

Security for the systems that **must not fail**.

Nord CS helps companies build, verify and prove the cybersecurity of their products, systems and organizations, **from the first risk assessment to the final compliance evidence**.

WHERE WE CAN HELP

FOUR SITUATIONS WE SOLVE EVERY DAY

01

A product must ship compliant

CRA, ISO/SAE 21434, IEC 62443 or DO-326A applies. The deadline is fixed.

02

An audit is coming

TISAX, ISO 27001 or NIS2 is ahead. The evidence still has gaps.

03

Security work eats engineering time

Threat analyses, risk assessments and documentation take weeks per product.

04

You are starting something new

A new product, platform or plant. Security must be designed in from day one.

01 · CONSULTING

Cybersecurity Consulting



Our experts take your product, system or organization through the **complete cybersecurity lifecycle**, for OT, automotive, medical, IT, avionics and space projects.

RISK ASSESSMENT → REQUIREMENTS → IMPLEMENTATION → VERIFICATION → COMPLIANCE

- **Audits & gap analyses:** cybersecurity audits, internal audits and gap analyses.
- **Risk & compliance assessments:** from product risk analysis to compliance readiness.
- **Training:** OT, automotive, IT, avionics and space security, secure product development, risk management.

STANDARDS & REGULATIONS WE COVER

- IEC 62443
- CRA
- ISO/SAE 21434
- ISO 27001
- TISAX
- NIS2
- FDA §524B
- DO-326A / ED-202A
- DO-356A / ED-203A
- DO-355 / ED-204A
- ECSS / ESA

02 · SOFTWARE

AITIGRITY



Our platform manages the **complete cybersecurity development lifecycle** for OT, automotive, medical, avionics and space products, including **continuous vulnerability monitoring** across the product lifetime.

WHAT IT MANAGES

- ASSETS
- THREAT ANALYSIS
- RISK ASSESSMENT
- REQUIREMENTS
- SECURITY MEASURES
- VERIFICATION
- COMPLIANCE EVIDENCE
- TRACEABILITY
- VULNERABILITY MONITORING

Less manual effort

Automates the structured work your standards demand.

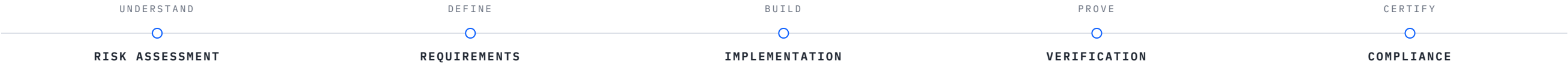
Full traceability

Every requirement, measure and evidence item stays connected.

Faster compliance

Audit-ready evidence as you work, not rebuilt at the end.

Cybersecurity Consulting



A report does not make a product compliant. The work does. Our senior engineers take your product through the **complete cybersecurity lifecycle** and leave your team with evidence an assessor accepts and artifacts you own.

IN FOCUS · EU CYBER RESILIENCE ACT · REGULATION (EU) 2024/2847

CRA readiness, engineered.

The CRA is not a reporting exercise. It is an evidence chain across your whole development lifecycle: risk assessment, the Annex I requirements, SBOM, technical documentation, a working vulnerability handling process, CE conformity. **We build these artifacts with your team, and our AITIGRITY platform keeps them current across the entire support period.** That is work a slide deck cannot do.

11 SEP 2026

Vulnerability and incident reporting obligations apply

11 DEC 2027

All main obligations apply for products on the EU market

CRA READINESS ASSESSMENT, FIXED SCOPE: product classification · Annex I gap analysis with a prioritized roadmap · SBOM and technical documentation plan · vulnerability handling and reporting runbook

The gaps that sink CRA projects: an SBOM nobody owns, a disclosure policy with no reporting path, an ISO certificate that never covered the firmware. We close exactly these.

WHEN A PRODUCT MUST SHIP

Lifecycle engineering

TARA, security requirements, implementation support, verification, compliance case. **One team inside your process and your tools**, start to finish.



WHEN AN AUDIT IS AHEAD

Gap analysis & audits

Gap analysis against your target standard, audits, risk and compliance assessments. **Findings you can act on** and a roadmap you can defend.



WHEN CAPACITY IS THE PROBLEM

Experts & training

Security engineers who join your team, **for a sprint or for a year**. Training that keeps the knowledge in house, hands-on, standard by standard.



STANDARDS & REGULATIONS BY DOMAIN

AUTOMOTIVE

ISO/SAE 21434 UN R155 / R156 TISAX

INDUSTRIAL & OT

IEC 62443 CRA

IT & ORGANIZATION

ISO 27001 NIS2

MEDICAL

FDA §524B EU MDR / MDCG 2019-16

AVIONICS

D0-326A / ED-202A D0-356A / ED-203A D0-355 / ED-204A

SPACE

ECSS ESA CYBERSECURITY REQUIREMENTS

AITIGRITY

Secure Your Product. Accelerate Your Development.

An integrated product cybersecurity engineering toolchain — from Secure by Design to continuous security throughout the entire product lifecycle.

Less Complexity. More Control.



SECURE BY DESIGN



END-TO-END TRACEABILITY



COMPLIANCE EVIDENCE



CONTINUOUS CYBERSECURITY

One integrated approach to secure products and faster compliance.

3–4 PM

What a 24-month programme becomes

100%

Audit-ready at every point

0

Rebuilds after release

One Toolchain. Full Cybersecurity Lifecycle.



Threat & Risk Analysis

Identify and assess cybersecurity threats and risks.



Security Requirements

Define and manage actionable security requirements.



Security Architecture

Build security into product architecture from the start.



Verification & Testing

Verify security measures and generate traceable evidence.



Vulnerability Management

Identify, assess, and manage vulnerabilities throughout the product lifecycle.



Continuous Monitoring

Maintain product security beyond release.

CRA Ready. Beyond CRA.

AITIGRITY structures and manages the cybersecurity engineering activities needed to support CRA compliance — from risk assessment and Secure by Design to verification, compliance evidence, and vulnerability management.

Beyond CRA, AITIGRITY supports cybersecurity engineering across industries, regulations, and standards:

EU CRA

ISO/SAE 21434

UNECE R155/R156

IEC 62443

EU MDR

FDA Cybersecurity

D0-326A/ED-202A

ECSS

From Risk to Compliance.

RISK → REQUIREMENTS → ARCHITECTURE → VERIFICATION → EVIDENCE → COMPLIANCE

One connected and traceable cybersecurity process — from the first identified risk to compliance evidence.

Let's secure the future together.

contact@nordcs.de
nordcs.de · aitigrity.com