EU CRA

EU Cyber Resilience Act (EU CRA)

Customer Statement

We Perform with Integrity: Our commitment to compliance with the EU Cybersecurity Resilience Act at METTLER TOLEDO.

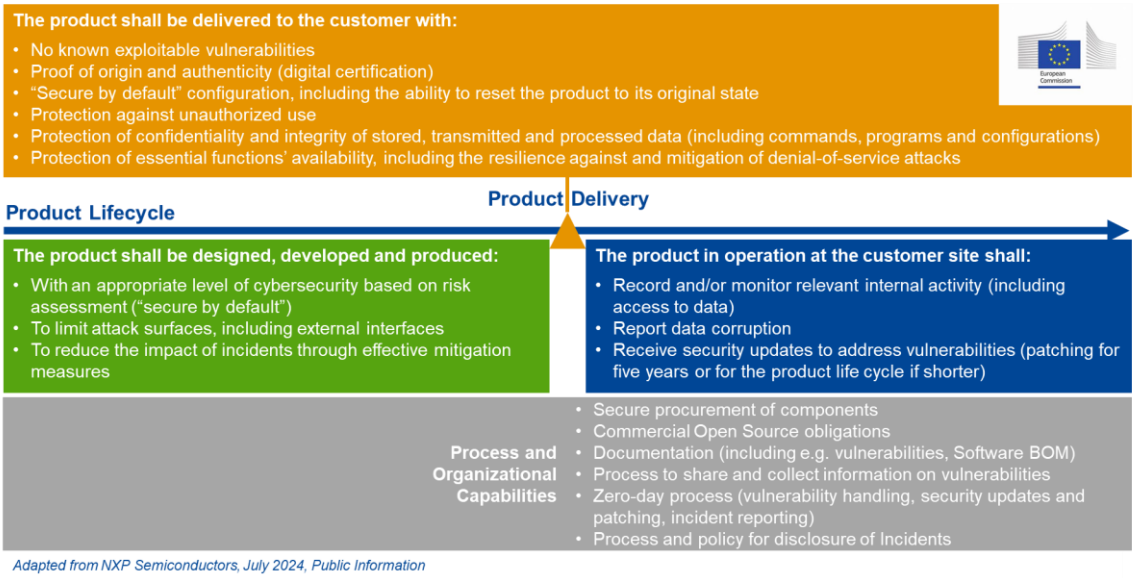
The EU Cyber Resilience Act (EU CRA): Key Insights

Background and Purpose

The EU Cyber Resilience Act (EU CRA) is designed to enhance the security of digital products, including software and connected devices. The Act establishes clear and consistent rules for companies to follow when making these products. This mandatory regulation reduces risks by requiring manufacturers to embed security in their products and promptly resolve any cybersecurity vulnerabilities identified in the field. The goal is to create a safer digital environment for everyone by encouraging the availability of "secure by default" products. The EU CRA requires manufacturers to place compliant products on the European Union market starting December 11, 2027. Manufacturers are also obligated to report severe incidents and actively exploited vulnerabilities to the relevant national authorities or Computer Security Incident Response Teams (CSIRTs) starting September 11, 2026.

Requirements

The EU CRA mandates that Products with Digital Elements (PDEs) which connect or interact with other devices or networks must meet essential cybersecurity requirements in their design, development, and production. The Act also requires vulnerability management throughout the product life cycle. The figure below provides an overview of the key obligations under the EU CRA.



Adapted from NXP Semiconductors, July 2024, Public Information

METTLER TOLEDO

Product Classification

The EU CRA categorizes PDEs into four groups with varying conformity assessment levels: "Common," "Important Class I," "Important Class II," and "Critical." "Important" and "Critical" PDEs are listed in Annexes III and IV. "Important" PDEs (e.g., firewalls) and "Critical" PDEs (e.g., Hardware Security Module, Smartcards) provide key cybersecurity functions or are essential for key entities or supply chains in the EU. They require compliance with harmonized standards and third-party certification. Products are listed under Annexes III or IV only if their core functions correspond to the specified types; combined products, such as Machinery, do not inherit the criticality classification. Despite differences in conformity assessments, the fundamental cybersecurity requirements for product characteristics remain consistent across all categories.

METTLER TOLEDO Statement

METTLER TOLEDO products are predominantly classified as "common" PDEs according to the EU CRA. METTLER TOLEDO is committed to both cybersecurity and cyber resilience, recognizing that effective cybersecurity requires both internal security measures and secure products. We strive to ensure a secure development and production environment through internal cybersecurity practices as well as secure and reliable operation of our products at customer sites through product security. A key component of this commitment is the official certification of our "MT Global Secure Product & Software Development Lifecycle" according to IEC 62443-4-1 covering all of our global R&D sites.

Our internal cybersecurity measures include, but are not limited to:

- Security teams in all regions
- Security Operations Center
- Advanced endpoint protection
- Encrypted storage and traffic
- Real time traffic monitoring
- Advanced firewalls
- Spam filter and suspicious mail reporting
- Internal and external penetration testing
- Network scanning tools
- End-user training and education

Our product security measures include, but are not limited to:

- Secure-by-design policies, processes and best practices
- Product Security Incident Response Team (PSIRT) and Open Source Compliance Officer (OSCO)
- Partnership with CERT@VDE for security advisories
- Product Security Subject Matter Experts (SMEs) within R&D Teams
- Software Composition Analysis (SCA), source code quality scanning, Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST) and penetration testing (both internal and by third parties)
- Secure-by-design training courses for R&D teams

METTLER TOLEDO is confident in the compliance of our products with the EU CRA when it takes effect because of the measures we already have in place. Our commitment to compliance with the EU CRA represents a further milestone in our continuous efforts to provide peace of mind to our customers.

Greifensee, April 10, 2026

Elena Markwalder
Head of Industrial Division and
GMC Sponsor Product Compliance

Markus Koepfli
Chief Information Officer

METTLER TOLEDO Legal Notice

This statement is METTLER TOLEDO's opinion at the date of its creation and does not create any new warranty for their products or software. The information provided is for your information only and does not extend METTLER TOLEDO's liability in any way. METTLER TOLEDO has made reasonable efforts to prepare this statement, but makes no representations, warranties, or assurances of any kind, express or implied, including but not limited to the accuracy, currency, completeness, or reliability of the information provided. METTLER TOLEDO shall not be liable for any damage or injuries resulting from accessing or using this information or relying on it. This statement is copyrighted and cannot be reproduced, published, or commercially exploited without written permission from METTLER TOLEDO