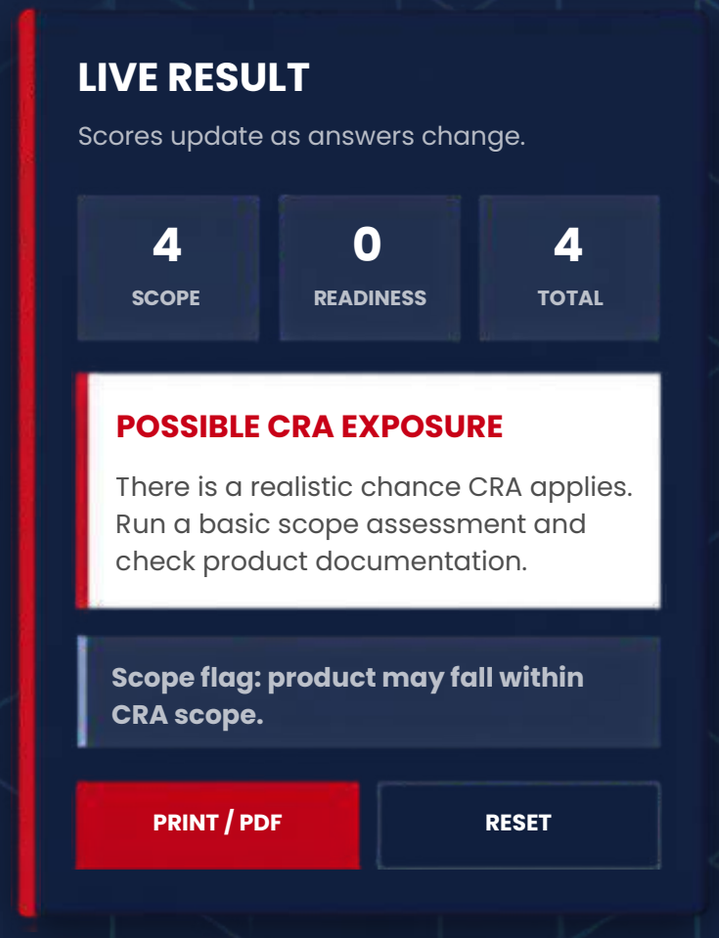
# CRA Diagnostic Test

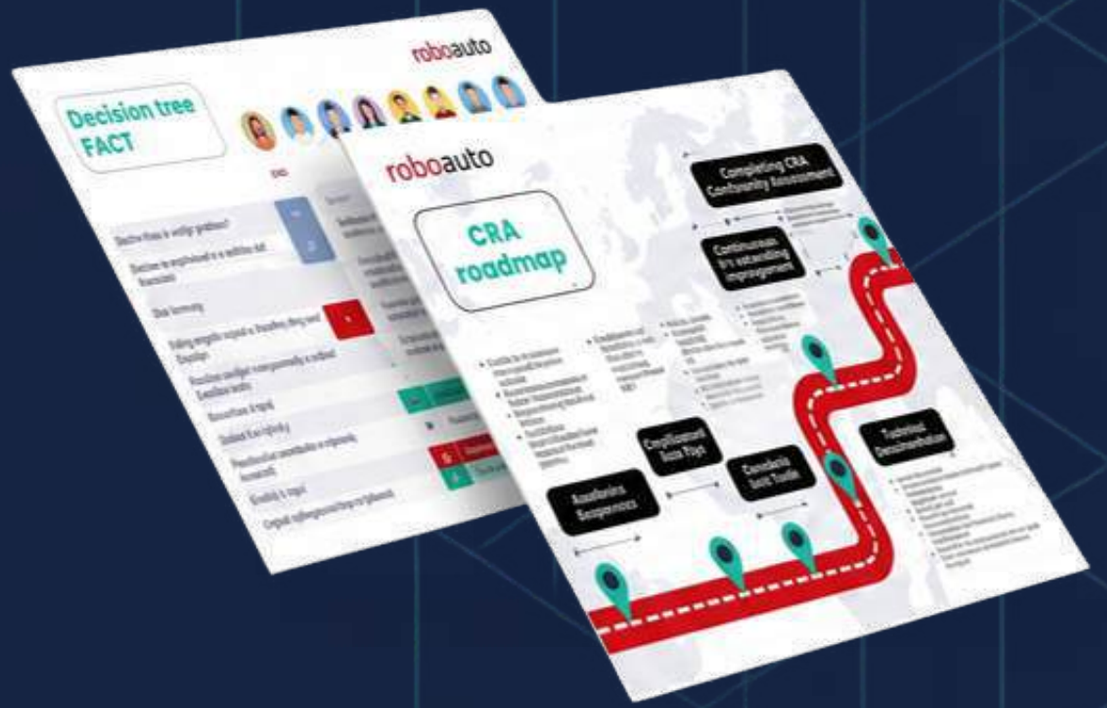
Interactive self-assessment for product scope, readiness gaps, and practical next-step urgency.

Quickly identify whether CRA is likely to affect afect your product and where the first risk questions sit.

**Start the diagnostic test now**



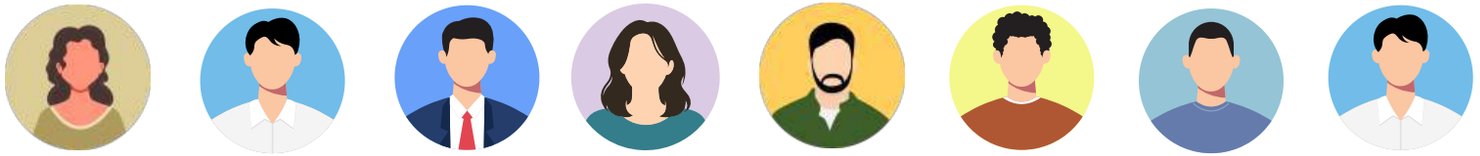
# Decision Tree Framework




Clarify scope and ownership before CRA turns into a management or R&D bottleneck.

Implementing a RACI matrix establishes clear cross-departmental accountability defining exactly who is **R**esponsible for execution, **A**ccountable for compliance, **C**onsulted on technical decisions, and **I**nformed of progress.

roboauto



| | CEO | CSO | CTO | Head of engineering | Product Manager | Developer | Product Security Lead | Tech Lead |
|---|---|---|---|---|---|---|---|---|
| Define roles for each product | A | | I | | C | | R | |
| Milestone mapping: 11/09/2026 and 11/12/2027 | A | C | I | | | | R | |
| PDE Catalog | | | | | R | | A | C |
| Annex classification& Criticality Class per Product | I | | | | R | | C | A |
| Version change management vs. impact on conformity | | | A | | C | | I | R |
| Security by design | | | A + I | | | C | | R |
| Secure-by-default | | C | | | I | R | | A |
| Technical documentation of security measures | | | | I | | R | C | A |
| Security in SDLC | | I | | A | | R | | C |
| Crypto management (keys & libraries) | | C | A | | | I | | R |

roboauto

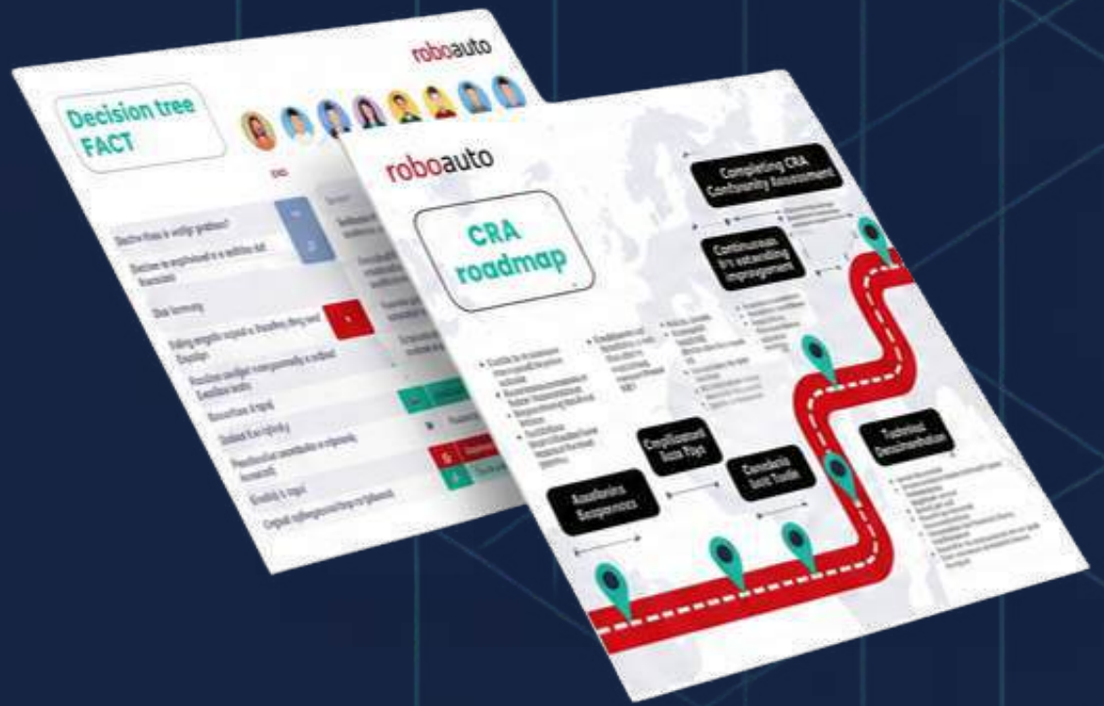
| | CEO | CSO | CTO | Head of engineering | Product Manager | Developer | Product Security Lead | Tech Lead |
|---|---|---|---|---|---|---|---|---|
| FW/OS hardening | | I | C | | | R | | A |
| VDP/CVD policy (intake, triage, SLAs) | | R | | | I | | A | C |
| Secure updates | | I | C | | | R | | A |
| Reporting of significant vulnerabilities/incidents | A | R | | | | | C | |
| Technical documentation (Annex I) – complete and up-to-date | | | | A | I | | R | C |
| EU declaration of conformity & CE marking | A | | | | I | | R | C |
| Conformity assessment process | A | | I | | | | R | C |
| Importer verification (CE, docs, traceability) | | I | A | | C | | R | |
| Distributor verification (labels, instructions, safety info) | | I | A | | C | | R | |
| Collection of operational and security data | | A | | | | R | I | C |

roboauto

| | CEO | CSO | CTO | Head of engineering | Product Manager | Developer | Product Security Lead | Tech Lead |
|---|---|---|---|---|---|---|---|---|
| Corrective Measures Market Withdrawal | A | R | | | | | C | |
| Component inventory (SBOM / VEX) | | | | | I | R | C | A |
| Contractual requirements for suppliers (patching, reporting, documentation) | A | | | | I | | R | C |
| Build provenance & artifact signing | | | I | C | | R | | A |
| Assign the Program Owner (Product Security Lead) | R + A | | C | | | | | |
| Training | | I | | A | | | R | C |
| Management reporting (compliance status, risks, resources) | I | | A | | C | | R | |
| Gap Analysis against CRA Annex I | | C | I | | | | R | A |
| Evidence packages per product | | | | | I | C | R | A |

# CRA Roadmap

Translate the compliance question into a practical sequence of decisions, dependencies, and workstreams.



roboauto

## Readiness Assessment

- Drafting CRA essential requirements for your product
- Assign the program owner (Product security lead)
- Gap analysis against CRA Annex I
- PDE Catalog
- Annex classification & Criticality class per product

## Implementation Plan

- Mapping the 11.9. 2026 and 11.12. 2027 milestones = creating the implementation plan

## Reporting (11.9. 2026)

- VDP/CVD policy
- Reporting of significant vulnerabilities/incidents
- Define roles for each product
- Component inventory
- Corrective measures / Market withdrawal

## Organizational and Procedural Implementation

- Importer verification
- Distributor verification
- Contractual requirements for suppliers
- Training

## Technical Implementation

- Security by design
- Version change management vs. impact on conformity
- Secure-by-default
- Security in SDLC
- Crypto management
- FW/OS hardening
- Build provenance & artifact signing
- Secure updates
- Collection of operational and security data
- Technical documentation of security measures

## Completing CRA Conformity Assessment

- Conformity assessment process
- Technical documentation (Annex I) – complete and up-to-date
- Evidence packages per product
- EU declaration of conformity & CE marking
- Management reporting

# CRA Checklist

Turn high-level CRA obligations into concrete items your team can review and assign.

# CRA COMPLIANCE CHECKLIST

## 1. CHECKLIST GUIDE

| FOCUS AREA | EXPLANATION |
|---|---|
| **Requirement / Verification** | Specific audit point (verifiable) |
| **Risk of non-compliance** | Business impact scenario |
| **Explanation (What &Why)** | Purpose, scope & strategic rationale |
| **Definition of Done** | Success criteria (clear & measurable) |
| **Evidence / Artifact** | Objective proof (logs, records, files) |
| **Critical Focus Areas** | Common pitfalls & blind spots |

## 2. MAIN CHECKLIST

**Scope & Timeline**

| REQUIREMENT / VERIFICATION | RISK OF NON-COMPLIANCE | EXPLANATION (WHAT & WHY) | DEFINITION OF DONE | EVIDENCE / ARTIFACT | CRITICAL FOCUS AREAS |
|---|---|---|---|---|---|
| Define roles for each product (Manufacturer / Importer / Distributor / AR) | Medium | Obligations vary by role in the supply chain. | RACI assigned per SKU, management-approved | RACI matrix; board meeting minutes | Roles conflict & missing RACI |
| Milestone mapping: Sep '26 (Reporting) & Dec '27 (main obligations) | Medium | Required resource and budget planning | Approved roadmap with owners and budget | Roadmap; project plan; budget framework | Supplier dependencies. |

## Asset Inventory & Classification

| REQUIREMENT / VERIFICATION | RISK OF NON-COMPLIANCE | EXPLANATION (WHAT & WHY) | DEFINITION OF DONE | EVIDENCE / ARTIFACT | CRITICAL FOCUS AREAS |
|---|---|---|---|---|---|
| PDE Catalog (incl. FW/ SW & connectivity) | Medium | Foundation for compliance and risk management | Comprehensive and up-to-date list | CMDB / product catalog; version export | Hidden variants/OEM modifications. |
| Annex classification& Criticality Class per Product | High | Determines the CE conformity assessment route. | Classification documented and legally validated | Decision table; legal opinion. | Misclassification. |
| Version change management vs. impact on conformity | Medium | Changes may trigger mandatory re-assessment. | Impact assessment process established | CR records; release notes; impact assessment. | Minor vs. major updates; OEM components |

## Secure-by-design

| REQUIREMENT / VERIFICATION | RISK OF NON-COMPLIANCE | EXPLANATION (WHAT & WHY) | DEFINITION OF DONE | EVIDENCE / ARTIFACT | CRITICAL FOCUS AREAS |
|---|---|---|---|---|---|
| Secure design (least privilege, hardening) | High | Inherent product safety | Principles defined and implemented | Architecture diagrams; ADR decisions. | Risk features disabled by default |
| Secure-by-default (secure default settings) | High | No user action required to enable protections | Secure by default (protections active); data minimization | Default configuration checklist; test. | Default passwords / ports / ciphers |
| Technical documentation of security measures | High | Mandatory for CE marking and market surveillance. | Document covers threats, measures, tests, and findings | TCF/technical report; traceability. | Missing or outdated evidence |

## SDLC & Testing

| REQUIREMENT / VERIFICATION | RISK OF NON-COMPLIANCE | EXPLANATION (WHAT & WHY) | DEFINITION OF DONE | EVIDENCE / ARTIFACT | CRITICAL FOCUS AREAS |
|---|---|---|---|---|---|
| Security in SDLC (SAST/ DAST, code review, pen-test) | High | Appropriate testing based on risk and product class. | Defined quality gates; remediation tickets | SAST/DAST reports; pen-test; remediation re-cords. | Recurring findings without remediation. |
| Crypto management (keys & libraries) | High | Prohibition of obsolete algorithms; Key Man-agement (KM) | Current cryptographic policy and inventory | Algorithm list; KMS/ HSM policy; crypto-graphic review. | Hard-coded keys; legacy libraries |
| FW/OS hardening (se-cure boot, integrity, up-date policy) | Medium | Improves resiliency | Security baseline ap-plied and audited | Baseline document; control results; excep-tions. | Exceptions without jus-tification or expiry. |

## Vulnerability & Patch Mgmt

| REQUIREMENT / VERIFICATION | RISK OF NON-COMPLIANCE | EXPLANATION (WHAT & WHY) | DEFINITION OF DONE | EVIDENCE / ARTIFACT | CRITICAL FOCUS AREAS |
|---|---|---|---|---|---|
| VDP/CVD policy (intake, triage, SLAs) | High | Also required for report-ing from Sep´26. | Approved policy and op-erating procedures | VDP; security.txt; SLA metrics | Ignored external re-ports |
| Secure updates (report submission, triage, SLAs) | High | Integrity and availability of security updates | Update channel de-ployed & validated | Signatures; test proto-cols; rollback plan. | Vendor lock-in; SPOF in distribution. |
| Reporting of significant vulnerabilities/incidents | High | Mandatory reporting deadlines and channels from 09/2026 | Playbooks; contacts; dry run performed | IR playbook; CSIRT/EN-ISA contacts; test re-cord. | GDPR / legal text ap-proval |

## CE Docs

| REQUIREMENT / VERIFICATION | RISK OF NON-COMPLIANCE | EXPLANATION (WHAT & WHY) | DEFINITION OF DONE | EVIDENCE / ARTIFACT | CRITICAL FOCUS AREAS |
|---|---|---|---|---|---|
| Technical documentation (Annex I) – complete and up-to-date | High | Ready for supervison | TCF covers threats, measures, tests, and updates | TCF; requirements traceability | Outdated versions; non-compliance |
| EU declaration of conformity & CE marking | Medium | Visibility under the CRA | Pilot DoC completed; templates for other products | DoC; CE marking in manual/on product. | Unclear intended use. |
| Conformity assessment process (internal vs. notified body) | Medium | Crucial for critical product classes | Decision documented & justified | Minutes; communication with NB | Under / over-assessment |

## Import & Distribution

| REQUIREMENT / VERIFICATION | RISK OF NON-COMPLIANCE | EXPLANATION (WHAT & WHY) | DEFINITION OF DONE | EVIDENCE / ARTIFACT | CRITICAL FOCUS AREAS |
|---|---|---|---|---|---|
| Importer verification (CE, docs, traceability) | Medium | Importer assumes responsibility | Controls established & auditable | Inbound checklists; inspection records. | Incomplete documentation |
| Distributor verification (labels, instructions, safety info) | Medium | Distributor verifies compliance requirements | Process established, staff trained | Checklist; control record. | Illegible or incorrect info |

## Post-market surveillance

| REQUIREMENT / VERIFICATION | RISK OF NON-COMPLIANCE | EXPLANATION (WHAT & WHY) | DEFINITION OF DONE | EVIDENCE / ARTIFACT | CRITICAL FOCUS AREAS |
|---|---|---|---|---|---|
| Collection of operational and security data | Medium | Reduces time of issue detection | Mechanisms & legal framework defined | Data collection description; DPIA; legal consent. | Proportionality; data minimization |
| Corrective actions / market withdrawal (tabletop exercise) | High | Obligation to respond to identified risks | SOP established and validated | SOP; test record; communication templates. | Communication speed and reach. |

## Supply Chain

| REQUIREMENT / VERIFICATION | RISK OF NON-COMPLIANCE | EXPLANATION (WHAT & WHY) | DEFINITION OF DONE | EVIDENCE / ARTIFACT | CRITICAL FOCUS AREAS |
|---|---|---|---|---|---|
| Component inventory (SBOM / VEX) | High | Rapid vulnerability response | SBOM per version; integrated with ticketing system | SBOM; VEX; notifications | Transitive dependencies; embedded modules |
| Contractual requirements for suppliers (patching, reporting, documentation) | High | Post-market conformity maintenance | CRA clauses in contracts | Contract addendums; due diligence checklist | Security SLAs; patching deadlines |
| Build provenance & artifact signing | Medium | Build and provenance integrity | Signing & audit trail enabled | CI/CD logs; signing policies; attestations | CI/CD access; secrets. |

## Governance

| REQUIREMENT / VERIFICATION | RISK OF NON-COMPLIANCE | EXPLANATION (WHAT & WHY) | DEFINITION OF DONE | EVIDENCE / ARTIFACT | CRITICAL FOCUS AREAS |
|---|---|---|---|---|---|
| Program ownership (product security lead) & RACI | High | Clear cross-departmental accountability | RACI approved; appointments valid | Policy; appointment letter. | Dual roles/accountability gaps. |
| Training (secure coding / testing / documentation / support) | Medium | CRA competence | Training plan with attendance records and practical exercises | Training records; tests; syllabi. | Theory only, without exercises. |
| Management reporting (compliance status, risks, resources) | Medium | Continuous monitoring and prioritization | Monthly/quarterly report with metrics | Dashboard; board meeting minutes | "Green" status without prooves. |

## Audit Readiness & Dry-Runs

| REQUIREMENT / VERIFICATION | RISK OF NON-COMPLIANCE | EXPLANATION (WHAT & WHY) | DEFINITION OF DONE | EVIDENCE / ARTIFACT | CRITICAL FOCUS AREAS |
|---|---|---|---|---|---|
| Gap assessment against CRA (Annex I) | High | Gap identification | Gap list and remediation plan (owner/deadline) | Gap report; risk register; remediation project. | Cumulative "minor" gaps. |
| Evidence packages per product | High | Expedites assessment and oversight | Full package: design, tests, DoC, TCF, SBOM, VEX | Evidence list; repository; versioning. | Document inconsistency. |

## 3. METRICS

| METRIC | VALUE | UNIT | DEFINITION | NOTE |
|---|---|---|---|---|
| Number of security findings (open) | (fill) | count | Open findings from SAST/DAST/pen-test (Severity Medium+). | (fill) |
| Median TTR for security fixes – last 90 days | | days | Median time from discovery to closure (Severity Medium+). | |
| % Products with DoC (Declaration of Conformity) | | % | Proportion of products in the portfolio with an approved DoC. | |
| % Products with Complete TCF | | % | Proportion of products with complete technical documentation (Annex I). | |
| SBOM Coverage (Current Versions) | | % | Proportion of products with a valid SBOM (latest released version). | |
| VDP SLA Compliance (External Reports) | | % | Proportion of external reports processed within SLA. | |
| Severe Incidents Reported to Authorities | | count | Number of mandatory reports under the CRA (from 09/2026). | |
| Time to Submit Mandatory Report | | hrs | Avg. time from detection to report submission. | |

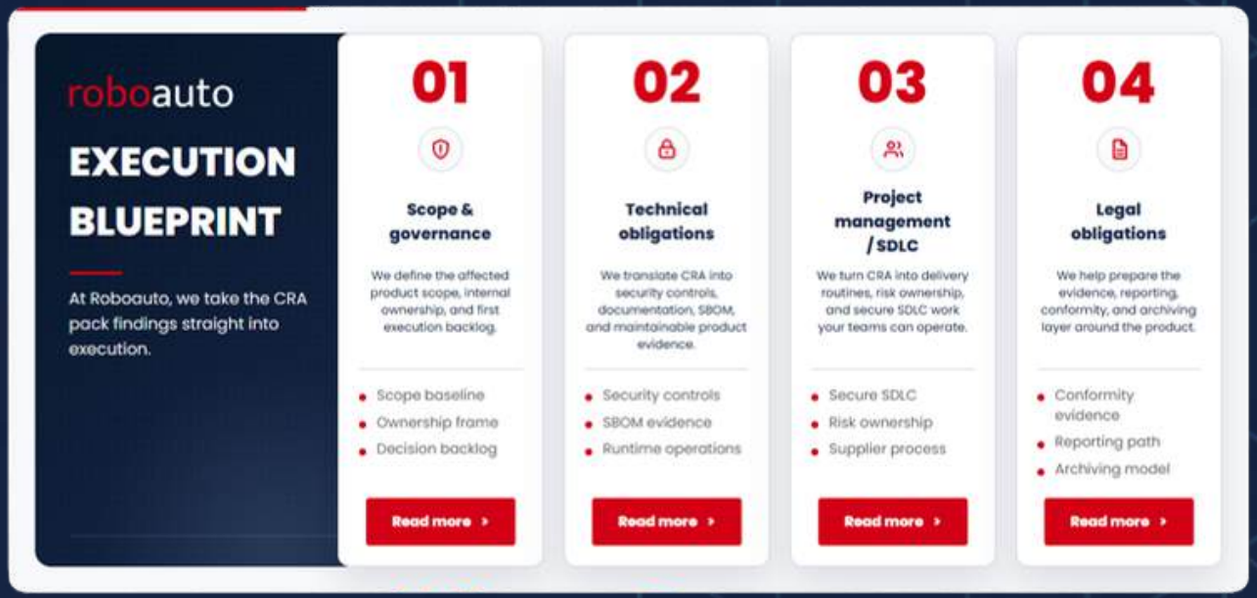
## 4. HOW YOU KNOW YOU'VE WON

- [ ] You have your entire portfolio classified & compliance routes locked in.
- [ ] Your VDP/CVD & secure update pipelines (w/ rollback) are live.
- [ ] You are fully prepped for the Sep '26 severe incident reporting trigger.
- [ ] You hold audit-ready Proof of Defense (TCF) & DoC/CE for every product.
- [ ] You've secured the full lifecycle via SBOM/VEX & ironclad vendor contracts.
- [ ] You have clear ownership (RACI/Lead) & no-fluff executive reporting established.

**CONGRATULATIONS ON ACHIEVING CRA READINESS!**

# CRA Execution Blueprint

Turn CRA priorities into a clear solution scope, support model, and next-step conversation.




**Explore the Blueprint**

# Ask us more

We are engineers, not bureaucrats.

We turn CRA insights into clear decisions, ownership, and technical workstreams.

Ready to define your scope? Book a technical alignment call with our colleague, Milan Krčma.

**Talk to our CRA expert**

**Milan Krčma**

@ milan.krcma@roboauto.cz

in linkedin.com/in/milan-krcma/