MM/DD/YYYY

Cyber Resilience Act (CRA) Readiness Assessment Customer Presentation

Cybersecurity Solutions and Services

PRESENTED BY NAME

SE ADVISORY SERVICES

EU Legislation for Cybersecurity*

Three complementary regulations shaping a unified cybersecurity landscape

Cyber Resilience Act (CRA)

Cybersecurity as a requirement for CE marking and for vulnerability management throughout the machine/digital product life cycle.

The NIS 2 Directive

Ensures continuous risk management and incident response in essential or important organizations.

New Machinery Regulation (NMR)

Expands the concept of functional safety, requiring that safety functions are also protected against cyberthreats.

SE ADVISORY SERVICES

Two legislative acts, one common objective

CRA: The Cyber Resilience Act applies to products with digital elements in the EU and incorporates cybersecurity as a CE marking requirement. It obliges OEMs to design, develop, and maintain products securely.

NIS2: Ensures the protection of systems supporting processes that, if disrupted, could generate a significant impact on the organization and third parties.

Impacted Organizations:

NIS2

- Sector of activity (direct vs. indirect)
- Size and turnover*
- Impact of a cyberattack

CRA

- Any digital product sold or distributed in the EU

.

Penalties:

NIS2

- Financial (max. €10M or 2% of turnover / max. €7M or 1.4% of turnover)
- Personal liabilities: temporary bans / administrative fines

CRA

- Loss of CE marking

Relationship between NIS2 & CRA:

- NIS2 anticipates the use of CRA-compliant products.
- Both regulations require similar capabilities:
  - Risk assessment
  - Vulnerability identification & mgmt. (notification/disclosure)
  - Supply-chain security, and
  - Incident preparedness

***EU 2003/361/EC: Medium or larger enterprises**

- 50<= Employees <=250
- Annual turnover >= 10M€
- Annual balance sheet >=10M€:

SE ADVISORY SERVICES

Legislation timeline

From commitment to compliance: accelerating the journey before time runs out.

CRA

- 20 Nov 2024: Publication of Regulation (EU) 2024/2847 (CRA) in the DOUE
- 10 Dec 2024: Entry into force (20 days after publication)
- 11 Jun 2026: Application of Chapter IV (Arts. 35–51) — notification/operation of conformity assessment bodies
- 11 Sep 2026: Application of Article 14 (vulnerability management/disclosure obligations)
- 11 Dec 2027: Full CRA application (cybersecurity requirements enforceable for CE marking)

NIS2

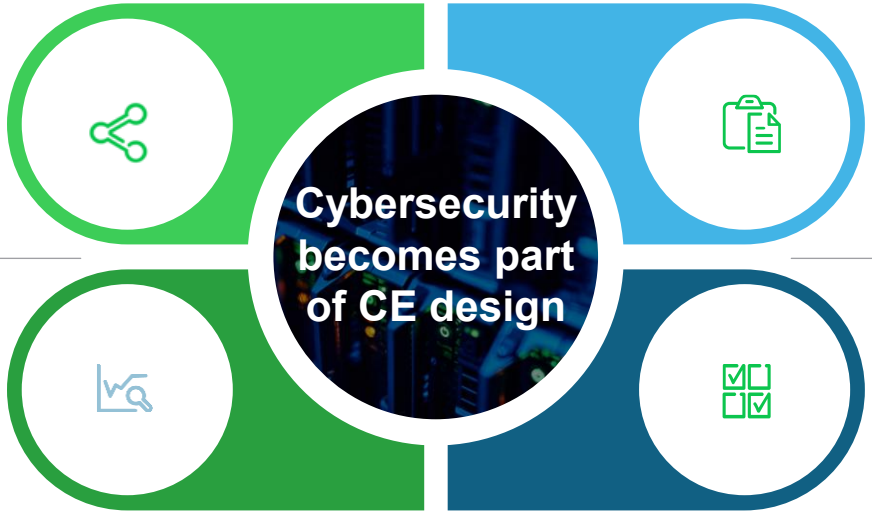
- 16 Jan 2023: NIS2 enters into force in the EU
- 17 Oct 2024: Deadline for Member States to adopt and publish transposition measures (application the following day)
- 17 Apr 2025: Member States must establish a list of essential and important entities
- 26 Jun 2025: ENISA publishes the NIS2 Technical Implementation Guidance
- April 2024: Belgium
  Oct 2024 – April 2025: Italy
  December 2025: Germany
  In progress: Spain

SE ADVISORY SERVICES

How the CRA changes industrial machine design

- **A machine is a digital product.** The OEM must demonstrate secure integration and maintenance.

- **Evidence, not assumptions**. Every change or vulnerability must be traceable.



- **CRA and the Machinery Regulation expand CE marking**. The technical file must include digital risk, updates, and support.

- **Shared responsibility**. OEM, integrator, and customer must provide evidence.

CRA, Machinery Regulation (MR), & NIS2 at machine level

Secure by operations*

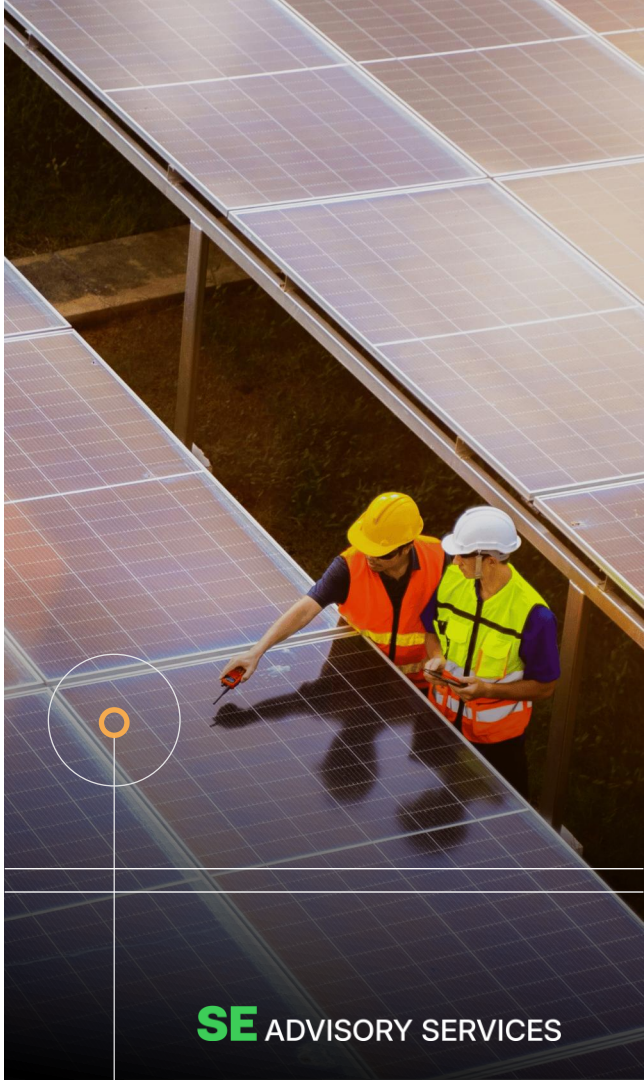
- **CRA** → applies to the machine as a product with digital elements. The OEM must integrate and document components securely throughout the life cycle.
- **NMR** → covers functional and physical safety of the machine–operator system and must be consistent with CRA measures.
- **NIS2** → applies to the network and operation when the machine is part of a customer-managed installation.

*A machine architecture may include elements subject to all three regulations. Compliance is demonstrated through documented design and traceable evidence.

Critical questions to navigate CRA readiness

- Do I clearly understand how CRA requirements impact the cybersecurity of our digital products?
- Do we know how CRA and related regulations translate into concrete technical requirements for products?
- Are our engineering teams equipped to address CRA requirements without delaying development timelines?
- Do we know what evidence is required to demonstrate due diligence for product cybersecurity?

- How can we demonstrate proactive CRA readiness to authorities and customers through structured evidence?
- How can we establish a structured cybersecurity framework for products aligned with CRA?
- How can we align engineering, cybersecurity, and compliance early in the product lifecycle?
- How can we prioritize investments to address CRA requirements while controlling development costs?



Understanding your CRA readiness

Our CRA Readiness* Assessment helps OEMs understand how their machines and supporting processes address the essential requirements of the Cyber Resilience Act. It turns regulatory expectations into clear engineering and documentation actions, using IEC 62443 as a practical reference where useful.

Documented gaps and targeted actions. We deliver clear findings and actionable recommendations that help the OEM improve design, documentation, and long-term maintenance practices.

Practical and proportional approach. We analyze design and lifecycle practices with a focus on what is realistic for the OEM and consistent with its operational context.

Independent review by OT-cybersecurity experts. Assessment performed by specialists familiar with connected machines, CRA obligations, and industrial environments.

The assessment is backed by Schneider Electric's experience applying CRA concepts to its own connected products and by cybersecurity teams involved in global OT projects reviewing architectures, processes, and technical documentation.

A service that goes beyond a check list. It provides real evidence to support the insights and recommendations suggested.

*The assessment report and workshop outputs are intended to support the OEM's internal cybersecurity activities and the preparation of its own CRA technical documentation. They do not represent a formal validation, approval or certification of CRA compliance, and they cannot be used as a substitute for the OEM's own conformity assessment activities or CE declaration.

SE ADVISORY SERVICES

Our approach

Strategic
Kick off Meeting

Tactic
Data Gathering

Tactic
Interview

Tactic
Assessment (Machine & Organization)

Tactic
Report Validation

Strategic
Report Submission
Final Presentation / Workshop

- Essential CRA requirements defined, as reflected in IEC 62443
- Equivalent/overlapping NIS2 controls are provided for traceability purposes.
- 100% remote delivery

- Pragmatic focus on the machine design.
- No scans or direct tests on the equipment.

- If safety-related functions are present, only the presence of cybersecurity measures to protect them are checked.

Methodology

STEP 01 — Kick off Meeting

- Confirmation of the scope and the expected inputs, objectives, roles, planning, and prerequisites.
- Clarification of assumptions, expected inputs, and communication channels.

STEP 02 — Data Gathering

- Gathering of architecture diagrams, network drawings, component list, SBOMs, and organizational procedures related to vulnerability management, software updates, incident handling, and risk assessment.

STEP 03 — Interview

- Clarify design decisions, lifecycle management, and how the OEM ensures traceability of cybersecurity actions.

STEP 04 — Assessment

- Machine level: the machine design and supporting evidence are compared with CRA essential requirements, using IEC 62443-3-3 controls as the reference.
- Organization level: the OEM's internal processes are listed to verify how they meet CRA expectations for vulnerability handling, updates, and incident response.

STEP 05 — Final Presentation / Workshop

- Submission of report to the customer.
- Conduct a workshop with the customer to present and validate the results, answer questions, and agree on next steps.

Prerequisites*

- Provision of product design and technical documentation
- Cybersecurity lifecycle processes and governance
- Traceability and evidence management for compliance

*Non-Exhaustive

Why Schneider Electric CRA readiness assessment?

Delivered value

- **CRA-aligned gap analysis**: Structured comparison of current OEM practices against CRA essential requirements and relevant IEC 62443-3-3 controls.
- **Evidence-based findings**: Clear, documented results supported by reviewed technical documentation and stakeholder interviews.
- **Prioritized recommendations**: Practical, risk-based improvement actions across design, process, and documentation, validated in a workshop.
- **Reusable compliance evidence**: Assessment report* reusable as supporting input for CRA technical documentation, CE marking, and audits.

Benefits

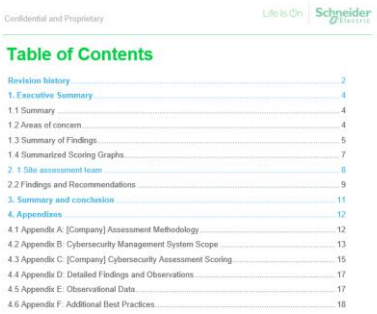
- **Demonstrate CRA readiness:** Gain a clear, documented view of how current design and process practices meet the essential requirements of the Cyber Resilience Act.
- **Targeted improvement actions:** Receive specific, practical recommendations to address the gaps identified during the assessment.
- **Faster path to CE conformity:** Use the assessment results to strengthen the technical documentation required for CRA compliance and CE marking.
- **Consistent integration of cybersecurity and safety:** For machines with safety-related functions, confirm that cybersecurity measures protecting those functions remain consistent with the OEM's safety documentation under the New Machinery Regulation.

*This is not a certification document and does not replace the OEM's own responsibility for CE or CRA conformity..

SE ADVISORY SERVICES

CRA Readiness Assessment report sample

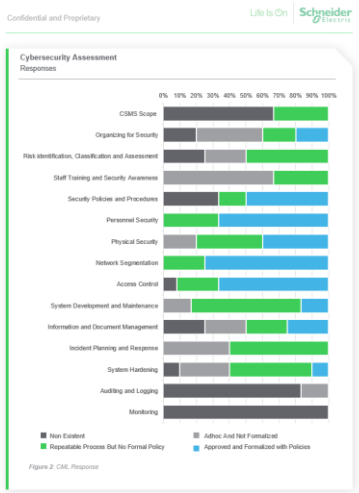
Table of contents



Findings & recommendation

Maturity score

Detailed view of maturity score



To be updated with the pictures of the final report template

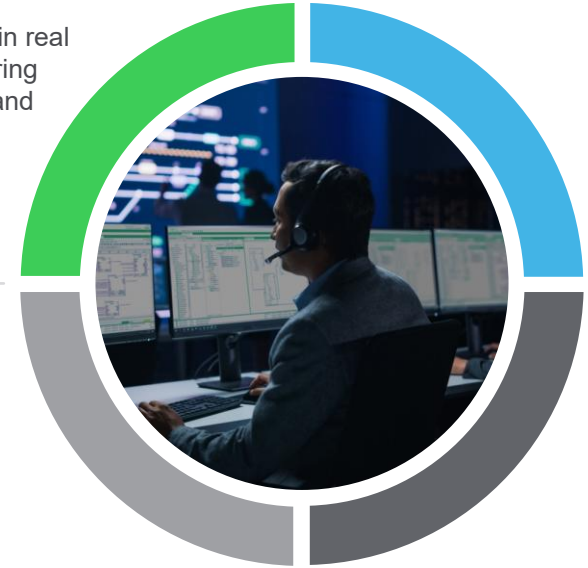
SE ADVISORY SERVICES

Partnering with Schneider Electric

For effective CRA compliance readiness

Designed by an OEM, for OEMs

Benefit from an assessment approach grounded in real industrial product development constraints, ensuring recommendations are practical, implementable, and aligned with OEM design lifecycles.



Guidance from recognized experts

Work with Schneider Electric specialists experienced in OT cybersecurity and in the application of new European regulatory frameworks such as CRA, NMR, and NIS2.

Proven industrial credibility

A global industrial leader with decades of experience delivering compliant, secure, and safety-critical products across multiple regulated markets.

Beyond Consulting

A true partner offering more than assessments, driving long-term OT cybersecurity resilience consulting services.

SE ADVISORY SERVICES

Global customers who trust Schneider Electric

Securing critical digital infrastructure for a major international airport.

Canada

France

Empowering the operations of a leading Mining & Minerals group with €3.88B in global revenue.

United States

Securing digital buildings for a $32B US Financial Services company.

Thailand

Protecting 34 sites for a $1.4B Food & Beverage leader.

SE ADVISORY SERVICES

Get in touch with our cybersecurity experts

Key contacts

Name & Region
emailaddress@se.com

Name & Region
emailaddress@se.com

cybersolutions@se.com

Contact us today Learn more about our cybersecurity assessment services :
cybersolutions@se.com

SE ADVISORY SERVICES

Thank you

Need help starting your **industrial cybersecurity journey**?

Visit our site to learn more

Download our eGuide

SE ADVISORY SERVICES