - critical because of its specific importance at the national/regional level for the particular sector or type of service or for other interdependent sectors in the Member State
 - the sole provider of services in the member state, and service is essential for the maintenance of critical societal or economic activities
 - trust services, public communication network provider, DNS
- NIS2 Annex I + II type entities of any size when a service disruption
 - could have a significant impact on public safety/security/health
 - could have significant systemic risks, especially for sectors where disruption could have a cross-border impact
- Member states may include critical research activities



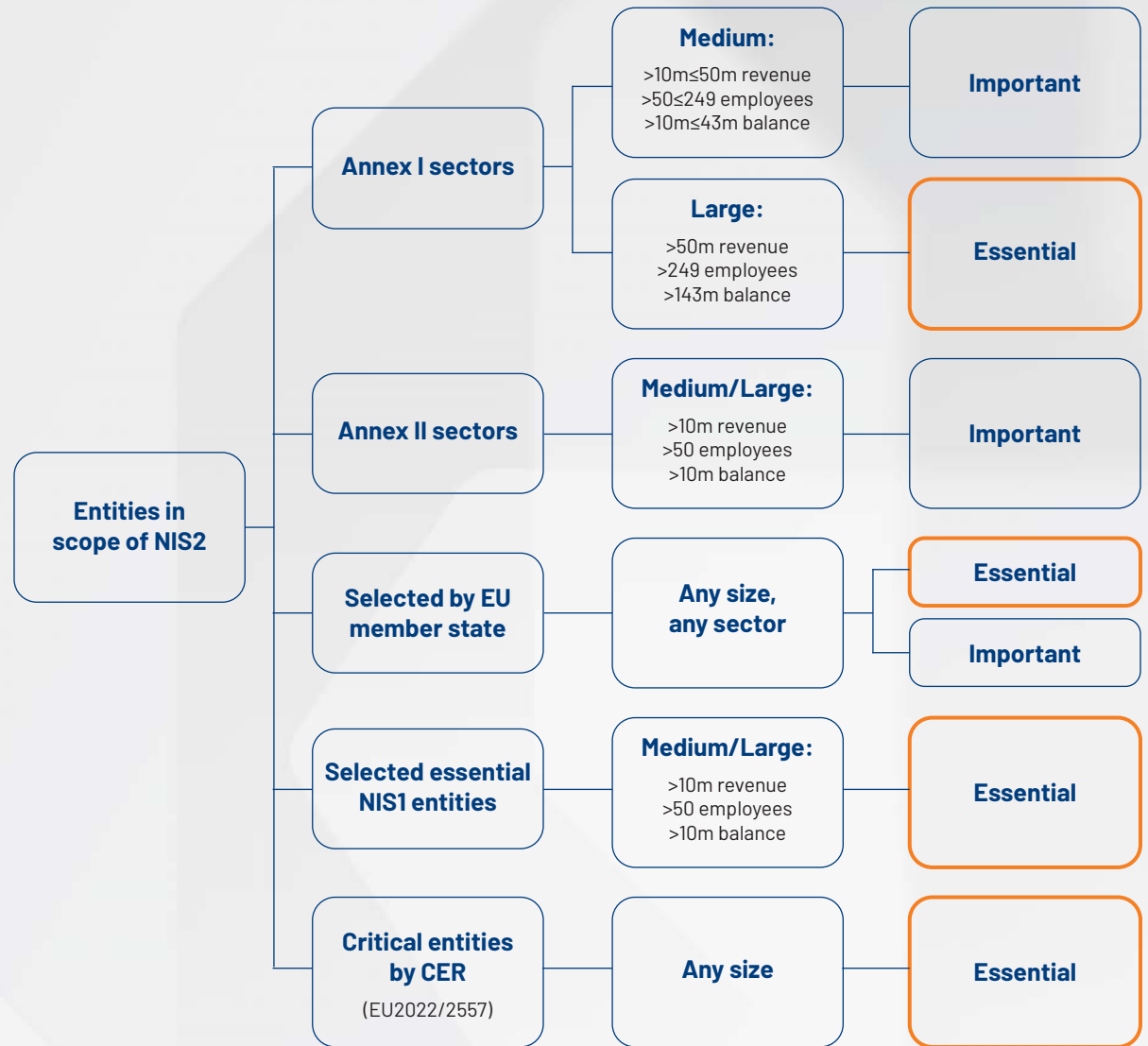
NIS2 distinguishes between **essential** and **important** entities. Essential entities have increased security requirements and face stricter supervision and higher penalties. The below image describes the major requirement.

Essential entities	Important entities
Legal representative for external communication	Legal representative for external communication
Ongoing, proactive supervision	Reactive supervision after incident
Entity tasks: Incident reporting/remediation duties, establish risk management measures	Entity tasks: Incident reporting/remediation duties, establish risk management measures
Severe enforcement , up to C-level liability	Less severe enforcement
Very high penalties/fees	High penalties/fees

Transposed into local member state law by 17th October 2024

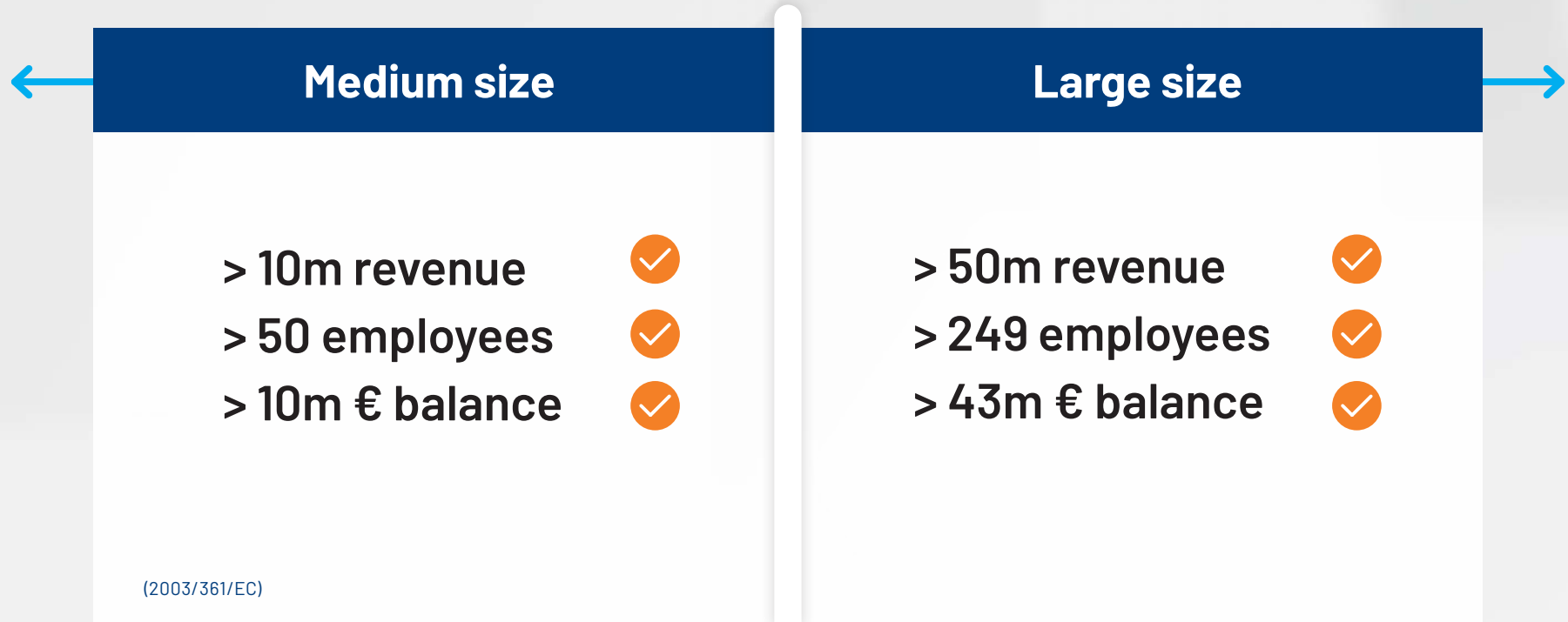
Guidance will be provided by ENISA to help determine if your organization is defined as “in scope”.

The chart on the right provides an indication, based on current definitions as to an organizations applicability; the EU agency will create and maintain a registry for essential and important entities for NIS2. Until then, you can perform a precheck to determine if you could be in scope. Because the methodology is rather complex (and flexible to be extended for the EU Commission), we provide a quick check-up chart.



To perform a pre-check to see if you are considered an essential or important entity, you need to know the following:

- 1 Your company size (see graphic below)



- 2 Is your industry/subindustry listed in Annex I or II? (see tables on the next pages)

Annex I: Sectors of high criticality

Sector	Subsector	Type of entity
Energy	Electricity	Energy supply, selected distribution system operators, selected transmission system operators, selected electricity producers, nominated electricity market operators and selected participants
	District heating and cooling	Operators for district heating or district cooling
	Oil	Operators of transmission pipelines, operators of oil production, refining and treatment facilities, storage, and transmission, selected central oil stockholding entities
	Gas	Selected suppliers, selected distribution system operators, selected transmission system operators, selected storage system operators, selected LNG system operators, selected natural gas undertakings
	Hydrogen	Operators of hydrogen production, storage, and transmission
Transport	Air	Selected air carriers, selected airport managing bodies, Air Traffic Control Services Providers (ATC)
	Rail	Selected infrastructure managers, selected railway undertakings
	Water	Selected inland, sea and coastal passenger and freight water transport companies, selected managing bodies of ports, selected operators of vessel traffic services
	Road	Selected road authorities, selected delegated traffic management control regulations, selected operators of Intelligent transport systems
Health	Pharma, Manufacturing, Laboratories, Services	Selected entities manufacturing medical devices considered as critical during a public health emergency, selected healthcare providers, EU reference laboratories, selected entities carrying out research and development activities of medicinal products, selected entities manufacturing basic pharmaceutical products and pharmaceutical preparations
Drinking water		Selected suppliers and distributors of water intended for human consumption, excluding those with majority of other general activity
Wastewater		Selected undertakings collecting, disposing, or treating urban, domestic, and industrial wastewater as an essential part of the business

Annex I: Sectors of high criticality (continued)

Sector	Subsector	Type of entity
Space	Infrastructure, Services	Selected operators of ground-based infrastructure, owned, managed, and operated by Member States or by private parties, that support the provision of space-based services
ICT service management (business-to-business)		Managed Services Providers (MSP), Managed Security Services Providers (MSSP)
Digital infrastructure		Internet exchange point providers, DNS service providers, excluding operators of root name servers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, trust service providers, providers of public electronic communications networks, providers of publicly available electronic communications services
Banking, Financial Markets, Public Administration		Not in the focus of this document

Annex II: Other critical sectors

Sector	Subsector	Type of entity
Postal and courier services		Selected postal service providers
Waste management		Selected entities, carrying out waste management but excluding undertakings for whom waste management is not their principal economic activity
Production, processing and distribution of food		Entities engaged in wholesale distribution, industrial production and processing of any food and drink. Not a food business (e.g. feed, live animals unless for human consumption, plants prior to harvesting)
Manufacture, production and distribution of chemicals		Selected undertakings carrying out the manufacture, production and distribution of substances and articles.

Annex II: Other critical sectors (continued)

Sector	Subsector	Type of entity
Manufacturing	Manufacturer of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices
	Manufacturer of computer, electronic and optical products	Entities that manufacture computers, electronic and optical products, electronic components and boards, loaded electronic boards, computers and peripheral equipment, communication equipment, consumer electronics, instruments and appliances for measuring, testing and navigation; watches and clocks, irradiation, electromedical and electrotherapeutic equipment, optical instruments and photographic equipment, magnetic and optical media
	Manufacturer of electrical equipment	Entities that manufacture electrical equipment, electric motors, generators, transformers and electricity distribution and control apparatus, batteries and accumulators, wiring and wiring devices, fiber optic cables, other electronic and electric wires and cables, wiring devices, electric lighting equipment, domestic appliances, non-electric domestic appliances, other electrical equipment
	Manufacturer of machinery and equipment n.e.c.	Entities that manufacture general-purpose machinery, engines and turbines (except aircraft), vehicle and cycle engines, fluid power equipment, other pumps and compressors, taps and valves, bearings, gears, gearing and driving elements, other general-purpose machinery, ovens, furnaces and furnace burners, lifting and handling equipment, office machinery and equipment (except computers and peripheral equipment), power-driven hand tools, non-domestic cooling and ventilation equipment, other general-purpose machinery n.e.c, agricultural and forestry machinery, metal forming machinery and machine tools, other special-purpose machinery, machinery for metallurgy, machinery for mining, quarrying and construction, machinery for food, beverage and tobacco processing, machinery for textile, apparel and leather production, machinery for paper and paperboard production, plastic and rubber machinery, other special-purpose machinery n.e.c.
	Manufacturer of motor vehicles, trailers and semi-trailers	Entities that manufacture motor vehicles, trailers and semi-trailers, bodies (coachwork) for motor vehicles, parts and accessories for motor vehicles, electrical and electronic equipment for motor vehicles, other parts and accessories for motor vehicles
	Manufacturer of other transport equipment	Entities that manufacture transport equipment, ships and boats, ships and floating structures, pleasure and sporting boats, railway locomotives and rolling stock, air and spacecraft and related machinery, military fighting vehicles, transport equipment n.e.c., motorcycles, bicycles and invalid carriages, other transport equipment n.e.c.
Digital providers		Not in the scope of this document
Research		Not in the scope of this document

If your sector or company size is not on either list, you may still be in scope if:

You are a major services provider to a client that is considered in the scope of NIS2. In this case, you will not face mandatory duties but will require some cybersecurity practices, like a defined process for vulnerability disclosure and communication with the client. Providers of managed security services are in scope.

Member states can exclude areas of defense, national security, public security, or law enforcement from the requirements of the directive.



NIS2 compliance requirements

Duty to provide entity contact details

All entities in scope must provide contact details:

- Initially notify ENISA of your entity name, addresses of main and other legal establishments in the EU, up-to-date contact details, including email addresses and telephone numbers
- Foreign corporations not established in the EU but providing services (e.g., data center and content and service providers) must provide a designated representative contact
- Update of changes within three months after the change became effective

Reporting obligations for a potential severe incident

All entities in scope must report severe incidents. Local government, authorities, and CSIRT support and information sharing across entities are one of the main areas of regulation. The importance of the topic is reflected in tight deadlines and can become subject to sanctions. A notification does not make the notifying entity subject to increased liability.

A **severe incident** that must be reported to local authorities or the CSIRT is characterized as:

- severely impacting services, or
- imposing a significant financial loss, or
- significant immaterial or material impact on a natural or legal person

The EU is building tools to support the reporting process and allow quick escalation and support of the incident response. Entities can ask to be supported by authorities.

Report	What?	Deadline
Early warning	<ul style="list-style-type: none"> Cross-border impact? Unlawful or malicious act? 	Within 24 hours after becoming aware
Incident notification	<ul style="list-style-type: none"> Update to early warning data? Initial assessment? Severity and impact? Indicators of compromise? (if available) 	Within 72 hours after becoming aware
Intermediate report	<ul style="list-style-type: none"> Relevant status updates? 	Government requested (anytime)
Final report (Progression report if attack is ongoing)	Detailed description of the incident, including severity and impact <ul style="list-style-type: none"> Type of threat or root cause Applied and ongoing mitigation measures Cross-border impact of the incident 	One month after submission of initial notification
Final report after ongoing attacks	(see above)	Within one month of handling the incident

Who and when to notify?

- The national competent authority or CSIRT
- Recipients of the services (incidents and potential incidents)
- Without undue delay, within 24 hours after having become aware of the incident

A final incident report must be sent no later than one month after the submission of the incident notification. It must at least include:

- A detailed description of the incident, its severity, and its impact
- Type of threat or root cause that likely triggered the incident
- Applied and ongoing mitigation measures
- Whether the incident has a cross-border impact or is caused by unlawful or malicious action



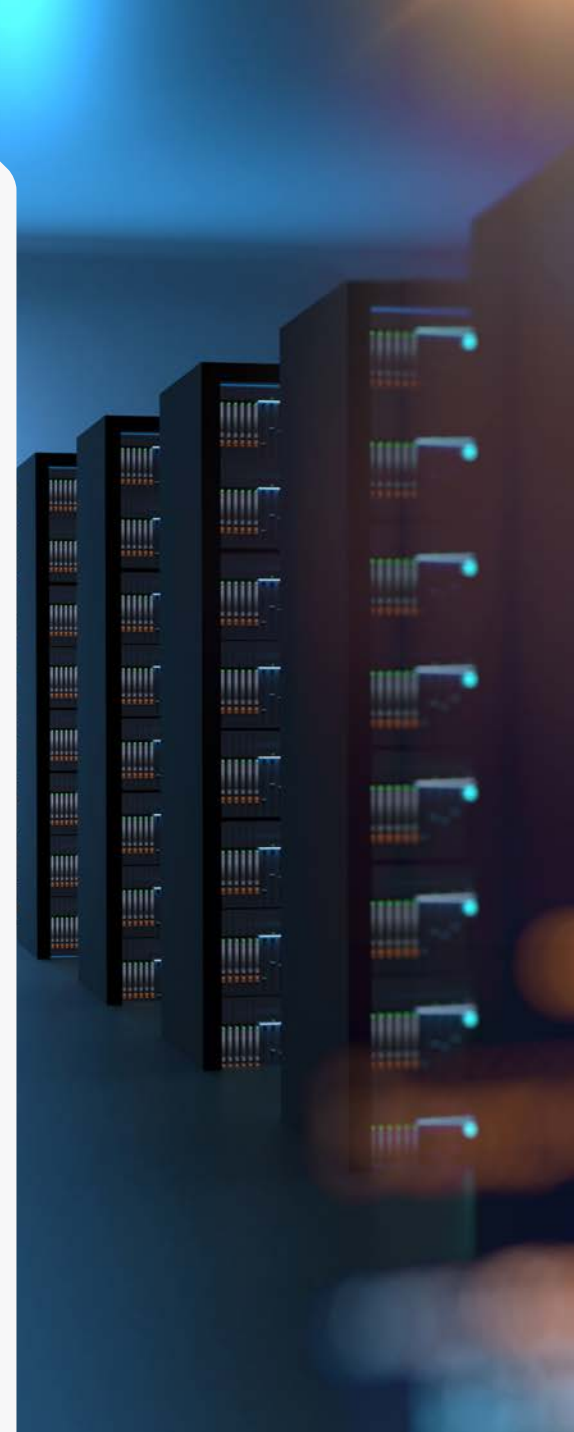
Minimum security risk management measures

NIS2 provides a minimum mandatory set of measures. Once transposed into local law in October 2024, the detailed requirements will be defined. The following list contains minimum mandatory areas of coverage for all entities; exceptions are mentioned.

All entities must take effective, appropriate, and proportionate technical and organizational measures to manage the cybersecurity risks posed to the security of networks and systems. These measures must ensure that the level of security is related to the risk presented. All measures and respective non-compliance are accounted for by management.

The following measures represent the minimum requirements to be covered:

- Asset management
- Basic cyber hygiene practices and cybersecurity training
- Incident handling
- Policies for risk analysis, information system security, and access control
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Business continuity, such as backup management, disaster recovery, and crisis management, are in place
- Supply chain security, including security of relationships between the entity and its direct suppliers/ service providers, are in place and considered
 - vulnerabilities specific to each supplier/service provider, and
 - product quality and cybersecurity practices of their supplier, including secure development procedures
 - results of coordinated security risk assessment of critical supply chains
- Security in the network and information systems lifecycle, including vulnerability handling and disclosure
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption
- Use of multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications, and secured emergency communication systems within the entity, where appropriate



Quick checklist for the first steps

- ✓ **Relevant assets are detected to a very high degree** within an appropriate timeframe. This also applies to OS-based and embedded systems in OT.
- ✓ **Security policies are documented, communicated, and assessed.**
- ✓ **Is a process to report potential significant incidents in place?**
- ✓ **Assets in scope have been identified**, and are monitored. Are vulnerabilities as threats managed?
- ✓ **The entity is capable of identifying**, monitoring, alerting, and possessing capabilities to respond to a threat.
- ✓ **A ticketing system to manage and document** incident detection triage and response is in place.
- ✓ **Critical processes and their assets are known and documented**, and security measures are in place.
- ✓ **Supply chain risks are identified**, and mitigating measures are in place.
- ✓ **Can evidence from a security management system be relied on** for industrial assets?

Supervision, enforcement, fines, and penalties

As a general rule, **essential entities** are subject to a stronger supervisory regime, while **important entities** are subject to lighter supervisory; important entities have no initial obligation to systematically document compliance with cybersecurity risk management requirements up to the point of a major incident or threat happens. If a threat or incident occurs, from this point they will be supervised, face enforcement of violations, and can be subject to fines and penalties.

Supervision

Essential and important entities face equal baseline measures. Additional requirements for essential entities will be covered in the next paragraph.

Supervision **all entities** in scope:

- Is coordinated with the legal representative of the entity
- Includes on-site inspections
- Includes off-site inspections
- Authority can request information to assess compliance
- Authority can request evidence of security policy implementation

Additional supervision for **essential entities** covers:

- regular and ad-hoc audits, including a collection of evidence
- random, unplanned checks by authorities



Enforcement of violations:

Should the supervision identify compliance violations, enforcement will come into effect. Again we will separate baseline enforcement from enforcement for essential entities alone.

For **all entities** in scope, local authorities can:

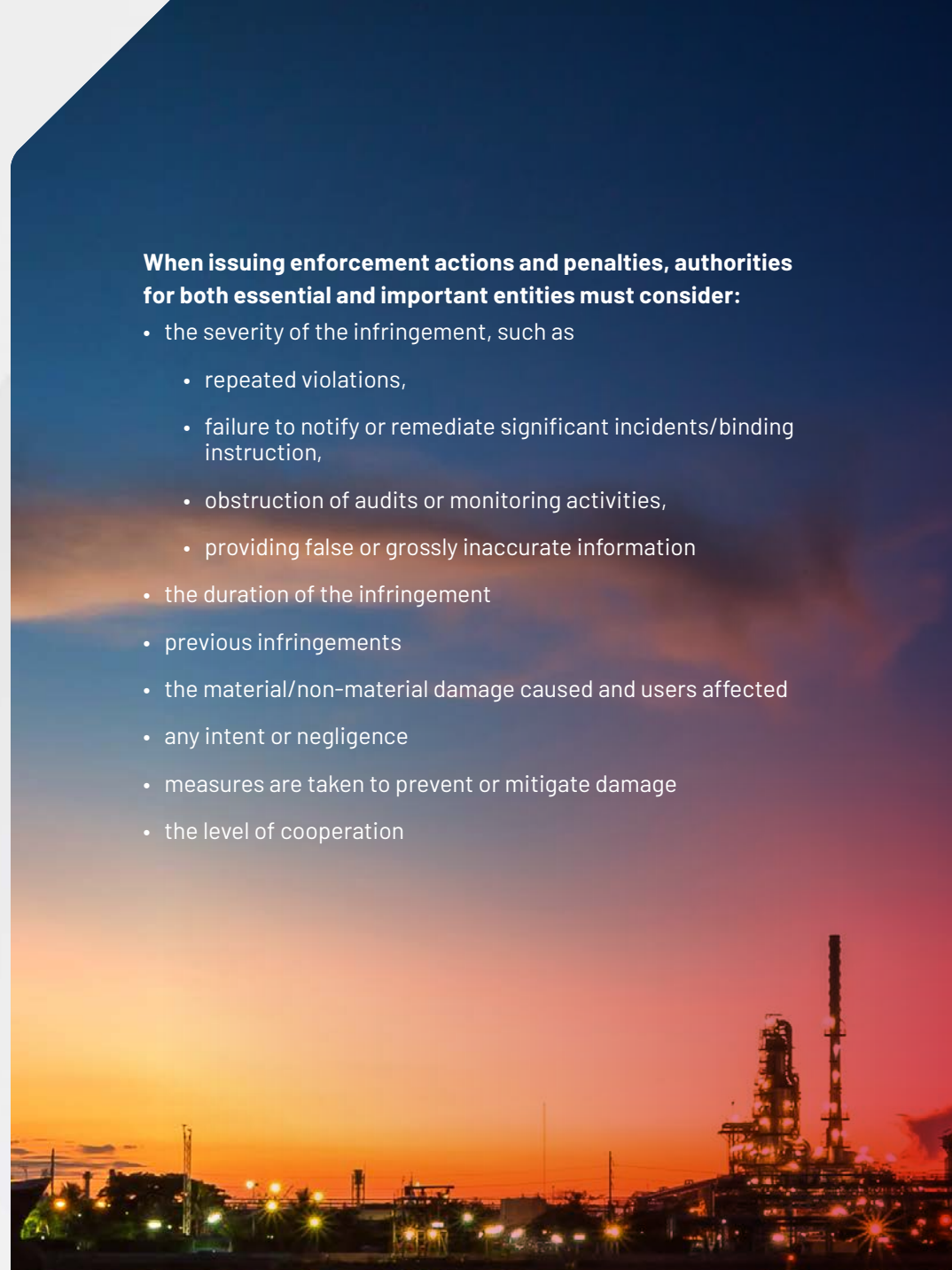
- issue warnings
- issue binding instructions to remediate incidents within the deadline
- order to cease and make infringement public
- order to implement security audit recommendations within the deadline
- impose administrative fines

Additional enforcement for **essential entities** includes:

- Initiate temporary prohibition to exercise managerial function at the CEO or legal representative level
- Designate a monitoring officer to oversee compliance
- Issue binding instructions to prevent incidents with deadlines for implementation and reporting

When issuing enforcement actions and penalties, authorities for both essential and important entities must consider:

- the severity of the infringement, such as
 - repeated violations,
 - failure to notify or remediate significant incidents/binding instruction,
 - obstruction of audits or monitoring activities,
 - providing false or grossly inaccurate information
- the duration of the infringement
- previous infringements
- the material/non-material damage caused and users affected
- any intent or negligence
- measures are taken to prevent or mitigate damage
- the level of cooperation



Penalties and fines

The directive states multiple times that penalties defined by each member state must be effective, proportionate, and dissuasive.

For all entities in scope, local authorities can:

- impose periodic penalty payments to cease infringement
- impose additional sanctions (effective by Jan 2025)

Important entities

Face maximum penalties of **at least 1.4% of global turnover, or €7M, whichever is higher**

Essential entities

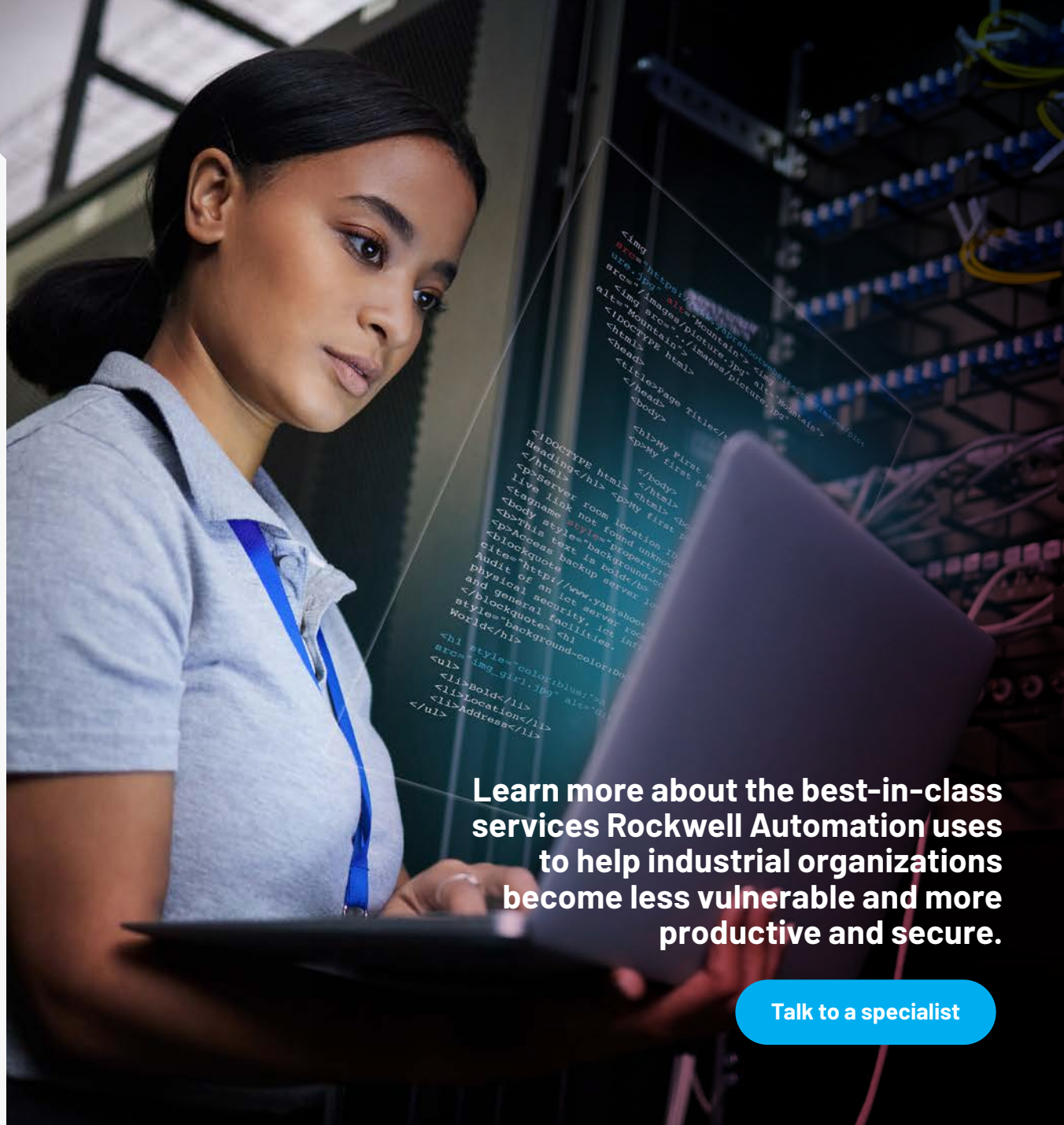
Face maximum penalties of **at least 2% of global turnover, or €10M, whichever is higher**

Accelerate compliance with a strategic partner

Organizations providers face unique challenges when it comes to creating and maintaining effective cybersecurity.

With the rise of Industrial Internet of Things (IIoT) blurring the line between digital and physical infrastructure, knowing how to achieve the desired level of communication in a safe and secure manner can be challenging. Figuring out how to comply with complex regulations and standards can also be difficult and time consuming.

As the world leader in industrial automation, Rockwell Automation knows how to help secure industrial systems for organizations of all sizes across all industries. We deliver unrivaled capability in OT cybersecurity with a powerful combination of specialized in-house cyber knowledge coupled with world-class partnerships. Rely on us for all your OT security needs, as many organizations in the Fortune 100 do.




Learn more about the best-in-class services Rockwell Automation uses to help industrial organizations become less vulnerable and more productive and secure.

[Talk to a specialist](#)

How Rockwell Automation can help with NIS2

One of the major changes for entities in the scope of NIS2 is the requirement to actively manage risks and not only detect and document but also remediate them. Rockwell Automation can provide products, services and solutions to help achieve compliance with the NIS2 directive. From assessing gaps to compliance and current risk posture, to providing security, risk and vulnerability management solutions for proactive analysis of risk and remediation.

NIS2 Obligations	Rockwell Services/Product Features
Policies and Procedures	Tabletop exercise, Incident Response Plan reviews, OT Risk Assessment, Tech Enabled Risk Assessment (Verve)
Incident handling	Network Design, Intrusion Detection, End Point Protection, Incident Response, Crown Jewels Assessment, Patch Management (Verve enabled)
Crisis management	Backup and Recovery Services, Incident Response, Verve Proactive Services
Supply chain security	Network Design and Blueprints, IDMZ
Security in Network	Network Design, CPwE, IDMZ, CIP Security, Intrusion Detection, OT Patch Management, Secure Remote Access, Virtualization
Risk Management	OT Risk Assessment, OT Pen Testing, Tech Enabled Risk Assessment (Verve)
Basic cyber hygiene	Asset Inventory, Vulnerability Analysis, Intrusion Detection, System Hardening, Application Whitelisting (Verve)
Cryptography, Encryption (P&P)	CIP Security, IPsec FactoryTalk Services, Stratix Managed Switch Encryption, OPC UA security (FactoryTalk Linx Gateway, Logix controllers, FactoryTalk Optix)
Human resources security (access control policies, asset management)	PlantPAx, FactoryTalk Directory, Asset Inventory, Crown Jewels Assessment, FactoryTalk AssetCentre, Access Management (Verve)
Multi-factor authentication	ThinManager, FactoryTalk Optix & Secure Remote Access, FactoryTalk Hub & applications, Azure AD authentication, OpenID connect integration FactoryTalk Security

Connect with us.    

rockwellautomation.com

expanding **human possibility**[®]

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600

ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608

UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800

Allen-Bradley and expanding human possibility are trademarks of Rockwell Automation, Inc.
Trademarks not belonging to Rockwell Automation are property of their respective companies.

Publication GMSN-SP032A-EN-P - April 2024

Copyright © 2024 Rockwell Automation, Inc. All Rights Reserved. Printed in USA.