Scoop

THE LATEST TRENDS, SERVICES & PROMOTIONS

ELECTRICAL & ELECTRONICS JULY 2026

Protecting Every Connection: Decoding the EU's Cyber Resilience Act (CRA) Requirements

As smart home technology evolves from simple convenience tools into critical home infrastructure—controlling door locks, alarm systems, video surveillance, and remote access—the stakes for cybersecurity have never been higher. A compromised smart device is no longer just a data privacy issue; it can represent a breakdown in physical security, leading to unauthorized home access, disabled alarms, and critical safety risks.

For manufacturers looking to enter or remain in the European Union market, the era of treating cybersecurity as an optional "value-add" is over. With the enforcement of the EU's Cyber Resilience Act (CRA, Regulation (EU) 2024/2847), security is now a fundamental, legally mandated requirement.

What is the Cyber Resilience Act (CRA)?

The CRA is a landmark regulation designed to ensure that products with digital elements are secure throughout their entire lifecycle. With full enforcement set for December 2027, it mandates a systematic approach to security rather than a checklist of individual features.

The act fundamentally shifts the responsibility for cybersecurity from the consumer to the manufacturer, requiring a complete, closed-loop management system that encompasses several key pillars:

- **Secure Product Design and Default Configuration:** Security must be embedded from the initial design phase rather than added as an afterthought.
- **Lifecycle Vulnerability Management:** Manufacturers must implement ongoing monitoring, rigorous verification, and timely patching of vulnerabilities from the pre-market phase through to post-market support.
- **Supply Chain Security:** Businesses are now responsible for the integrity of their software and hardware supply chains, ensuring that integrated components do not introduce systemic risks.
- **Access Control and Data Protection:** Robust measures must be implemented to maintain the confidentiality, integrity, and availability of user data, ensuring that only authorized users have control over critical home infrastructure.

Smart security products—including smart locks, cameras, baby monitors, and security gateways—are now explicitly classified under the CRA, making these stringent requirements a mandatory gateway to the European market.

Streamlining Compliance with ETSI EN 304 632

To support the CRA, the technical standard ETSI EN 304 632:2026 has been developed to provide a clear compliance framework for smart home products with security functions.

This standard serves as a critical bridge between high-level legislative requirements and actionable technical implementation. It allows manufacturers to align their internal processes with CRA objectives by providing detailed guidance on core product capabilities, including:

- **Defining Technical Requirements:** The standard clarifies the necessary security features for doors, alarms, and control systems, ensuring they meet the performance criteria expected by the EU.
- **Vulnerability Governance:** By referencing CEN/CLC prEN 40000-1-3, the framework ensures that businesses do more than just "harden" their products. It mandates the creation of formal processes for receiving, verifying, and patching vulnerabilities, as well as publishing updates and tracking their impact.
- **Mapping to CRA Requirements:** Appendix A of ETSI EN 304 632 provides a direct mapping to the CRA's core mandates, such as data minimization, logging, and attack surface reduction.
- **Future Compliance:** The document indicates that if the standard is formally cited in the Official Journal of the European Union, adherence to its normative clauses will provide a "presumption of conformity" with the relevant CRA requirements, significantly simplifying the path to certification.

By utilizing this framework, manufacturers can move beyond basic security checks and build a mature, defensible compliance posture that addresses the full product context, including data, architecture, and interfaces.

How SGS Can Help Your Business

Navigating these complex regulations requires deep technical expertise and a structured compliance roadmap. SGS offers a comprehensive "one-stop" service to help manufacturers transition to these new standards seamlessly. Our services include:

- **CRA "Ready" Assessment:** We evaluate your Software Development Life Cycle (SDLC) activities, technical requirements, and vulnerability management processes to ensure you are prepared for official Notified Body (NB) certification.
- **Technical Evaluation:** We provide professional audits based on ETSI EN 304 632, helping you identify which requirements apply to your specific product context and architecture.
- **Vulnerability Governance:** Through our evaluation of CEN/CLC prEN 40000-1-3, we assist in establishing the necessary workflows for vulnerability reception, handling, and closed-loop management.
- **Global Expertise:** With our extensive global network of cybersecurity laboratories, SGS provides the testing and certification support needed to bring your smart products to the EU market with confidence and efficiency.

As the deadline for the CRA approaches, proactive compliance is not just about meeting a regulation—it is about securing your brand's reputation and ensuring the safety of the end-users who trust your products. Ready to start your compliance journey? Contact our expert to learn more!

Our cutting-edge testing solutions – coupled with our global presence and partnerships with key operators and stakeholders – make SGS the perfect partner for your wireless testing needs.

FOR ENQUIRIES

SGS HONG KONG

Mr Eddy Fong
e Eddy.Fong@sgs.com
m +852 6439 8648