

10 Core Procurement Artefacts

These are the artefacts most commonly requested by procurement teams, Notified Bodies, and regulators. Build them incrementally. The early ones unlock pilot conversations; the later ones unlock formal submissions.

Key:

- ✔ **Mandatory** / will cause delays if missing.
- ✔ **Expected** / commonly asked.

Artefact	What it is and Why	Minimum Standard	DTAC	EU MDR/ IVDR	FDA 510(k)	Update Cadence
1 Security Architecture and Boundaries	Diagram and narrative showing device/app/cloud/integrations and trust boundaries. Shows what you control vs what the customer controls and where data flows.	One diagram (data flows and trust boundaries) plus 1-2 pages on responsibilities.	✔	✔	✔	On significant design change.
2 Threat Model and Risk Register	Top threat scenarios with risk ratings, mitigations, and residual risk rationale. Shows systematic identification and treatment of device-specific threats.	Top scenarios, risk rating (likelihood/impact), mitigations, residual risk rationale, named owners.	✔	✔	✔	Per major release.
3 Risk-control Traceability Matrix	Single table linking threats, controls, verification, and evidence location. Proves controls actually address identified risks with test evidence.	Risk/threat, control, verification method, evidence link, status.	✔	✔	✔	Quarterly review.
4 SBOM and Vulnerability Monitoring	Software Bill of Materials per release plus documented CVE monitoring workflow. Shows what third-party components you use and how you handle vulnerabilities.	SBOM stored with each release plus documented CVE monitoring/triage process with decision records.	✔	✔	✔	Every release; monitoring ongoing.
5 Vulnerability Disclosure Policy (VDP/ PSIRT)	Public reporting route, triage process, severity model, escalation. Shows how you handle security issues discovered after deployment.	Public reporting contact, triage steps, severity model, decision owners, comms triggers.	✔	✔	✔	Quarterly review.

Artefact	What it is and Why	Minimum Standard	DTAC	EU MDR/IVDR	FDA 510(k)	Update Cadence
6 Secure Update/Patch Policy	How you deliver updates: signing, rollback, routine vs urgent timelines. Ensures vulnerabilities can be patched without breaking devices.	Signed updates, rollback/fail-safe behaviour, routine vs urgent patch timelines, supported versions.	✓	✓	✓	Annual plus on platform change.
7 Security Test Evidence	Automated scans plus independent testing scoped to system boundary. Verifies controls work in practice.	SAST/DAST/dependency scans with triage logs plus scoped independent testing across system boundary.	✓	✓	✓	Continuous (automated); annually or major change (independent).
8 Logging/Monitoring Approach	What events are logged, alerting triggers, retention, access controls. Shows you can detect and investigate security incidents.	Events logged (admin actions, auth failures, key workflows), alerting, retention, access controls.	✓	✓	✓	Per environment change.
9 Supplier Security Controls	Vendor due diligence, access boundaries, onboarding/offboarding, contracts. Covers third-party risk from cloud, manufacturers, and contractors.	Supplier list, access boundaries, onboarding/offboarding, minimum security requirements, incident notification expectations.	✓	✓	✓	Per supplier; annual review.
10 Incident Response Playbook and Rehearsal	Roles, escalation, containment steps, evidence you have tested it. Shows you can handle incidents quickly without improvising.	One-page roles/escalation/comms/containment checklist plus evidence of rehearsal (tabletop exercise minimum).	✓	✓	✓	Rehearse at least annually.



Note: The artefacts are the core set. There are additional artefacts that may apply depending on your product type, deployment model, and target market. Use this table as a starting reference.