

Meeting DORA requirements with DefectDojo

Regulation (EU) 2022/2554 and its ICT risk management standard, Delegated Regulation (EU) 2024/1774, set out how EU financial entities must find, prioritize, and fix vulnerabilities. Here are the DORA obligations that run through a vulnerability management program, each paired with the DefectDojo capability that answers it.

IN FORCE

Jan 16, 2023

DORA entered into force, opening a two-year implementation window.

IN EFFECT NOW

Jan 17, 2025

DORA applies across more than 20 types of EU financial entities.

MINIMUM SCAN CADENCE

Weekly

Automated scanning of ICT assets supporting critical or important functions.

THREAT-LED TESTING

Every 3 years

TLPT for financial entities their competent authority identifies.

☒ **Covered:** DefectDojo does this work

☐ **Supports:** your process, enforced and recorded

Sensei is a DefectDojo Pro capability in beta that requires its own license entitlement.

SECTION 1 · RTS 2024/1774, ARTICLE 10 · IN EFFECT SINCE JAN 17, 2025

Vulnerability and patch management

DORA REQUIREMENT	HOW DEFECTDOJO CHECKS THE BOX	EDITION
☒ RTS 2024/1774, ART. 10(2)(A) Identify and keep current the trustworthy information sources you use to stay aware of vulnerabilities.	EPSS and CISA KEV data enrich findings at import and daily after, and a KEV listing raises a finding's Priority and Risk. PSIRT polls advisory feeds from publishers including CISA, NVD, and EUVD, and matches each advisory against your SBOM inventory.	PRO
☐ RTS 2024/1774, ART. 10(2)(B) Run automated vulnerability scanning and assessments on ICT assets, at least weekly for assets supporting critical or important functions.	Your scanners (and Sensei, for code repositories) run the scans, and DefectDojo keeps the proof that they ran. Results arrive from CI/CD and the API, and Pro connectors sync supported tools on a recurring schedule. Every Test is dated on the product it covers, so the scan cadence for each critical asset is on the record.	COMMUNITY EDITION PRO
☐ RTS 2024/1774, ART. 10(2)(C) Verify that ICT third-party service providers handle vulnerabilities in the services they provide and report at least the critical ones to you in a timely manner.	Import the scan and pen test reports your providers send as findings on a product for each provider. Their critical issues then carry your SLA, your triage, and your history, and overdue items show up in the same queue as your own.	COMMUNITY EDITION PRO
☒ RTS 2024/1774, ART. 10(2)(D) Track third-party libraries, including open source libraries, used by ICT services supporting critical or important functions.	SCA and SBOM results from tools such as Dependency-Track and Gripe arrive as deduplicated findings per product. Pro imports CycloneDX and SPDX SBOMs into a component inventory and checks it against each new advisory.	COMMUNITY EDITION PRO
☐ RTS 2024/1774, ART. 10(2)(E) Set up procedures for the responsible disclosure of vulnerabilities to clients, counterparties, and the public.	Write, review, and publish your own security advisories. Publishing requires every reviewer's approval, an embargo date blocks release until it passes, and each publish is snapshotted exactly as sent.	PRO
☒ RTS 2024/1774, ART. 10(2)(F) Prioritize patches and mitigations by the vulnerability's criticality and the classification and risk profile of the affected asset.	Priority and Risk weigh finding severity, product-level business criticality and exposure, EPSS, and KEV, so the queue reflects both the vulnerability and the asset it sits on. Community Edition sorts and filters by severity and SLA days.	COMMUNITY EDITION PRO
☒ RTS 2024/1774, ART. 10(2)(G) AND (H) Record every detected vulnerability affecting ICT systems, then monitor and verify its remediation.	Every finding keeps its status and Object History. Reimporting a recurring scan closes findings that no longer appear and reopens any that return, so the next scan confirms each fix.	COMMUNITY EDITION PRO
☒ RTS 2024/1774, ART. 10(4)(D) Set deadlines for installing patches and updates, with escalation procedures when a deadline cannot be met.	Per-product SLAs set the deadline by severity or (in Pro) by risk, notify owners on breach, and can post breach notices to the Jira issue. When a deadline cannot be met, a Risk Acceptance records why and when it expires. Sensei opens pull requests that fix findings.	COMMUNITY EDITION PRO SENSEI (BETA)

Digital operational resilience testing

DORA REQUIREMENT	HOW DEFECTDOJO CHECKS THE BOX	EDITION
✓ ARTICLE 25(1) Run appropriate tests, such as vulnerability assessments and scans, open source analyses, source code reviews, and penetration testing.	Results from 360+ security tools in Community Edition (500+ in Pro) land on one product and are deduplicated (across tools in Pro), so SAST, SCA, infrastructure scans, and pen test reports read as one record of the asset.	COMMUNITY EDITION PRO
✓ ART. 25(1) AND RTS ART. 10(2)(B) Review and scan source code where feasible, as part of regular automated vulnerability scanning.	Sensei scans connected GitHub and GitLab repositories on demand and automatically when a pull request is opened, and imports the results as findings on the product. Each run is logged in Scan Activity, and Sensei can open a pull request that fixes what it found.	PRO SENSEI (BETA)
✓ ARTICLE 24(5) Prioritize, classify, and remedy every issue a test reveals, and validate that each weakness is fully addressed.	Pen test and assessment findings go into an Engagement alongside scanner output, with the same severity, SLA, and Jira workflow. A retest reimported into the same Test closes what was fixed and reopens what was not, which becomes the validation record.	COMMUNITY EDITION PRO
☐ ARTICLE 26 Threat-led penetration testing at least every three years for entities their competent authority identifies, with remediation plans for what the test finds.	Bring TLPT findings into their own Engagement, push them to Jira, and track each one against an SLA. The Report Builder and, in Pro, the Remediation Metrics dashboard show progress against the plan.	COMMUNITY EDITION PRO

Governance, assets, and evidence

DORA REQUIREMENT	HOW DEFECTDOJO CHECKS THE BOX	EDITION
☐ ARTICLE 8(1) Identify, classify, and document ICT-supported business functions and the ICT assets that support them.	Model each ICT asset as a product in DefectDojo's hierarchy and record its business criticality and external exposure. In Pro, that classification drives Priority, Risk, and risk-based SLAs for every finding on it.	COMMUNITY EDITION PRO
☐ ARTICLE 5(2) The management body defines, approves, and oversees the ICT risk management framework and remains accountable for it.	Executive Insights and Remediation Metrics dashboards in Pro track SLA performance by product, giving the management body a current view of vulnerability risk. Community Edition reports come from the Report Builder.	COMMUNITY EDITION PRO
☐ ARTICLE 6(1) Keep a sound, well-documented ICT risk management framework, with the records that show it operating.	Risk Acceptances store the justification and supporting files, with an expiration date that returns findings to Active for review. Object History records changes to products, engagements, tests, findings, and Risk Acceptances. Pro adds an instance-wide Audit Log and a history API.	COMMUNITY EDITION PRO

COMMUNITY EDITION

The handling loop, free

Self-hosted under BSD-3. 360+ parsers, deduplication, per-product SLAs with breach notifications, Risk Acceptances, Jira sync, the Report Builder, and object history on every finding.

DEFECTDOJO PRO

Risk-ranked, audit-ready

500+ integrations, in the cloud, on-premises, or air-gapped. For DORA, Pro adds Priority and Risk weighted by asset classification and EPSS and KEV enrichment (RTS Art. 10), scheduled connectors for the scan record, and Executive Insights for management body oversight (Article 5).

PSIRT MODULE (BETA)

Libraries and disclosure

SBOM import and advisory matching for third-party and open source libraries, plus a review-gated workflow for publishing your own advisories (RTS Art. 10(2)(d) and (e)). Requires the PSIRT Advisory Engine entitlement.

ABOUT DEFECTDOJO

DefectDojo is the open source unified vulnerability management platform that remediates at the speed of AI, enabling security teams to focus on fixing the most critical vulnerabilities first. Parse any security finding, aggregate across your stack, prioritize what matters, and report on your security posture and compliance.

BOOK A DEMO

Walk through asset classification, risk-based SLAs, and your scan evidence with our team.

Book yours at defectdojo.com/book-a-demo

This datasheet maps DefectDojo capabilities to DORA and Commission Delegated Regulation (EU) 2024/1774 for planning purposes and is not legal advice. DefectDojo records findings, decisions, and remediation. Outside of Sensei repository scans, it does not run your scans. It does not classify or report major ICT-related incidents or maintain your register of information on ICT third-party arrangements. Confirm your obligations, including whether Article 16 applies, with qualified counsel. Beta capabilities may change before general availability.