Kigen

GUIDE

EU CRA COMPLIANCE GUIDE FOR EMBEDDED CELLULAR PRODUCTS

YOUR QUESTIONS ANSWERED OR FAQS

Cybercrime is now one of the largest economic threats facing businesses worldwide, with global costs estimated in the trillions of dollars annually. The EU Cyber Resilience Act (CRA) is Europe's response, introducing mandatory cybersecurity requirements for products with digital elements sold into the EU market.

A common challenge has seen much discussion: **how can we build connected products that can be securely deployed, updated, maintained, and evidenced throughout their lifecycle?** For cellular IoT products, eSIM technology emerged as one of the most practical foundations for CRA readiness. This guide answers your questions around practical impact and implementation.

The Cyber Resilience Act is an EU regulation that introduces cybersecurity requirements for products with digital elements placed on the EU market.

Manufacturers must demonstrate:

1. **Secure-by-design development**
2. **Vulnerability management processes**
3. **Security update capabilities**
4. **Technical documentation**
5. **Incident and vulnerability reporting**
6. **Ongoing product maintenance**

Reporting obligations begin in September 2026, while the main CRA requirements apply from December 2027. For hardware manufacturers, that means products being designed today may need to comply throughout their operational lifetime.

The CRA introduces significant consequences for serious non-compliance. Organisations may face fines of up to **€15 million or 2.5% of total annual worldwide turnover**, whichever is higher. Non-compliant products may also have their access to the EU market restricted.

The CRA is not punitive by design. **Its purpose is to raise the baseline of connected-product security.** However, manufacturers that delay preparation may face greater engineering, compliance and commercial challenges as the deadlines approach.

CRA readiness is an engineering and product-lifecycle priority—not simply a documentation exercise.

Several bodies share responsibility:

These organisations **assess conformity, oversee compliance, and enforce requirements** within their jurisdictions.

- Oversees implementation of the CRA.

Each EU Member State appoints:

- Notifying Authorities
- Notified Bodies
- Market Surveillance Authorities

- Supports vulnerability reporting and cybersecurity coordination across the EU.
- Operates the Single Reporting Platform for CRA-related reporting.

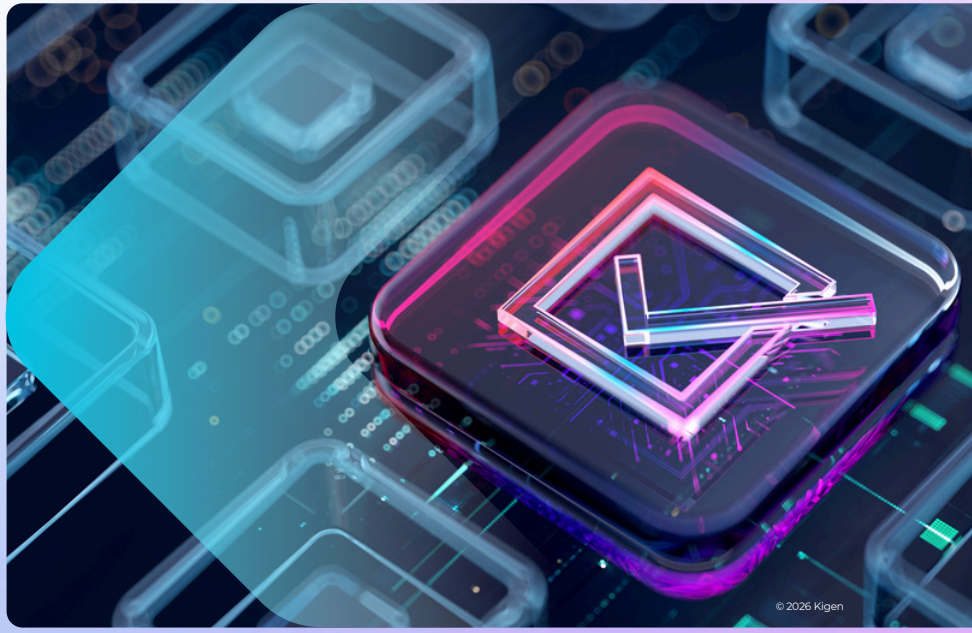
The CRA aims to reduce the growing economic and societal impact of insecure connected products. Historically, many connected devices have shipped with:

Weak security controls

Limited update mechanisms

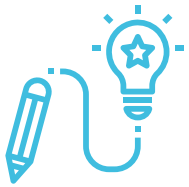
Poor vulnerability disclosure processes

The CRA seeks to establish a common cybersecurity baseline across the EU market. While some view this as an increasing regulatory burden, manufacturers that act early can turn security into a competitive advantage and simplify procurement discussions with enterprise customers.



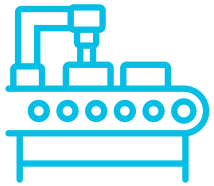
No. Formal harmonised standards will continue to evolve, but waiting may create significant delays.

Most cellular IoT products require:



Hardware Design

Certification



Manufacturing Preparation

Connectivity Integration

Field testing

These activities take years. A practical approach is to begin implementing recognised security practices now while monitoring emerging CRA guidance.

3 useful standards include:

- **ETSI EN 303 645 (secure IoT design)**
- **ISO/IEC 29147 (vulnerability disclosure)**
- **ISO/IEC 30111 (vulnerability handling)**

Under definitions of embedded class devices, hardware devices such as smart meters, security boxes, network cameras, smartcards and similar devices are classified as 'critical components' and represent the most intensive effort beyond 3rd party assessements. Embedded cellular designs benefit from eSIM as a secure element protecting device identity and the embedded crypto processor within the eUICC.

eSIM adoption has become significantly easier as IoT standards have evolved. The latest GSMA IoT eSIM architecture (SGP.32) brings many of the benefits previously available only in consumer eSIM deployments to constrained IoT devices.

1. **Select a certified eSIM solution**
2. **Choose a secure provisioning ecosystem**
3. **Integrate remote profile management early**
4. **Select a certified eSIM solution**
5. **Validate lifecycle operations before deployment**

Manufacturers can use Kigen's secure provisioning ecosystem or integrate their preferred connectivity providers.

eSIM does not make a product CRA-compliant by itself. However, it helps address several important CRA requirements.

An eSIM secures:

Device identity

Network credentials

Connectivity authentication

These credentials are critical assets because they determine how devices connect, authenticate, and receive updates.

This becomes particularly valuable for devices deployed in remote or inaccessible locations.

For cellular IoT deployments, **eSIM provides access to a mature ecosystem that includes**:

4 Remote profile lifecycle management

3 Secure provisioning infrastructure

2 Certified eUICC operating systems

1 Auditability and operational evidence

When evaluating suppliers, look beyond connectivity. Key capabilities matter:

Capability	Why it matters
GSMA-certified eUICC	Trusted device identity
Secure eSIM OS	Protection of credentials
Multiple form factors	Supports product roadmap scaling
SAS-certified provisioning	Supports product roadmap scaling
eIM support	Remote lifecycle management
Interrupted download recovery	Reliable field operations
Audit logs and evidence	Supports CRA documentation
Developer SDKs and APIs	Simplifies integration and testing

The goal is not simply connectivity. It is secure lifecycle management.

One of the biggest challenges in CRA compliance is vulnerability management. Once organisations generate vulnerability scanners, they often produce large numbers of alerts.

Many are **false positives.**
Reachability analysis helps determine whether a vulnerability is:

1. **Present**
2. **Reachable**
3. **Mitigated**
4. **Actionable**

Instead of treating every vulnerability equally, teams can prioritise based on actual risk.

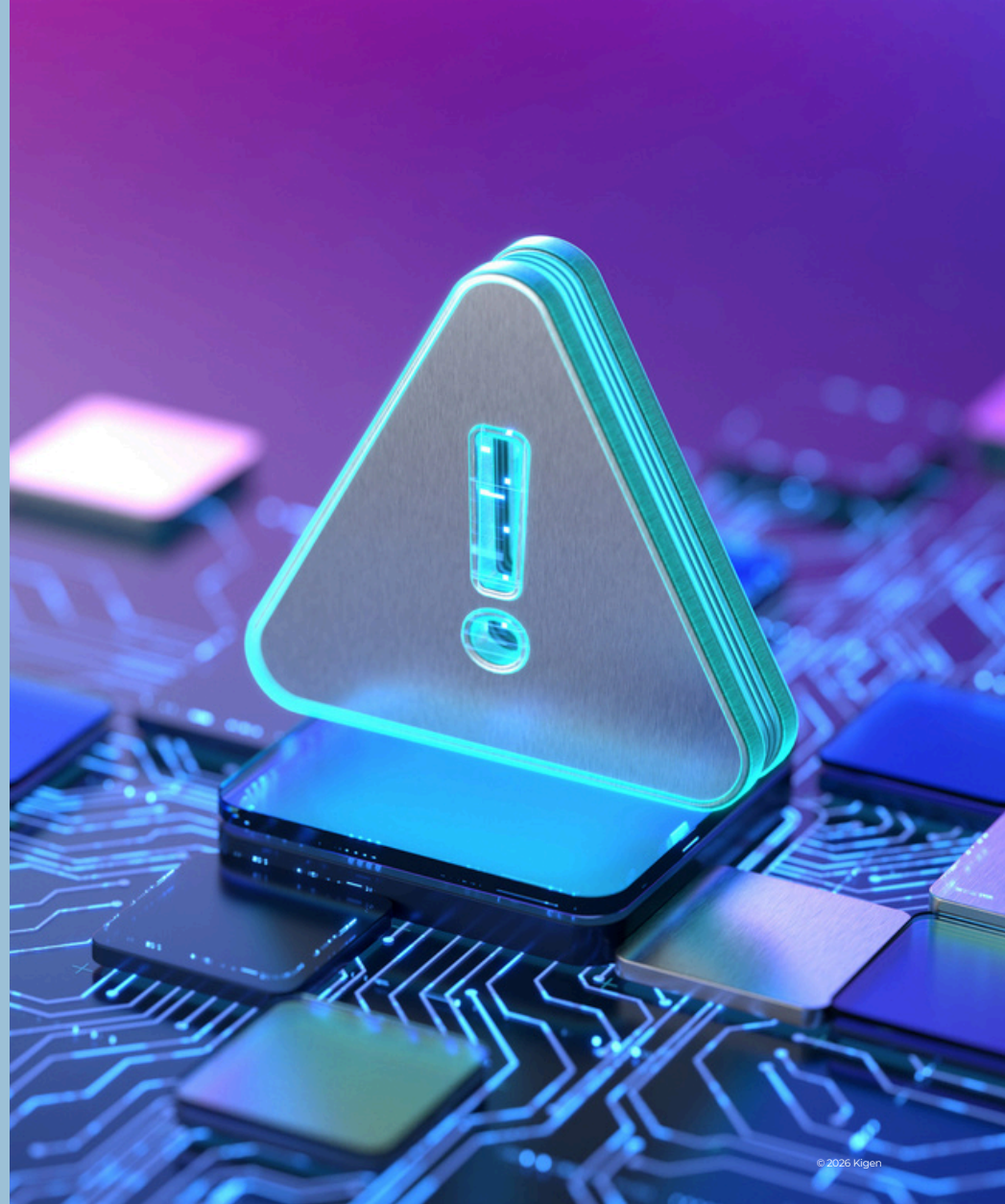
A practical workflow combines >>

Adopt a risk-based approach.
For each vulnerability, determine:

1. **Is the vulnerable component present?**
2. **Is it externally exposed?**
3. **Is mitigation already in place?**
4. **Select a certified eSIM solution**
5. **Does remediation require action?**

Automating this process using SBOM and reachability tooling significantly reduces operational burden.

Many organisations are adopting CycloneDX-based workflows and API-driven vulnerability reporting to streamline compliance activities.

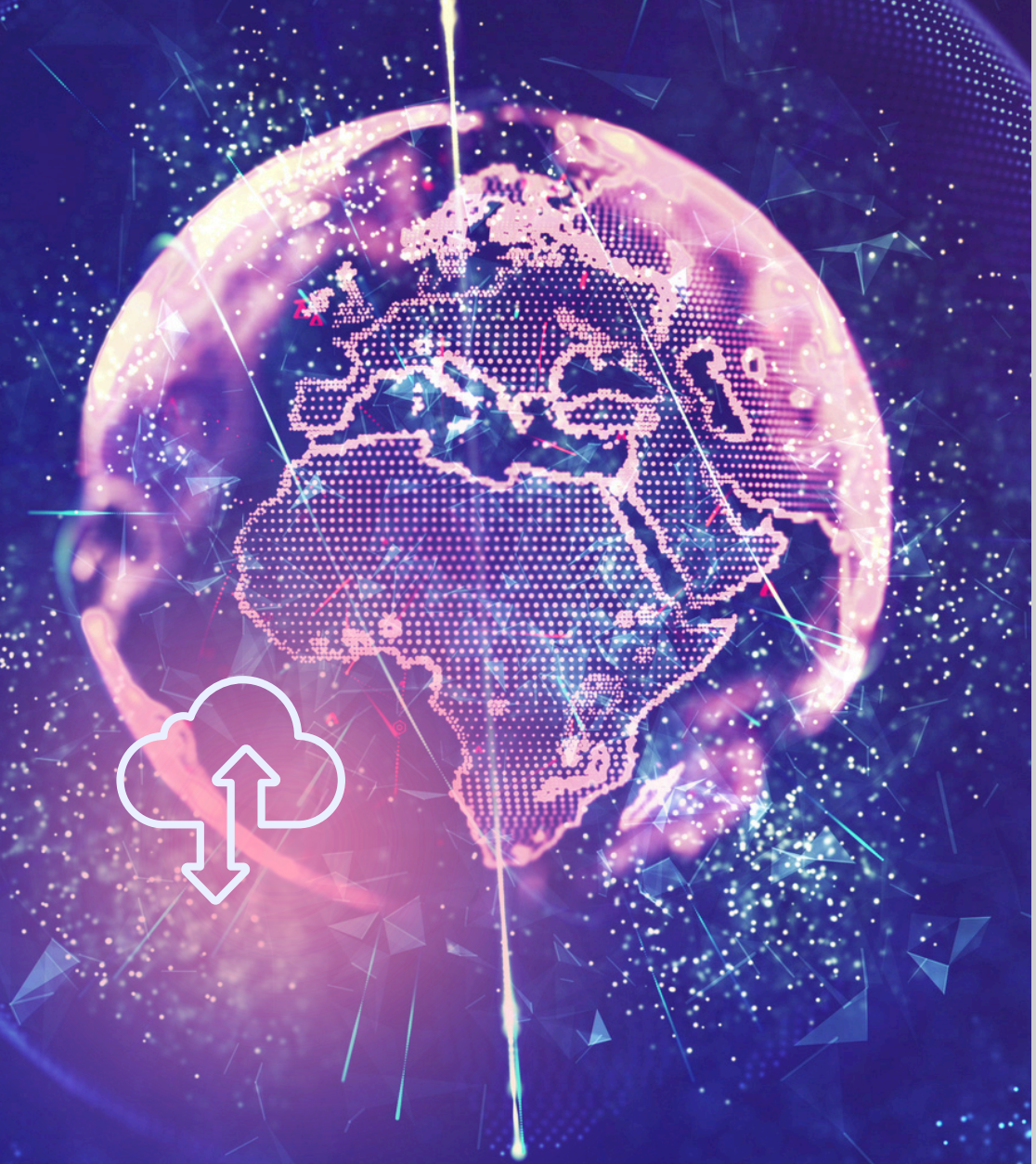


CRA compliance requires more than delivering updates. Manufacturers must demonstrate that products can be securely maintained throughout their lifecycle.

eSIM remote management helps by:

- **Supporting profile lifecycle operations**
- **Providing operaitonal evidence**
- **Enabling secure provisioning changes**
- **Maintaining device reachability**

This information can become part of the product's compliance documentation.



Yes.
Modern IoT eSIM architectures can support NB-IoT deployments. However, manufacturers should verify:

1. **Transport support**
2. **Retry behaviour**
3. **Timeout handling**
4. **Recovery mechanisms**
5. **Non-SMS bearer support where required**

Battery-powered NB-IoT devices often experience intermittent connectivity, making interrupted download recovery particularly important.

If the eIM implementation supports the required transport mechanisms, remote profile management can operate successfully over NB-IoT networks.

The CRA aims to reduce the growing economic and societal impact of insecure connected products.
Historically, many connected devices have shipped with:

1. **Product complexity**
2. **Existing security maturity**
3. **Documentation readiness**
4. **Vulnerability management processes**
5. **Supply chain visibility**

Many organisations already face compliance obligations under RED, CE marking, telecom approvals, and sector-specific regulations.

CRA introduces additional requirements around cybersecurity lifecycle management.

Beyond compliance, embedded teams should consider and plan for the costs of connectivity needed for security updates for lifecycle management.

The European Commission provides a CRA cost calculator to help organisations estimate likely impacts.
The earlier security processes are integrated into development workflows, the lower the long-term compliance burden tends to be.

For embedded developers and hardware manufacturers, CRA compliance is becoming a product design requirement rather than a documentation exercise.

1. **Building secure connectivity into product architecture**
2. **Generating SBOMs**
3. **Implementing vulnerability disclosure processes**
4. **Using reachability analysis to reduce false positives**
5. **Designing secure update mechanisms**
6. **Selecting partners that provide lifecycle evidence**

eSIM is not a shortcut to compliance, but it provides one of the strongest foundations for secure identity, remote management, and long-term maintainability in cellular IoT products.

The investment in eSIM allows you to plan that your updates for application and SBOM will land and can report back for CRA-compliance

Kigen helps manufacturers build secure cellular products using:

1. **GSMA-certified eSIM technology**
2. **Secure eUICC operating systems**
3. **Secure provisioning infrastructure**
4. **eIM-enabled remote management**
5. **Embedded developer tooling**
6. **Portable C-SDKs and reference implementations**

This enables manufacturers to move from prototype to production with a secure connectivity foundation while generating the evidence increasingly required for CRA readiness.

Scan the QR code and leave your information.
We will contact you shortly.
For more information, please visit Kigen.com.
Or follow @Kigen and the #FUTUREOF***SIM***
conversation on LinkedIn.

License and legal information