eurofins | Electrical & Electronics

REDDA - CRA SEMINAR

Thami Elidrissi

Cyber resilient Products

eurofins | Electrical & Electronics

- **Standards, Assessments and Future Outlook**
- **From RED Delegated Act to Cyber Resilience Act (CRA)**
- **Focus:**

  RED-DA Requirements

  CRA Preparation

  EN 18031 Assessments

  ETSI / IEC / ISO Cybersecurity Standards

  CRA Readiness Roadmap

  Practical Compliance Strategies

  Take-away

Why This Topic Is Critical Now

eurofins | Electrical & Electronics

Cybersecurity Becomes a Product Requirement

In the Past:
Focus on functionality

Security as an optional feature

Penetration testing only project-specific

Today:
Cybersecurity is CE-relevant

Security by Design is becoming mandatory

Manufacturers are liable for vulnerabilities

Lifecycle security becomes mandatory

Affected Products:

IoT Devices
Radio Equipment
Embedded Systems
Industrial Devices
Consumer Electronics
Smart Home
MedTech
Automotive Components

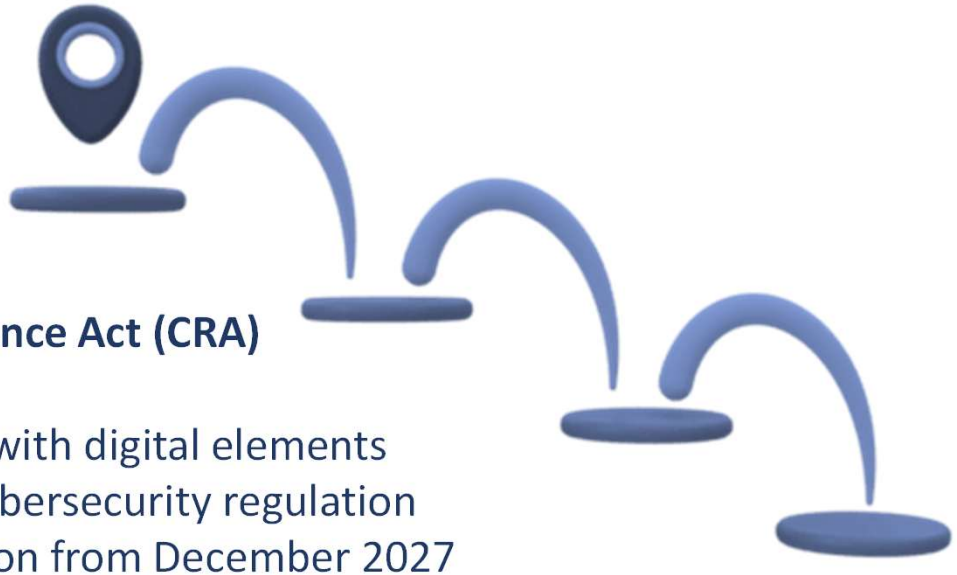
Key Takeaway:
Even basic connectivity may trigger CRA applicability.

European Cybersecurity Regulation

eurofins | Electrical & Electronics

The New Regulatory Landscape

RED Delegated Act (RED-DA)
Focus:
Radio equipment
Product cybersecurity
Mandatory since August 2025



Cyber Resilience Act (CRA)
Focus:
All products with digital elements
Horizontal cybersecurity regulation
Full application from December 2027

EU Objectives:
Protection of critical infrastructure
Consumer protection
Reduction of cyberattacks
Harmonized security level

RED-DA Overview

eurofins | Electrical & Electronics

RED Article 3(3)(d)(e)(f)

Art. 3(3)(d)
Protection of Networks
No harmful impact on communication networks
Protection against misuse

Art. 3(3)(e)
Privacy & Data Protection
Protection of personal data
Access protection
Secure processing

Art. 3(3)(f)
Fraud Protection
Protection of virtual assets
Protection of payment functions
Protection against identity misuse

EN 18031 Standards Family

eurofins | Electrical & Electronics

Technical Basis for RED-DA

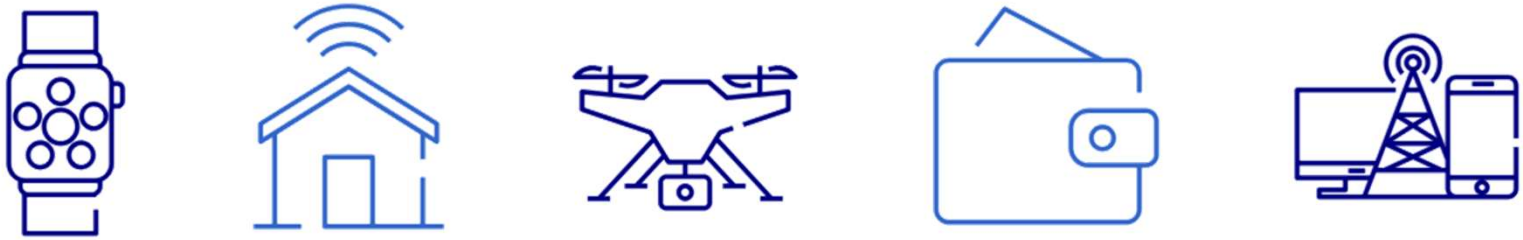
EN 18031-1:2024
Internet-connected Radio Equipment

EN 18031-2:2024
Protection of Privacy & Personal Data

EN 18031-3:2024
Fraud Prevention & Financial Protection

Main Assessment Areas:

- Authentication
- Access Control
- Secure Update
- Secure Boot
- Cryptography
- Logging
- Data Protection
- Hardening
- Vulnerability Handling



CRA: The Major Shift

eurofins | Electrical & Electronics

Cyber Resilience Act (CRA)

Applies to:

✓ Software
✓ Hardware
✓ Embedded Systems
✓ IoT Devices
✓ Cloud-connected Products

Core Principles:

- Security by Design
- Security by Default
- Vulnerability Management
- Secure Development Lifecycle
- Security Updates
- Incident Reporting

New Reality:

Cybersecurity becomes part of the entire product lifecycle.

CRA Timeline

eurofins | Electrical & Electronics

CRA Timeline

December 10, 2024

CRA officially enters into force

September 11, 2026

Mandatory:

- Vulnerability Reporting
- Incident Reporting

December 11, 2027

Full CRA applicability

Challenge:

Companies already need:

- Processes
- Security Governance
- Documentation
- Engineering Readiness

Key Cybersecurity Standards

eurofins | Electrical & Electronics

Cybersecurity Standards Landscape

- **ETSI EN 303 645 With TS 103 701**

Consumer IoT Security

- **IEC 62443-4-1**

Secure Development Lifecycle

- **IEC 62443-4-2**

Security Technical Requirements

- **ISO/IEC 27001**

Information Security Management

- **ISO/SAE 21434**

Automotive Cybersecurity

- **Practical Reality:**

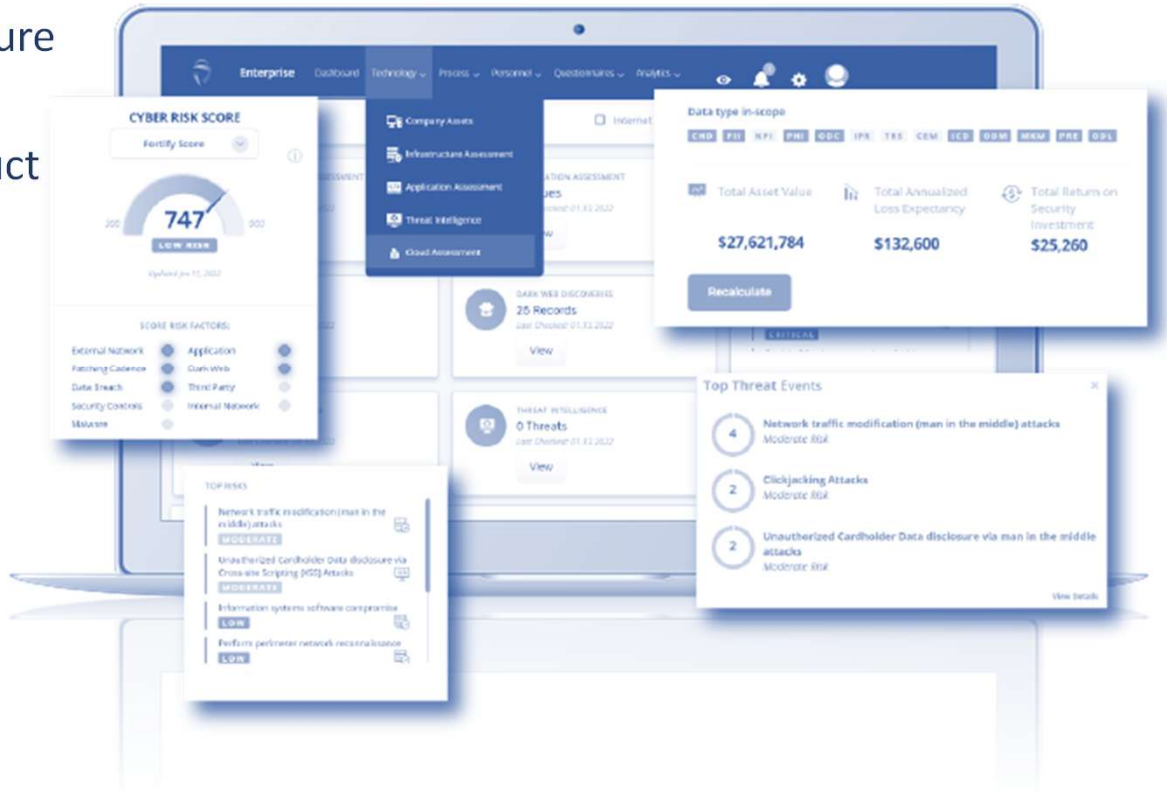
No single standard covers everything.

Assessment Methodology

eurofins | Electrical & Electronics

Typical Cybersecurity Assessment Flow

1. **Scope Definition**
   Understanding the product & architecture
2. **Gap Analysis**
   Comparing standards against the product
3. **Technical Assessment**
   Technical verification
4. **Evidence Review**
   Documentation review
5. **Risk Evaluation**
   Risk & threat analysis
6. **Final Compliance Report**
   Proof of conformity



Typical Technical Assessments

eurofins | Electrical & Electronics

Security Assessment Examples

Technical Evaluations:

- ✓ Password Security
- ✓ Secure Boot
- ✓ Firmware Integrity
- ✓ Encryption Validation
- ✓ OTA Update Security
- ✓ Access Rights
- ✓ API Security
- ✓ Session Handling
- ✓ Vulnerability Scanning
- ✓ Misconfiguration Review

Goal:

- ✓ Demonstrating structured security controls.

Common Weaknesses

eurofins | Electrical & Electronics

What Companies Often Underestimate

Typical Findings:

- ❌ Default Passwords
- ❌ Insecure Update Processes
- ❌ Missing SBOM
- ❌ No Vulnerability Policy
- ❌ Weak Cryptography
- ❌ Missing Logs
- ❌ Insecure APIs
- ❌ Hardcoded Credentials

Reality:

Many products fail more because of processes than technology.

CRA Readiness Roadmap

eurofins | Electrical & Electronics

Practical Implementation Approach

Phase:

1. Regulatory Screening
2. Gap Analysis
3. Security Improvements
4. Testing & Assessments
5. Technical Documentation
6. Lifecycle Compliance

Important:

CRA is not a one-time project.

Phase 1 – Screening

eurofins | Electrical & Electronics

“Is my product even affected?”
The first step is to evaluate the regulatory relevance of the product.

Key Questions:
Does the product contain software, firmware, or digital functions?
Can the product send, receive, or process data?
Does the product include network or radio communication?
Will the product be placed on the EU market?
Is it a consumer or industrial product?
Is there already RED relevance?

Objective of this Phase:
Determine the CRA scope
Determine the RED-DA scope
Assess the criticality of the product
Identify the product class
Define applicable regulatory requirements

Typical Outcome:
✓ Product Classification
✓ Regulatory Scope Matrix
✓ Initial Risk & Compliance Assessment

Phase 2 – Gap Analysis

eurofins | Electrical & Electronics

“Where do we stand today against the requirements?”

This phase consists of a structured comparison of the existing product against relevant standards and regulatory requirements.

Typical References:

EN 18031-1/-2/-3
ETSI EN 303 645
IEC 62443-4-1
IEC 62443-4-2
CRA Annex I (part I and II)
CRA Annex II (User info.)
CRA Annex VII (technical doc).
Internal Security Policies

Evaluated Areas:

Technical Security

Secure Boot
Authentication
Encryption
Access Control
Secure Updates
Logging
Hardening

Organizational Security

Secure Development Lifecycle
Vulnerability Management
Incident Handling
Supplier Security
SBOM Management

Objective:

Achieve transparency regarding:
Existing compliance gaps
Technical weaknesses
Missing processes
Missing evidence

Typical Outcome:

✓ Gap Analysis Report
✓ Prioritized Findings
✓ CRA Readiness Score

Phase 3 – Remediation

eurofins | Electrical & Electronics

“How do we close the identified gaps?”

After the analysis, the actual technical and organizational implementation begins.

Technical Measures:
Implementation of Secure Boot
Improvement of password policies
Introduction of secure OTA updates
API hardening
Cryptography improvements
Deactivation of insecure services

Organizational Measures:
Introduction of a Vulnerability Disclosure Policy
Establishment of an Incident Response Process
Implementation of a Secure Development Lifecycle
Strengthening supplier management
Integration of SBOM management

Important:
Many CRA requirements affect not only the product itself, but also company-wide processes.

Typical Outcome:
✓ Improved Product Architecture
✓ Defined Cybersecurity Processes
✓ Security Governance Framework

Phase 4 – Evidence Package

eurofins | Electrical & Electronics

“How do we demonstrate compliance?”

CRA and RED-DA require traceable and well-structured technical documentation.

Typical Contents:

Technical Documentation
Product description
Architecture diagrams
Data flow
Security design

Risk Analysis
Threat modelling
Attack surface analysis
Risk treatment

Test Evidence
Test reports
Assessment reports
Vulnerability scans
Penetration testing results

Process Evidence
Update policy
Vulnerability handling
Incident management
Secure Development Lifecycle

Important:
It is not enough to implement security —
it must also be documented in a verifiable manner.

Typical Outcome:
✓ Technical Compliance Dossier
✓ Audit-Ready Documentation
✓ Preparation for Notified Body Assessment

Phase 5 – Conformity Assessment

eurofins | Electrical & Electronics

“Which assessment procedure is required?”
Depending on the product and risk class, different conformity assessment routes may apply.

Possible Routes:

Internal Production Control
The manufacturer declares conformity independently.

Notified Body Involvement
Required for:
Certain critical products
Missing harmonized standards
Higher assurance requirements

Role of the Notified Body:
Technical evaluation
Documentation review
Independent conformity assessment
Support for regulatory confidence

Challenge:
Many companies underestimate:
Preparation time
Documentation quality
Technical depth of assessments

Typical Outcome:
✓ CE Compliance Readiness
✓ Audit Readiness
✓ EU Market Access

Phase 6 – Lifecycle Compliance

eurofins | Electrical & Electronics

“Compliance does not end after certification.”
CRA fundamentally changes the understanding of product compliance.

New Reality:
Cybersecurity becomes a continuous process.

Manufacturer Obligations After Market Placement:

Monitoring
Monitor vulnerabilities
Follow threat intelligence

Vulnerability Handling
CVE management
Security patches
Responsible disclosure

Security Updates
Secure update processes
Update availability
Update integrity

Post-Market Surveillance
Analyze security incidents
Evaluate customer feedback
Continuously monitor compliance

Important:
A product remains compliant only if security is actively maintained.

Typical Outcome:
✓ Sustainable Compliance
✓ Reduced Cyber Risks
✓ Long-Term Regulatory Stability

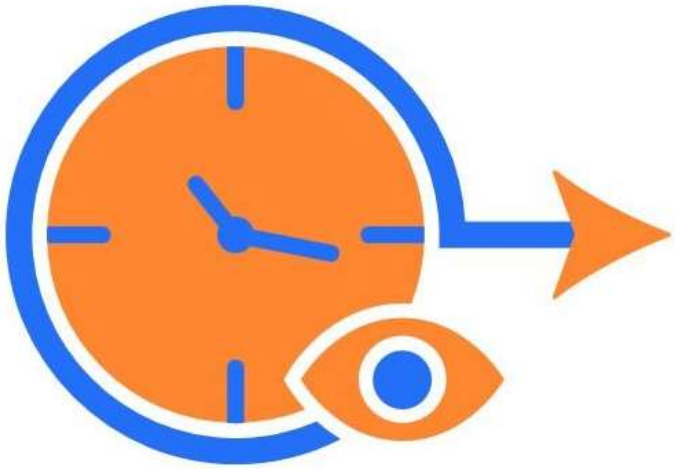
Future Outlook

eurofins | Electrical & Electronics

Where Is the Market Heading?

Expected Developments:

- More mandatory certifications
- Higher SBOM requirements
- AI security requirements
- Supply chain security focus
- Cloud & OTA governance
- Global alignment of cybersecurity standards



Trend:

Cybersecurity becomes a market access requirement.

Closing & Key Takeaways

eurofins | Electrical & Electronics

Key Learnings

RED-DA

Already a reality for radio products

CRA

Transforms the entire product development lifecycle

Successful Companies:

✓ Integrate security early
✓ Establish SDLC processes
✓ Build compliance strategically
✓ Combine technology + governance

Cybersecurity Compliance = Business Enablement

Take-Away

eurofins | Electrical & Electronics

- Cyber Resilience is a product lifecycle
- Standards Competence + Assessments + Documentation
- Vulnerability Management is crucial.
- Cybersecurity Compliance = Business Enabler

eurofins | Electrical & Electronics

Dipl.Ing Thami El Idrissi

Cybersecurity Global Director
Eurofins E&E Global

Thami.ElIdrissi@cpt.eurofinseu.com

www.eurofins.com/ee