OPEX®

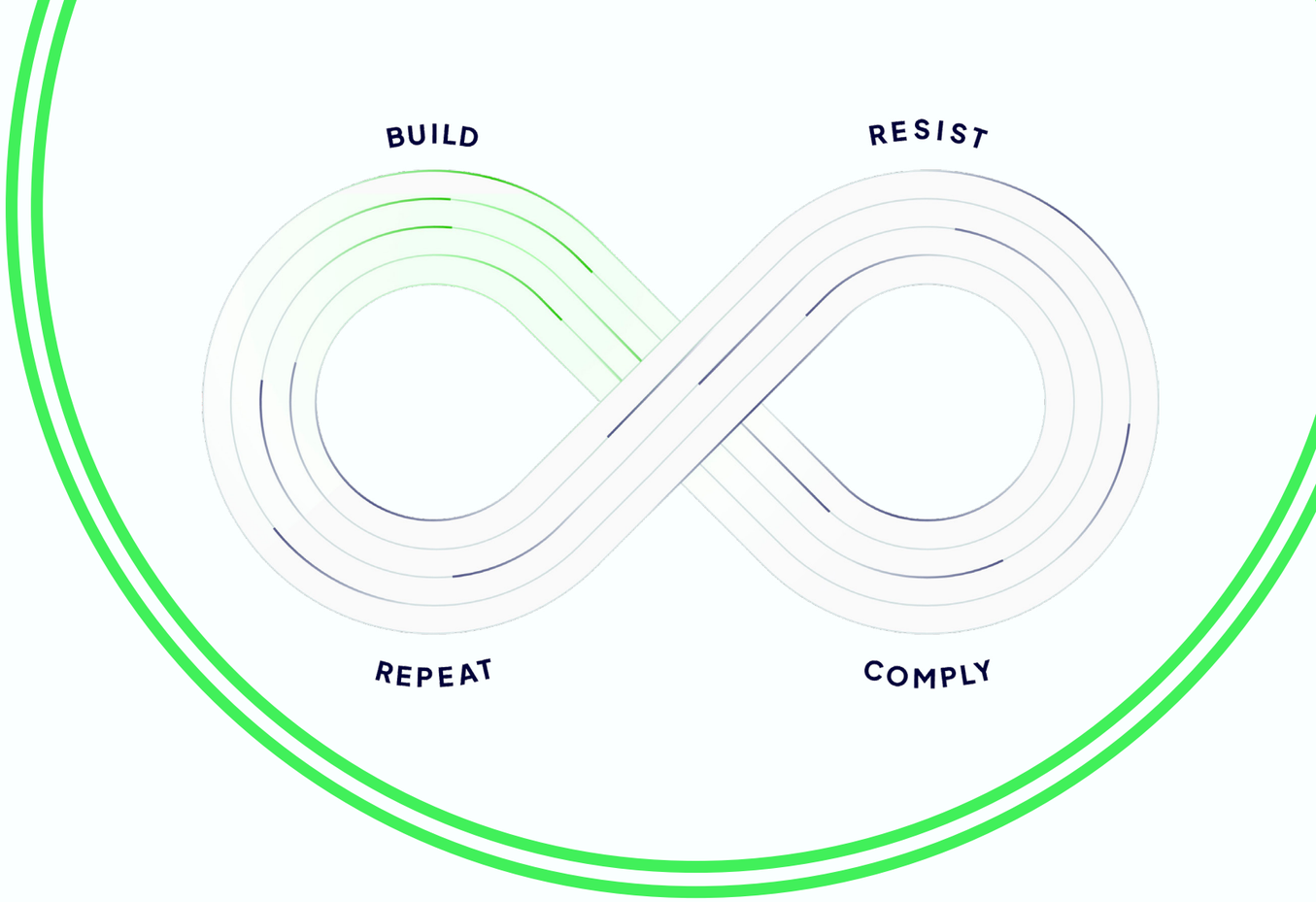
A SUCCESS STORY

HOW OPEX ACHIEVED CRA READINESS

Through ONEKEY's Structured Expert Assessment

ONEKEY

STRENGTHENING DESIGN ENGINEERING PR◎CESSES WITH CLARITY, CONFIDENCE, AND D◎CUMENTED ASSURANCE



Executive Summary

OPEX Corporation worked with ONEKEY to validate the CRA readiness of its Design Engineering organization. Through a structured, standards-based assessment aligned with IEC 62443-4-1 and ISO 19011, ONEKEY confirmed CRA alignment, clarified responsibility boundaries, and identified targeted improvement areas. The outcome provides OPEX with documented assurance, confidence, and a strong foundation for efficient company-wide CRA compliance.

Background

OPEX Corporation is one of the leading automation and manufacturing companies, founded in 1975 and headquartered in Moorestown, New Jersey, USA. The company operates globally with installations across multiple continents and a dedicated European hub in Duisburg, Germany.

OPEX is recognized for its innovative engineering and strong industry expertise, supported by a global workforce of more than 1,600 employees.

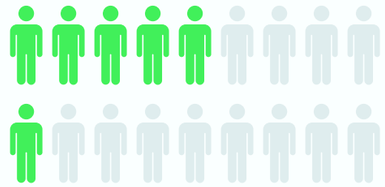
Its core products and service offerings include warehouse automation systems, document and mail automation technologies, high-speed scanning solutions, sortation equipment, and comprehensive fulfillment infrastructure.

As OPEX prepared its Design Engineering unit for the upcoming Cyber Resilience Act, the company sought expert support to confirm that its secure development processes, already established under IEC 62443-4-1, would meet the new regulatory expectations.

The Challenge: Clarifying CRA Obligations within the Engineering Domain

At the start of the project, OPEX was preparing for the upcoming requirements of the European Cyber Resilience Act (CRA). While the company had already implemented secure development practices based on IEC 62443-4-1, it was unclear whether the existing processes within the Design Engineering department would sufficiently meet CRA obligations, especially in areas such as SBOM transparency, vulnerability management, and secure update mechanisms.

Additionally, OPEX sought internal clarity and validation: could their Design Engineering team confidently demonstrate that it had fulfilled its CRA-related responsibilities? The goal was to provide internal management with well-founded confirmation, while also identifying any technical or organizational gaps that would require cross-functional follow-up.



68% of companies are not familiar with the requirements of the CRA.*

4% of companies have already taken comprehensive measures.*

* https://www.onekey.com/resource/iot-ot-cybersecurity-report-2025

Collaboration

The collaboration between OPEX and ONEKEY was characterized by transparency, professionalism and technical depth. The Design Engineering team at OPEX proactively shared detailed documentation, provided clarifications on process maturity and responded constructively to review feedback.

Throughout the engagement, both sides maintained close communication via frequent coordination calls, structured document exchanges, and validation reviews. This enabled a precise scoping of CRA-relevant responsibilities and ensured that the expert opinion was not only technically accurate but also operationally meaningful for internal stakeholders.

By focusing the analysis on the engineering domain, the project made it possible to isolate completed compliance elements from broader organizational topics, setting a clear boundary between what had already been delivered and what remains to be addressed in cross-functional teams.

The Solution: Structured CRA Readiness Assessment by ONEKEY

To assess CRA readiness within the Design Engineering scope, ONEKEY conducted a structured expert review, building on the secure development processes already established under IEC 62443-4-1. The approach included:

- A document-based evaluation of development policies, security controls, update mechanisms, and vulnerability handling processes
- A detailed mapping of CRA requirements against the existing IEC 62443-4-1 implementation
- Integration of new technical documentation provided by OPEX, covering SBOM automation, vulnerability scan routines, and update signing procedures

The review strictly followed the principles of ISO 19011 to ensure objectivity, traceability, and reproducibility of the findings.

IEC 62443-4-1 Foundation

⌄

ONEKEY Technical Review

⌄

CRA Requirements Mapping

⌄

Implementation of CRA Measures

⌄

Documented CRA Alignment

OPEX CORPORATION: BENEFITS OF USING ONEKEY

Validation with Structure and Depth

The assessment provided a clear mapping of OPEX's existing engineering practices against CRA obligations, giving the team a structured view of their current maturity.

Clarity and Confidence

OPEX Design Engineering received formal confirmation letters documenting CRA alignment, enabling the team to confidently demonstrate that its responsibilities had been fulfilled.

Targeted Improvement

Rather than generating a generic checklist, ONEKEY identified specific improvement areas such as lifecycle documentation, vulnerability reporting, and audit readiness.

Strategic Alignment

The outcome helped OPEX define responsibility boundaries and set the stage for company-wide CRA initiatives.

Efficiency and Direction

By leveraging IEC 62443-4-1 and focusing on only relevant CRA articles, unnecessary work was avoided and efforts were directed toward impactful enhancements.

WHY OPEX CORPORATION CHOSE ONEKEY

The main reason OPEX Corporation chose ONEKEY was its collaborative approach that was characterized by transparency, professionalism, and technical depth. ONEKEY provided a structured expert assessment rooted in recognized standards such as IEC 62443-4-1 and ISO 19011, ensuring objective, reproducible results tailored to CRA expectations.

„With ONEKEY's guidance, we were able to confirm that our Design Engineering team meets the expectations of the Cyber Resilience Act. Their structured assessment gave us the clarity we needed —both to validate our existing practices and to define what needs to happen next. It was a very good experience throughout, especially in aligning our efforts with the CRA and IEC 62443. We truly appreciate the collaboration."

— Nenad Vujovic, Director of DMA Design Engineering, OPEX Corporation

CONCLUSION

ONEKEY enabled OPEX Corporation to move from a technically mature but fragmented state to a documented, structured, and strategically aligned position regarding CRA readiness. With validated evidence, improved clarity, and clearly defined next steps, the Design Engineering department is well-prepared to support broader CRA compliance across the company.

Beyond confirming regulatory alignment, the assessment provided OPEX with a reliable foundation for proof-based internal and external communication. Clear responsibility boundaries and documented outcomes allow the organization to demonstrate compliance with confidence while avoiding unnecessary effort. By focusing on relevant CRA requirements and building on existing IEC 62443-4-1 practices, ONEKEY helped OPEX translate technical maturity into measurable, auditable assurance—supporting long-term compliance, operational efficiency, and strategic readiness for future regulatory demands.

ABOUT ONEKEY

ONEKEY is the leading European specialist in Product Cybersecurity & Compliance Management and part of the investment portfolio of PricewaterhouseCoopers Germany (PwC). The unique combination of the automated ONEKEY Product Cybersecurity & Compliance Platform (OCP) with expert knowledge and consulting services provides fast and comprehensive analysis, support, and management to improve product cybersecurity and compliance from product purchasing, design, development, production to end-of-life.

Critical vulnerabilities and compliance violations in device firmware are automatically identified in binary code by AI-based technology in minutes – without source code, device, or network access. Proactively audit software supply chains with integrated Software Bills of Materials (SBOMs) generation. “Digital Cyber Twins” enable automated 24/7 post-release cybersecurity monitoring throughout the product lifecycle.

The patent-pending, integrated ONEKEY Compliance Wizard already covers the EU Cyber Resilience Act (CRA) and requirements according to IEC 62443-4-2, ETSI EN 303 645, UNECE R 155 and many others.

The Product Security Incident Response Team (PSIRT) is effectively supported by the integrated automatic prioritisation of vulnerabilities, significantly reducing the time to remediation.

Leading international companies in Asia, Europe and the Americas already benefit from the ONEKEY Product Cybersecurity & Compliance Platform (OCP) and ONEKEY Cybersecurity Experts.

ONEKEY
onekey.com
+49 211 1587 41 04
info@onekey.com

SecurITy made in Germany

V20251001EN