Embedded France
L'EMBARQUÉ MADE IN FRANCE

Embedded France, Embedded Cybersecurity Working Group

White paper:
Embedded Systems Cybersecurity Trends & Implementation

Version 1.4, November 9th 2025.

Executive Summary

In many industries, the driving forces for cybersecurity requirements are the mandatory regulations. Within the EU, regulation is even the most important mega-trend, imposing mandatory cybersecurity measures, alongside other standards, national regulations, and some international standards.

European regulation is very active regarding cyberspace security. In this whitepaper, we make a synthesis, stressing the important points (what, who, when) in this regard. We also propose useful hints to get ready. Indeed, the clock is ticking! We recall the chronology until all the arsenal is entering into force (2027).

All products that are directly or indirectly connected to another device or network will need to apply a conformance procedure and write a declaration of conformity. The exact compliance modalities & processes are still under definition. But what is for sure is that non-compliance will cause sanctions.

The primary audience for this white paper is corporate cybersecurity governance. But cybersecurity developers will also be curious about the practical information about compliance requirements and practical ways to comply. This document is a vade mecum to fully understand the operational impact of EU regulation on the processes and products of all companies (even outside EU) that aim to sell digital products on the EU market.

This white paper states what *shall (=must)* be done and additionally gives recommendations on how they *ought* to be done. Indeed, CEN / CENELEC is preparing standards in this respect, but definitely some actions must be anticipated. We deliver in this document pieces of advice that serve this purpose.

Embedded France is an association where the private sector gathers in order to strengthen France’s leadership in the embedded systems B2B market. More particularly, its cybersecurity Working Group aims at providing return on experience and guidance for the changing state of the art in this field, shaped by growing requirements on trustworthiness, that can only appear if the underlying technologies are cyberproof by design and designed to remain so along their lifecycle. Embedded France is your partner in this respect, and we hope that this white paper will shed some light of clarity on the topic of the regulation of embedded systems.

Table of Contents

Regulation as a Driver for Cybersecurity

State of the Union

We are concerned with “embedded-oriented” mega-trends. Below, find one picture taken at the entrance of Embedded World 2025 which took place March 11-13 in Nüremberg (Germany). It clearly shows that there is an urgent topic to comply with.

The question becomes more problematic when considering that EU CRA is just one regulation. In practice, there are several of them. Several think tanks (such as Renaissance Numérique, or The Digital New Deal) also underline this legislative puzzle. It can be stated and analyzed as follows:

- Multiple regulations coexist;
- Complying is all is looking like a challenge, but (fortunately) they are mostly aligned one with each other;
- There are means to comply with all, but not as an afterthought: the compliance must be an objective to follow in the first place;
- This whitepaper guides in this respect;
- Our proposed methodology (step by step) allows you to make good decisions and actions in this respect.

We thereafter explain the *a priori* complexity of the multitude of regulations. In practice, it is even delicate to determine which norms a given product or industry is subject to. There is a risk that complexity is “destructive”, in that the confusion hinders the goal of increasing the overall cybersecurity level.

Methodology Overview

As an introduction, let’s make the difference between *organizations, supply chain* & *products*.

Organisations developing, producing, and selling embedded systems need to address three levels of cybersecurity:

- Their IT infrastructure and processes, like any organisation;
- The end-to-end supply chain for the development, manufacturing, delivery, maintenance and service processes of their products and solutions;
- The cybersecurity of their products once operated by their customers.

These three levels are different and require independent courses of action, although they have to rely on each other to yield the right level of security.

Taking the example of the automotive industry (well-structured - hence out of the scope of EU CRA, but perfectly illustrative):

- The IT and OT infrastructures of the company need to be protected against cyberattacks. Still, these infrastructures are massively connected to the outside world, having to deal with their customers, the connectivity of the vehicles, the dealership and servicing networks, the suppliers, to cite a few.

- The whole supply chain for a given vehicle type needs to be traced and protected from the earliest stages of design: mastering the software components of each electronic control unit (there can be around 100 of them in each car) from coding to loading in each manufactured car, key distribution for the encrypted processes such as car access, connectivity… All of them are subject to field upgrades during the lifecycle of the vehicle.

- The cybersecurity of the vehicle itself, once in customers’ hands, depends on the electronic architecture and the technologies implemented in the vehicles.

We now address the different regulations individually.

Debunking Horizontal Regulations

EU CRA (Cyber Resilience Act)

What?

The EU CRA aims to enhance the cybersecurity of “*products with digital elements*” (*sic*) by imposing security requirements throughout their lifecycle.

This text imposes minimum requirements for the cybersecurity of digital products. The CRA covers the hardware and software parts of products (a software or hardware product and its remote data processing solutions, including software or hardware components marketed separately). Non-commercial" open-source software is excluded, except that distributed for commercial purposes (integrated into products). The CRA applies to all manufacturers based in the EU. In addition, abroad manufacturers shall comply as well if they intend to distribute their products within the EU market.

By implementing the CRA, manufacturers must:

- Integrate cybersecurity right from the product design stage
- Deploy a cyber risk analysis process
- Implement a product vulnerability management process.
- Depending on the criticality of their products, either carry out a self-assessment or obtain third-party certification.

The CRA requires the manufacturer to:

- Clearly indicate the end-of-support date for updates;
- Report identified vulnerabilities in their products within a constrained timeframe, that can be as low as 72 hours (a European notification platform will be set up); early warning notification shall arise within 24 hours;

Penalties:

Penalties are provided for non-compliance: no CE marking, financial fines, and can go as far as product withdrawal.

EU CRA applies to all markets except medical, aero, vehicles (UN ECE R.155), and defence (not a competency of the EU)

Who is concerned?

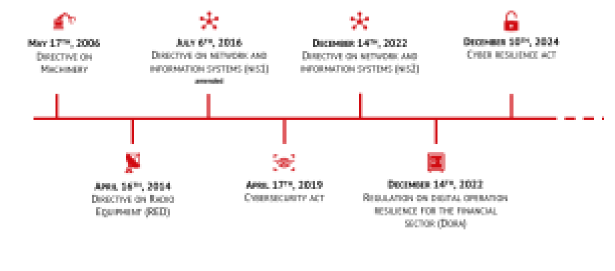
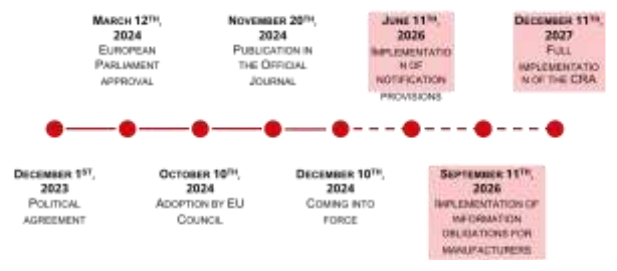
- Manufacturers
- importers, and
- distributors of digital products.

When?

The CRA will be implemented gradually. Important dates are:

- June 11, 2026: application to conformity assessment bodies;
- September 11, 2026: entry into force of system vulnerability notification obligations for manufacturers;
- December 11, 2027: entry into force of the CRA in its entirety.

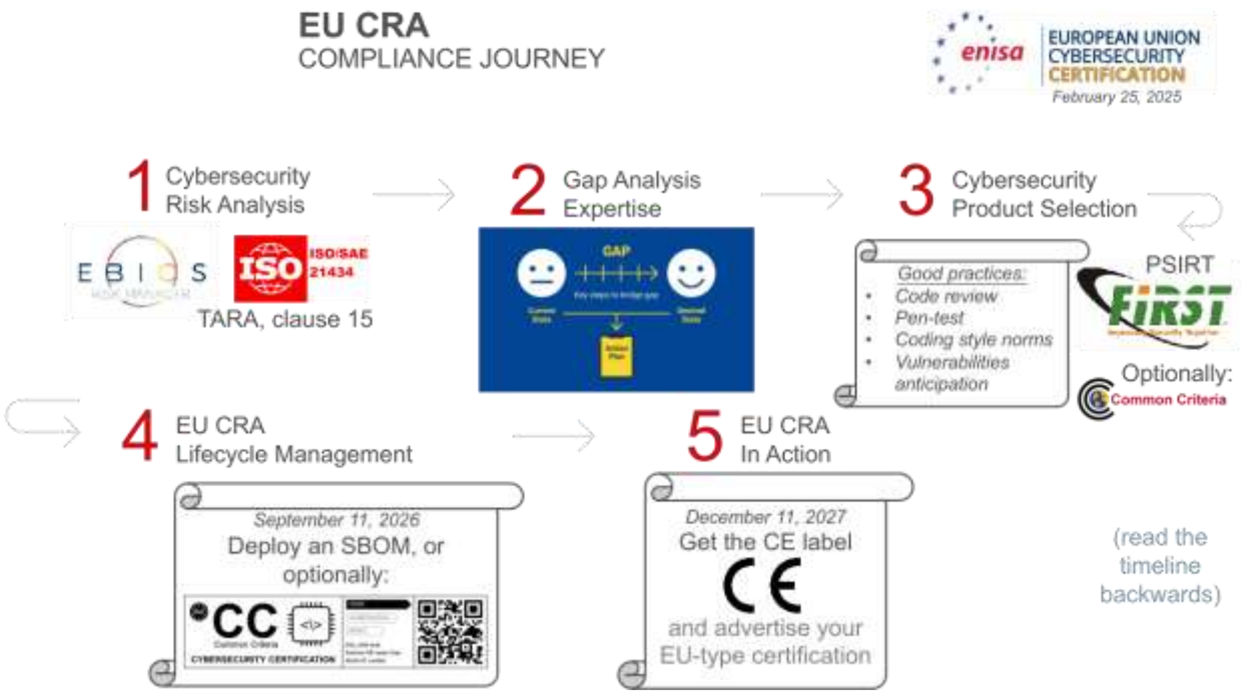
The timelines are defined below:

An ever-evolving European cybersecurity regulatory environment is leading to EU CRA…	… with a well-defined implementation timeline towards 2027.
	

May 17th, 2006
Directive on Machinery
July 6th, 2016
Directive on network and information systems (NIS1)
amended
December 14th, 2022
Directive on network and information systems (NIS2)
December 10th, 2024
Cyber resilience act
April 16th, 2014
Directive on Radio Equipment (RED)
April 17th, 2019
Cybersecurity act
December 14th, 2022
Regulation on digital operation resilience for the financial sector (DORA)

March 12th, 2024
European Parliament approval
November 20th, 2024
Publication in the Official Journal
June 11th, 2026
Implementation of notification provisions
December 11th, 2027
Full implementation of the CRA
December 1st, 2023
Political agreement
October 10th, 2024
Adoption by EU Council
December 10th, 2024
Coming into force
September 11th, 2026
Implementation of information obligations for manufacturers

The following diagram shows the path to the CE logo:



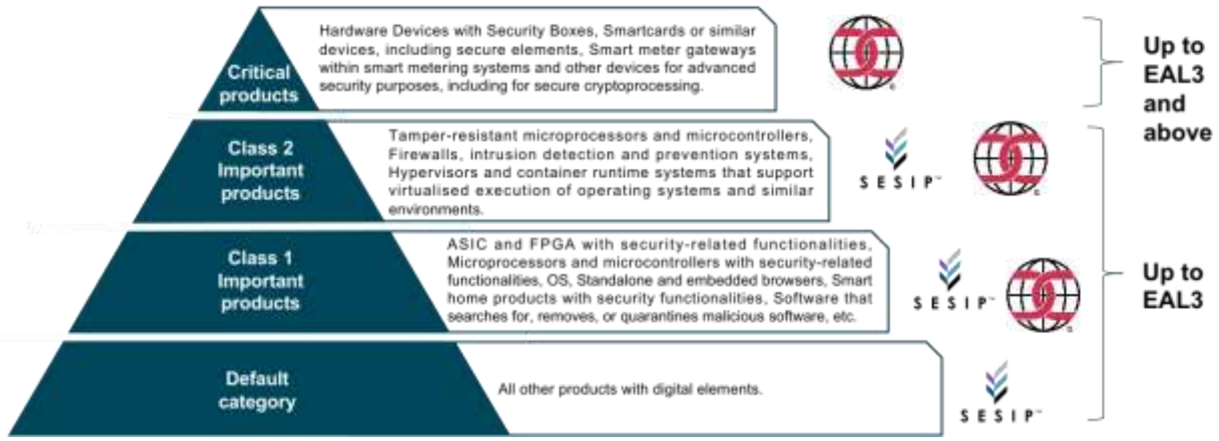
There are three ways to achieve compliance:

1. When the product pertains to a class of applications that is not regulated by EU CRA, simply obey the domain-specific standard;
2. When there is no other "better saying" standard, there is a shortcut if the product is CC-certified, as proposed by the EUCC scheme;
3. Otherwise, a full-fledged certification is required, as described below.

In the first case, direct application of the standards already in place is mandatory. This should be business as usual, as this standard already governs the given industry.

In the second case, this amounts to applying Common Criteria (i.e., ISO/IEC 15408) to the product. This is also very well framed. Products falling into the "critical" category might already use this path. It is now mandated that the scheme be EUCC. From a user perspective, this scheme does not differ much from regular CC certification, except in the organization of the test labs. Their quotations are also different, though. One possible transposition of EU CRA requirement into EUCC compliance is depicted below:

Classes can be mapped with standards and Evaluation Assurance Levels (EALs)



Critical products

Hardware Devices with Security Boxes, Smartcards or similar devices, including secure elements, Smart meter gateways within smart metering systems and other devices for advanced security purposes, including for secure cryptoprocessing.

Class 2 Important products

Tamper-resistant microprocessors and microcontrollers, Firewalls, intrusion detection and prevention systems, Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments.

Class 1 Important products

ASIC and FPGA with security-related functionalities, Microprocessors and microcontrollers with security-related functionalities, OS, Standalone and embedded browsers, Smart home products with security functionalities, Software that searches for, removes, or quarantines malicious software, etc.

Default category

All other products with digital elements.

Eventually, complying with the pure EU CRA requires a full interpretation of this regulation. Hence the steps we recommend are listed below:

1. Find a partner to perform an initial cybersecurity risk assessment. This can be concretized as a consulting service;
2. Perform a gap analysis, which can be one step of the risk management strategy. The organization of EBIOS workshops is suitable at this stage;
3. Study the need for action, e.g., through the adoption of good practices, such that:
    a. Anticipation of the vulnerabilities
    b. Code review
    c. Pen testing
    d. Coding as per (security) norms & checking thereof
4. Deploy a software bill of material (SBOM):
    a. Decide on the correct granularity
    b. Reflect on tooling and automation
5. Put in place a vulnerability management system (e.g., a PSIRT), aligned with ISO/IEC 29147:2018 for vulnerability disclosure and ISO/IEC 30111:2019 for vulnerability handling process;
6. With these actions executed, you are ready to enter the EU CRA era!

Producers of digital products must manage to map the technology they will be using through their supply chain, for the proper risks to be mapped to the right technology.

The byproduct of conformity is to advertise in terms of product quality and added value.

EU CRA by compliance recommends 41 norms, amongst them:

- IEC 62443 - industrial systems;
- EN 18031:2024 - radio electric devices;
- IEC 63452 - railway / trains. Are in the scope of EU CRA.The future norm ISO CEI 63452 integrate some requirements from the CRA, the European Commission has not formally accepted to exonerate this section the comply to CRA.

Penalties: Non-compliance can result in fines up to €15 million or 2.5% of the company's total worldwide turnover.

Steps to ensure compliance:

- Conduct a thorough risk assessment of all digital products;
- Implement security measures throughout the product lifecycle, including secure by design and secure by default principles;
- Regularly update and patch products to address vulnerabilities;
- Document compliance and maintain records for audits;
- Train staff on cybersecurity best practices.

AI Act

What? The Artificial Intelligence (AI) Act regulates the use of artificial intelligence based on its risk level, with specific requirements for each category.

Who is concerned? Developers and users of AI systems, as well as AI service providers.

When?

- 2025: Implementation expected;
- 2026: Full compliance required.

Penalties: Non-compliance with certain AI practices can result in fines up to €35 million or 7% of the company's annual turnover. Other violations can result in fines up to €15 million or 3% of the company's annual turnover.

Steps to Ensure Compliance:

- Classify AI systems based on their risk level;

- Implement appropriate safeguards for high-risk AI systems, including transparency and accountability measures;
- Conduct regular audits and assessments of AI systems;
- Ensure data protection and privacy compliance;
- Provide clear documentation and user instructions.

Please refer to the presentation that our Working Group gave on Tuesday March 25, in Bruxelles (Belgium): https://eucyberact.org/session/22-months-to-comply-to-european-cyber-resiliency-act-eu-cram03a/

Debunking Vertical Regulations

RED (Radio Equipment Directive)

What? The RED establishes essential requirements for radio equipments to ensure their safety and compatibility.

Who? Manufacturers, importers, and distributors of radio equipment.

When?

- 2014: In force since;
- Ongoing: Regular updates to include new technologies.

Penalties: Non-compliance can lead to fines and product recalls, but specific amounts vary by member state.

Steps to Ensure Compliance:

- Ensure all radio equipment meets essential requirements for safety and compatibility;
- Conduct conformity assessments and obtain necessary certifications;
- Maintain technical documentation and compliance records;
- Monitor and update equipment to address new technological developments;
- Train staff on regulatory requirements.

NIS2 (Network and Information Security Directive)

What? The NIS2 directive aims to improve the cybersecurity of networks and information systems in the EU.

Who? Operators of essential services and digital service providers.

When?

- 2024: Expected to come into force;
- 2025: Compliance requirements start.

Penalties: Non-compliance can result in fines up to €10 million or 2% of the company's total worldwide turnover.

Steps to Ensure Compliance:

- Implement robust cybersecurity measures for networks and information systems;
- Conduct regular risk assessments and vulnerability scans;
- Establish incident response plans and reporting mechanisms;
- Ensure continuous monitoring and improvement of security practices;
- Train staff on cybersecurity protocols.

"Machines" Directive

What? This directive establishes safety requirements for the design and manufacture of machines.

Who? Manufacturers of machines and importers.

When?

- 2006: In force since;
- Periodic: Revisions to update safety requirements.

Penalties: Non-compliance can lead to fines and product recalls, with specific amounts varying by member state.

Steps to Ensure Compliance:

- Design and manufacture machines according to safety requirements;
- Conduct conformity assessments and obtain necessary certifications;
- Maintain technical documentation and compliance records;
- Regularly update and maintain machines to ensure ongoing compliance;
- Train staff on safety standards, and follow the norm project EN 50742, entitled “Protection against corruption”.

We list and analyse some regulations related to automotive markey, namely UN ECE R155, R156 and ISO/SAE 21434.

UN Regulation No. 155 (UN R155) – Cybersecurity Management System (CSMS)

A. **What?**

UN Regulation No. 155 mandates that vehicle manufacturers establish and maintain a Cybersecurity Management System (CSMS). This system must address the identification, assessment, and mitigation of risks resulting from threats, vulnerabilities, and attacks targeting vehicles and their connected infrastructure. The regulation provides a structured threat catalog (e.g., backend servers, communications, data integrity, insider threats) and matches each threat with mitigation measures and documentation requirements.

B. Who?

- Vehicle manufacturers and their accredited representatives
- Suppliers, service providers, the whole automotive supply chain
- Type approval authorities in contracting countries

C. When?

- Applies to all new vehicle types submitted for approval since July 2022 in signatory countries.
- CSMS certificate renewal is required every 3 years, unless revoked earlier for non-compliance.
- Requirements must be met:
    - During the design phase (risk analysis, mitigation selection)
    - Prior to initial type approval and when updating evaluation methods
    - Throughout the vehicle lifecycle (documentation, continuous threat analysis, etc.)

D. Penalties:

- Refusal or withdrawal of type approval for the affected vehicle type
- Revocation of the CSMS certificate in case of non-compliance
- Notification shared among other contracting states via the DETA database
- Commercial impact: vehicles cannot be placed on the market; potential recall or sales block

E. Steps to ensure compliance

1. Prepare comprehensive CSMS documentation, detailing processes, roles, and controls
2. Conduct systematic risk analyses covering threats from Part A, mitigations from Parts B and C
3. Implement processes for threat detection, prevention, response, and recovery
4. Obtain and maintain the CSMS certificate via audits and continuous improvement
5. Update authorities on major changes, maintain traceability, renew certificates as required
6. Record all key actions and processes and ensure accessibility in the DETA database

UN Regulation No. 156 (UN R156) – Software Update Management System (SUMS)

A. What?

UN Regulation No. 156 outlines requirements for secure software update processes in vehicles. It mandates traceability for each update, documentation of impacts on approved systems, validation of software/hardware configurations, and authorities' access to update information.

B. Who?

- Vehicle manufacturers and their accredited representatives
- Embedded systems suppliers affected by updates
- Type approval authorities overseeing SUMS compliance

C. When?

- Applies to new vehicle types seeking approval in countries adopting the regulation, as per each jurisdiction's schedule.
- Requirements must be met:
    - When designing embedded software architectures
    - At every update cycle (deployment, verification, validation, documentation)
    - During technical inspections and post-approval surveillance

D. Penalties:

- Refusal or withdrawal of type approval for failure to comply
- SUMS certificate revocation
- Mandatory notifications and updates to approvals in the DETA database
- Commercial impact: unable to deploy updates, market access blocked, recall risk

E. Steps to Ensure Compliance

1. Document the SUMS, specifying traceability, compatibility, and information flow requirements
2. Establish and maintain procedures for impact analysis, version identification, and configuration records before and after updates
3. Maintain up-to-date RXSWIN registry (software identification numbers) and affected components
4. Demonstrate and validate the security of each update (integrity, authenticity, robust testing)
5. Obtain and regularly renew SUMS certificate (at least every 3 years)
6. Make update records available to authorities as requested for audits, investigations, or recalls.

ISO/SAE 21434 – Road Vehicles Cybersecurity Engineering

A. What?

International standard specifying cybersecurity requirements throughout the lifecycle of road vehicle embedded systems. Covers risk management, vulnerability handling, measure documentation, and cybersecurity governance.

B. Who?

- Vehicle manufacturers and suppliers
- Subcontractors involved in hardware/software design and development
- Cybersecurity auditors and consultants

C. When?

- Applies throughout the component lifecycle: design, development, production, operation, maintenance, end-of-life
- Must be updated following major system changes or internal/external audits

D. Penalties

- Non-compliance identified in audits
- Loss of third-party certification, possible loss of type approval if ISO/SAE 21434 is referenced by regulators
- Commercial risks: contract exclusion, failed RFQs, lost partnerships

E. Steps to Ensure Compliance

1. Establish documented cybersecurity governance (policies, roles, responsibilities, periodic reviews)
2. Systematic risk analysis and assessment for embedded components and interfaces
3. Implement and document technical and organizational cybersecurity measures
4. Ensure incident and mitigation traceability over the entire product lifecycle
5. Organize internal or external audits and follow improvement plans

DORA, DMA, DSA are other cybersecurity regulations, presented hereafter. They primarily apply to operators, but have some impacts with the endpoints. Hence, having some awareness about them can be beneficial even in the context of embedded systems.

DORA (Digital Operational Resilience Act)

What? DORA aims to enhance the digital operational resilience of financial institutions.
Who? Financial institutions and ICT service providers.
When?

- 2024: Expected to come into force.
- 2025: Compliance requirements start.

Penalties: Non-compliance can result in fines up to 2% of the company's total worldwide turnover. Critical third parties could be fined up to €5 million, and individuals can face fines up to €1 million.

Steps to Ensure Compliance:

- Implement strong IT security measures for financial institutions.
- Conduct regular resilience testing and assessments.
- Establish incident response plans and reporting mechanisms.
- Ensure continuous monitoring and improvement of security practices.
- Train staff on operational resilience protocols.

Digital Market Act (DMA)

What? This regulation aims at preventing anti-competitive practices of the digital giants and correcting the imbalances of their domination on the European digital market.

Who? The “gatekeepers”. The European Commission has published a list of companies that should be considered as such (Alphabet Inc., Amazon.com Inc., Apple Inc., Booking, ByteDance Ltd., Meta Platforms, Inc., Microsoft Corporation).

When? In force since May 2nd, 2023 and fully in force since March 6th, 2024.

Penalties:

In the event of non-compliance, penalties up to 10% of total worldwide annual turnover (20% in the event of a repeat offence).

In the event of a repeat offence, a ban on buyouts/acquisitions of digital companies, or even the dismantling of their activities.

Digital Services Act

What? The objective of this regulation is to combat online misinformation and illegal content and to strengthen platforms’ transparency and accountability.

Who? All online intermediaries offering their services, including internet service providers, cloud service providers, online platforms. Specific obligations for very large online platforms (17) and very large online search engine (2).

When? In force since August 25th, 2023.

Penalties:

- Penalties up to 6% of total worldwide annual turnover;

- In the event of a repeat offence, those may be banned from doing business within the European Union.

How our Solutions Respond to Compliance?

We provide comprehensive solutions designed to help you meet regulatory compliance requirements efficiently and effectively. Our offerings include:

- Risk Assessments: Identify and mitigate potential risks to ensure compliance;
- Security Implementations: Deploy robust security measures tailored to your needs;
- Continuous Monitoring: Keep track of compliance status and address issues promptly;
- Training Programs: Educate your staff on compliance requirements and best practices.

Your Compliance, Through Cybersecurity Journey

We support your compliance journey at every stage:

1. Assessment: Evaluate your current compliance status and identify gaps;
2. Implementation: Deploy necessary security measures and controls;
3. Monitoring: Continuously monitor compliance and address emerging threats;
4. Review: Regularly review and update compliance measures to stay aligned with regulations.

Certification is One Way

Achieving certification is a key step in demonstrating compliance. For example:

- EUCC (European **C**ybersecurity **C**ertification): Part of the EU CRA, leveraging Common Criteria to certify the security of digital products. – Publication of a *vade mecum* Feb 18, 2025;
- ISO/IEC 27001: International standard for information security management systems.

Technology is Another

Leveraging advanced technology can also ensure compliance:

- AI and Machine Learning: Automate compliance monitoring and threat detection;
- Blockchain: Ensure data integrity and transparency;
- Cloud Security: Secure cloud environments to meet regulatory requirements.

Providing the Means for Compliance

We offer the tools and expertise to help the concerned actors (manufacturers, importers, distributors, developers, users, financial institutions, etc.) comply with regulations:

- Customized Solutions: Tailored to meet specific regulatory requirements;
- Expert Guidance: From initial assessment to full compliance;

- Ongoing Support: Continuous assistance to maintain compliance.

What should I do?

1. Start a security analysis of your organisation and software;
2. If possible, find a company to accompany you through the audit;
3. Write down all observations to build the necessary documentation.

Takeaways:

- Hopefully, the complexity of regulations and induced norms has been clarified;
- Some elements of compliance have been presented;
- There are local & engaged actors to accompany you.

Call for Action

- Organize your organization to be cybersecure and to comply to EU regulation;
- Adopt our methodology, which allows you to walk step-by-step in the compliance journey;
- Consider joining Embedded France association to benefit & share your expertise!

The authors of this white paper are affiliated with the following Embedded France members. Besides, the French cybersecurity agency (ANSSI) contributed some insights and participated to the preparatory meetings.

CAP'TRO
Capgemini
ESIEE PARIS
MathWorks
AMPERE
cetrac
GRENOBLE INP UGA Esisar VALENCE
MOABI
PROVENRUN
Quantyss
SCIENSYS
SYSGO EMBEDDING INNOVATIONS
TRUST IN SOFT
VIVERIS
SAFRAN AEROSPACE·DEFENCE·SECURITY
SECURE-IC THE SECURITY SCIENCE COMPANY
THALES
We are CYBER

Embedded France
L'EMBARQUÉ MADE IN FRANCE