Accelerate Your CRA Readiness and CE Mark

Gain the visibility and risk insight needed to confidently meet CRA requirements.

RUNSAFE SECURITY

Documentation Category	Requirements / Example Content	RunSafe	RunSafe Capability/Notes
Cybersecurity Risk Assessment Report Documented threat model, risk scoring, mitigations, and residual risk de	Identify product scope and intended use		Subject to RunSafe customers' practices.
	Define threat model and attack surfaces	✓	Subject to RunSafe customers' practices.
	Apply risk scoring methodology	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon).
	Document mitigations and residual risk	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon). RS Protect makes vulnerability non-exploitable.
	Maintain lifecycle updates	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon).
Secure Development Lifecycle (SDL) Documentation Evidence security embedded across lifecycle.	Secure-by-design controls	✓	RunSafe enforces policies at build time so customers do not release code violating a regulatory control or company governance policy
	Code review and testing practices		Subject to RunSafe customers' practices.
	CI/CD security integration	✓	RunSafe integrates into CI/CD pipelines. With buildtime-generated SBOMs, RunSafe embeds security checks directly into development workflows. RunSafe protect prevents exploitation of vulnerabilities.
	Supplier and component controls	✓	RunSafe captures data on open source repos and risk related to open-source software controls, and enumerates vulns by component
	Documentation retention		Subject to RunSafe customers' practices.
Software Bill of Materials (SBOM) Inventory of software components and dependencies.	Generate in commonly used format	✓	RunSafe automatically generates Cyclone DX compliant SBOMs, reporting on all mandatory NTIA minimum elements
	Cover at least top-level dependencies	✓	RunSafe covers all software (OS, firmware, apps, libraries) with a full dependency tree
	Include in technical documentation		Subject to RunSafe customers' practices.
	Maintain across lifecycle	✓	RunSafe continuously updates, generating a buildtime SBOM so it is created when firmware or software image is produced to ensure product accuracy.
	Provide to authorities upon request		Subject to RunSafe customers' practices.
Vulnerability Management & Monitoring Plan Process for identifying and remediating vulnerabilities.	Continuous vulnerability monitoring	✓	RunSafe incorporates dozens of sources (including NVD and vendor advisors) to identify vulnerabilities associated with each component of an SBOM. Supports VEX to communicate known, specific vulnerabilities
	Defined triage methodology	✓	Risk Reduction Analysis tool analyzes exposure to CVEs and potential zero days; and determines if a vuln is exploitable when RunSafe protections are applied
	Patch and mitigation procedures	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon). RS Protect makes vulnerability non-exploitable.
	Remediation tracking	✓	RunSafe eliminates exploitation of entire classes of vulns even when a patch is not available, offers a service to know whether vuln is proteced from exploitation
	Decision documentation	✓	RunSafe identifies the version where patching is needed, and users can triage patches; also RunSafe confirms when a vulnerability is not exploitable
Incident Response & Regulatory Reporting Procedure Process for reporting exploited vulnerabilities and incidents.	24-hour authority notification workflow		Subject to RunSafe customers' practices, but RunSafe scans every 24 hours, allowing customers to act within that 24-hour window.
	Incident severity classification	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon).
	Internal escalation process		Subject to RunSafe customers' practices.
	User communication plan		Subject to RunSafe customers' practices.
	Record retention		Subject to RunSafe customers' practices.
Supply Chain Due Diligence Records Evidence of oversight for third-party components	Third-party component identification	✓	All software components with a full dependency tree. Reports on all mandatory NTIA minimum elements
	Open-source tracking	✓	RunSafe captures data on open source repos and risk related to open-source software
	Supplier security evaluation		Subject to RunSafe customers' practices.
	Monitor upstream vulnerabilities	✓	RunSafe incorporate sources to identify vulnerabilities with the SBOM, monitors for new alerts, and analyzes exposure to CVEs and potential zero days; and determines if exploitable
	Document supplier actions		Subject to RunSafe customers' practices.
Security Update & Support Policy Documented lifecycle support commitments.	Minimum 5-year support commitment		Subject to RunSafe customers' practices.
	Secure update release process		Subject to RunSafe customers' practices.
	Update availability controls		Subject to RunSafe customers' practices.
	End-of-support communication		Subject to RunSafe customers' practices.
	Archive and retention practices		Subject to RunSafe customers' practices.
EU Declaration of Conformity & CE Marking File Formal declaration and supporting evidence.	Confirm essential cybersecurity requirements	✓	RunSafe reports provide technical evidence supporting conformity claims.
	Reference harmonized standards		Subject to RunSafe customers' practices.
	Index of technical documentation		Subject to RunSafe customers' practices.
	Retention for required period		Subject to RunSafe customers' practices.