BLUE GOAT CYBER

Medical Device Cybersecurity · FDA Specialists

EU MDR & IVDR CYBERSECURITY GUIDE

EU MDR & IVDR Cybersecurity Guide

MDR Annex I, IVDR, MDCG 2019-16, and the Cyber Resilience Act - plus a harmonized FDA + EU submission package.

© Blue Goat Cyber. For educational use. Not legal or regulatory advice.

EU MARKET ACCESS

EU MDR & IVDR cybersecurity guide.

EU MDR (2017/745) and IVDR (2017/746) embed cybersecurity directly into the General Safety and Performance Requirements. **MDCG 2019-16 Rev.1** is the de-facto guidance Notified Bodies use, and the **Cyber Resilience Act** adds horizontal cybersecurity requirements for products with digital elements. If you're filing FDA + CE in parallel, you can build one evidence package that satisfies both - if you plan it that way.

Key takeaway: Notified Bodies are increasingly asking for the same artifacts FDA reviewers want - SBOM, threat model, pen test, postmarket plan. A harmonized package saves months of duplicated work.

1. MDR Annex I §17.2 + IVDR Annex I §16.4 - the core requirements

State of the art	Devices with software shall be designed against the state of the art for IT security.
Minimum IT environment	Manufacturer specifies the minimum hardware, network, and security characteristics needed.
Protection by design	Protection against unauthorized access required by design - not bolted on.
Lifecycle risk management	Repeatable, verifiable cybersecurity risk management throughout the lifecycle.

2. MDCG 2019-16 Rev.1 - the operative guidance

- **Security risk management** integrated with ISO 14971.
- **Secure design and manufacture** - analogous to FDA's SPDF.
- **Security verification and validation** expectations (incl. pen testing).
- **Postmarket surveillance, incident reporting, and updates**.
- **IT security capabilities** communicated to operators (analogous to MDS^2).

3. Cyber Resilience Act - what's coming

Scope	Horizontal cybersecurity requirements for products with digital elements placed on the EU market.
Vulnerability handling	Mandatory CVD process and ENISA notification of actively exploited vulnerabilities.

Security updates	Free security updates throughout the expected product lifetime.
Conformity assessment	Important / critical product classes require third-party assessment.
Lex specialis	MDR/IVDR carve-outs are still being clarified - assume some overlap, plan for both.

4. Notified Body evidence pack

- Cybersecurity risk assessment integrated with ISO 14971 risk file.
- SBOM (CycloneDX 1.5 + VEX preferred).
- Threat model with mitigations traced to design controls.
- Penetration test report - manual, exploit-driven, not just scanner output.
- Postmarket surveillance plan with vulnerability monitoring and CVD policy.
- User-facing security documentation (analogous to MDS^2).
- Software lifecycle process evidence (IEC 62304 + IEC 81001-5-1).

5. FDA vs. EU - side-by-side evidence requirements

SBOM	FDA: machine-readable required. EU/MDCG: expected; CRA will mandate. Same artifact works.
Threat model	FDA: STRIDE-per-element + ANSI/AAMI SW96. EU: ISO/IEC 62443-4-1 patterns. Same model, mapped both ways.
Pen test	FDA: manual, exploit-driven. EU: same expectation under IEC 81001-5-1. Same report works.
Postmarket / CVD	FDA: 524B + 2026 guidance. EU: MDCG 2019-16 + CRA. Same program, two policy references.
Labeling	FDA: cybersecurity labeling for end users. EU: IT security capabilities for operators. Aligned via MDS^2.

6. Harmonized FDA + EU submission architecture

- **One canonical SBOM** (CycloneDX 1.5) - referenced by both submissions.
- **One threat model** with two annexes mapping to FDA and MDCG terminology.
- **One pen test report** with executive summaries tailored to each regulator.
- **One postmarket / CVD policy** citing FDA 524B + ISO/IEC 29147/30111 + MDCG.
- **One labeling/MDS^2 set** updated in lockstep when posture changes.

7. Common Notified Body deficiency themes

- Cybersecurity risk not integrated with ISO 14971 - treated as a separate file.
- No evidence of pen testing by qualified independent testers.

- Postmarket plan reads as policy, not a working process.
- User documentation missing IT environment requirements.
- IEC 81001-5-1 process gaps - especially activity records and traceability.

Key takeaway: If you're entering EU and US markets, design the evidence package once, with both audiences in mind. Retrofitting a US-only package for CE adds months.

READY FOR THE NEXT STEP?

Talk to a senior medical device security engineer.

We've contributed cybersecurity documentation, threat models, SBOMs, and pen test reports to **250+ FDA submissions** across 510(k), De Novo, and PMA pathways - with a **100% submission success rate**. If you're building a cyber device and want to go in with airtight artifacts on the first try, we should talk.

Book an EU + FDA harmonization session
30 minutes. No slide deck. Bring your device profile and your top three questions.

bluegoatcyber.com/contact

WHAT WE DO

- **FDA premarket cybersecurity** - SPDF, threat model, SBOM, pen test, security risk assessment, eSTAR-ready package
- **FDA cybersecurity deficiency response** - rapid remediation when reviewers send a letter
- **Postmarket programs** - vulnerability monitoring, VEX, coordinated disclosure, patch validation
- **Legacy device remediation** - bring older devices up to current FDA expectations