CRA Reporting Readiness Checklist

The Cyber Resilience Act's first reporting requirements take effect September 11, 2026. Use this checklist to review the processes, product information, and internal coordination that may come into play if your organization becomes aware of a reportable cybersecurity issue.

Cybersecurity Reporting and Intake

- [ ] Is there an accessible channel for customers and other parties to report cybersecurity issues?
- [ ] Is the reporting channel actively monitored?
- [ ] Is there a defined process for routing a report to the appropriate people?
- [ ] Can a report received outside normal business hours reach someone who can evaluate it?

Product and Configuration Information

- [ ] Can potentially affected products and configurations be identified quickly?
- [ ] Are relevant software and firmware versions readily identifiable?
- [ ] Can third-party components be traced across products and configurations?
- [ ] Are product revisions, component records, and configuration information accessible?
- [ ] Can design and production records help establish where an affected component was used?

Roles and Reporting Responsibilities

- [ ] Is responsibility for evaluating technical information clearly defined?
- [ ] Is responsibility for determining whether an event meets the CRA reporting threshold clear?
- [ ] Is authority for submitting notifications through the Single Reporting Platform (SRP) established?
- [ ] Are primary and backup reporting responsibilities identified?
- [ ] Is there a process for sharing information among the functions involved?

Information for CRA Reporting

- [ ] Is the product information needed for an early warning readily available?
- [ ] Can additional technical information be assembled as the reporting process progresses?
- [ ] Are cybersecurity findings and reporting decisions connected to the incident record?
- [ ] Can mitigation and update information be connected to the same event?
- [ ] Can relevant information be carried forward from the 24-hour early warning to subsequent reporting?

Cross-Functional Coordination

- [ ] Can technical findings be escalated to the appropriate functions quickly?
- [ ] Are reporting, technical response, mitigation, and customer communication activities connected?
- [ ] Are internal handoffs clearly understood?
- [ ] Can the people involved work from a common incident record?
- [ ] Is there continuity if a primary contact is unavailable?

Final Readiness Check

If a reportable cybersecurity issue occcured today:

How quickly could we identify what is affected?

Could we get the available information to the appropriate people?

Are reporting responsibilities clear?

Could our current process operate within the CRA reporting timeline?