die
RESILIENZ GmbH

CRA Compliance: Painless

Declarations of Conformity—seamlessly integrated into your processes.

YOUR GUIDANCE TO COMPLIANCE

Empowering Your Cyber & Business Resilience

- UPCOMING CRA REQUIREMENTS DEMAND EVIDENCE, NOT JUST POLICIES
- THE COST OF DELAY GROWS QUICKLY (REWORK, AUDITS, SUPPLIER PRESSURE)
- STAY COMPETITIVE: CUSTOMERS EXPECT SECURITY AND COMPLIANCE BY DESIGN

At die RESILIENZ GmbH, we help organizations navigate the EU Cyber Resilience Act (CRA) and related European regulatory frameworks with confidence—using proven processes that significantly reduce compliance effort and risk.

NON-COMPLIANCE CAN PUT YOUR BUSINESS AT RISK

The **CRA** affects **product security**, **processes**, **reporting**, and **documentation**—and **violations** can result in **fines, sanctions**, and long-term legal exposure.

€ Up to €15M or 2.5% of turnover

Breach of essential cybersecurity requirements (**Annex I**) and core obligations (Arts. 13–14).

€ Up to €10M or 2% of turnover

Breach of key operational/compliance obligations (Arts. 18–23, 28, 30–33, 39, 41, 47, 49, 53).

€ Up to €5M or 1% of turnover

Providing incorrect, incomplete, or misleading information to notified bodies or market authorities.

CE Loss of CE marking / EU market ban

Sales bans, recalls, and potential EU-wide restrictions with major reputational damage.

DON'T WAIT UNTIL IT'S TOO LATE

Deadlines are fixed—act now to avoid costly rework and penalties.

9/11/26
Vulnerability reporting
must be in place

12/11/27
CE Marking, User Docs, Essential
Requirements & SSDLC

Cyber Resilience Act (CRA)

We support you end-to-end in achieving CRA readiness—from portfolio assessment to secure-by-design implementation. You get clear evidence and documentation to meet regulatory requirements without slowing down development.

CE Compliance

We set up CE workflows that connect technical documentation, test evidence, and declarations. The result is a traceable, audit-ready CE process integrated into your product lifecycle.

Process Management

We make your Secure Software Development Lifecycle (SSDLC) practical and easy to operate. We close gaps and embed security and compliance into your existing QMS and day-to-day routines.

Software Compliance

We make your Secure Software Development Lifecycle (SSDLC) practical and easy to run. We close gaps and integrate security/compliance into your existing QMS and daily routines.

New Product Development

We help you build new products with security by design from day one. With reviews and automation (tests + documentation), you ship secure, CRA-ready products faster.

Refit / Retrofit

We secure legacy systems without costly redevelopment. By isolating and hardening software in controlled environments (VMs and containers), you keep operations running while moving toward CRA compliance.

Willy-Brandt-Platz 2
12529 Schönefeld, Brandenburg

☎ +49 173-2038076

resilienz.gmbh

✉ anfrage@resilienz.gmbh

die
RESILIENZ GmbH

CRA Compliance: Painless

Declarations of Conformity—seamlessly integrated into your processes.

GAP ANALYSIS

Your development processes for products with digital elements

From **€ 20K**

Depending on your product's complexity

- ✓ Inventory: Delta for a secure development process according to standards
- ✓ Highlighting standards of good practice
- ✓ Report with action points

IMPLEMENTATION

Achieving CRA compliance for your products with digital elements

From **€ 70K**

Through coaching or via our team

- ✓ Retrofit of existing products
- ✓ Complete reimplementation
- ✓ Securing the development process (supply chain, SBOM, vulnerability, update, and incident management)

AUDITING

Validation of established development processes by an auditing body

From **€ 30K**

Depends on the auditor and the market situation.

- ✓ Through established institutions
- ✓ e.g., aligned with IEC 62443-4-1, BSI TR-03183, ISO 27001/ISO 27005, or ISO 33001 (risk management)
- ✓ Prove CRA compliance

GAP ANALYSIS (CRA Readiness)

- ✓ **Objective:** Provide management clarity on readiness, risk, and required investment.
- ✓ **Scope:** Portfolio, governance, SSDLC, documentation, and reporting obligations.
- ✓ **Current-state review:** Processes, roles, tooling, and existing compliance evidence.
- ✓ **Gap identification:** What's missing against CRA essential requirements and key operational duties.
- ✓ **Risk & impact view:** Market access, delivery delays, rework costs, and audit exposure.
- ✓ **Prioritization:** Quick wins vs. structural changes—what to do first.

Turning **SSDLC** from theory into practice

SSDLC is a continuous approach that integrates security into every phase of software development. Each phase produces documented, verifiable security deliverables for CRA compliance, aligned with IEC 62443-4-1 and ISO/IEC 27002, and structured as a four-step cycle.

- ✓ Requirements analysis and threat modeling
- ✓ Secure design and architecture
- ✓ Secure implementation and integration
- ✓ Verification, validation, and handover to operations

OUR PRODUCTS/SERVICES:

- ✓ Secure coding
- ✓ Process management for SSDLC
- ✓ Technical and customer documentation support
- ✓ Gap analyses (process-level assessments)
- ✓ Technical investigations (security verification and validation)
- ✓ Academy (coaching and training)
- ✓ Certification and conformity assessment
- ✓ Project management for CRA readiness
- ✓ Procurement support for compliant products
- ✓ User training and enablement
- ✓ Third-party distribution and specialist referral
- ✓ Controls in the development environment (technical and organizational)
- ✓ Communication processes with customers and regulators

Willy-Brandt-Platz 2
12529 Schönefeld, Brandenburg

☎ +49 173-2038076

resilienz.gmbh

✉ anfrage@resilienz.gmbh