

EU MDR/IVDR Cybersecurity Evidence Crosswalk

Reviewed 2026-10-18 | Map MDR and IVDR cybersecurity duties to evidence, technical-file locations, owners, and review triggers, with a worked connected-analyzer example.

Build an EU cybersecurity crosswalk by connecting each applicable general safety and performance requirement (GSPR) to device-specific security evidence in the technical documentation. Use MDR Annex I 17.2 and 17.4 for medical device software, and IVDR 16.2 and 16.4 for IVD software. Include risk management, control testing, minimum IT security requirements, and postmarket processes. Record why a requirement applies, not just whether a document exists.

[Download the matching evidence crosswalk PDF.](#)

This is a working evidence index for engineering and RA/QA teams, not another comparison of EU and US submission pathways. For the regulatory overview, read [medical device cybersecurity in the EU](#). For multi-market planning, use [MDC Crosswalk](#) as a companion reference. The European Commission and legislation linked below remain the authorities for EU requirements.

Establish applicability before mapping evidence

Record the intended purpose, device classification, applicable regulation, conformity-assessment route, software boundaries, and marketed configurations. Include device software, companion software, interfaces, and supporting services where they affect device safety or performance. Explain which parts belong to the regulated product rather than assuming that every connected component has the same legal status.

The tables below paraphrase selected provisions. They are not a complete GSPR checklist or a declaration of conformity. The manufacturer must assess all applicable requirements. Notified Body involvement depends on the device and conformity-assessment route; not every device receives a full Notified Body technical-file review.

Binding requirement to practical evidence

Legal anchor	Duty in plain language	Evidence and controlled file location
MDR / IVDR Annex I 3	Maintain an iterative risk management system throughout the device lifecycle	Risk management plan, security risk assessment, safety links where relevant, and approved risk decisions; Annex II section 5
MDR 14.2(d) / IVDR 13.2(d)	Reduce risks from foreseeable external influences, including negative interactions with the IT environment	Deployment assumptions, interface inventory, threat model, and environment-specific control/test records; device description and Annex II sections 5 and 6
MDR 17.2 / IVDR 16.2	Develop software to the state of the art, considering lifecycle, risk management, information security, verification, and validation	Secure development records, security requirements, architecture, traceability, and security test evidence; Annex II sections 3, 5, and 6
MDR 17.4 / IVDR 16.4	Specify minimum hardware, IT network, and IT security requirements, including protection against unauthorized access	Approved deployment baseline, identity/access requirements, network assumptions, and configuration instructions; Annex II sections 2 and 4
MDR 18.8	Protect active devices, as far as possible, against unauthorized access that could prevent intended function	Access-control design, service-interface restrictions, abuse-case tests, and residual risk rationale; Annex II sections 5 and 6. Do not invent an identical IVDR 18.8 counterpart
MDR 23.4(ab) / IVDR 20.4.1(ah)	State the minimum hardware, IT network, and IT security requirements in the instructions for use for applicable software devices	Controlled IFU and security deployment instructions, consistent with the tested operating environment; Annex II section 2
MDR / IVDR Annex II 4	Document conformity with applicable GSPRs and justify nonapplicability	GSPR checklist linking each applicable row to identified standards, methods, and controlled evidence; Annex II section 4
MDR Articles 83-86 / IVDR Articles 78-81, plus Annex III	Operate postmarket surveillance and produce the applicable PMS report or PSUR	PMS plan, vulnerability monitoring inputs, trend analysis, remediation records, and periodic report inputs; Annex III and the QMS
MDR Articles 87-89 / IVDR Articles 82-84	Assess serious incidents and field safety corrective actions and meet applicable vigilance duties	Reportability decisions, authority notifications where required, field safety notices, and corrective-action records; vigilance procedure and PMS evidence

Verification and validation are manufacturer lifecycle obligations mentioned in the legislation. Blue Goat Cyber supports the cybersecurity evidence and security testing within that lifecycle, not general software verification and validation services.

Guidance and standards are not the same as legislation

[MDCG 2019-16 Rev.1](#) explains security by design, security risk management, security capabilities, testing, and lifecycle responsibilities. It is nonbinding guidance. Threat modeling, component inventories or SBOMs, vulnerability assessments, and security test reports are practical evidence choices; do not label every artifact as an explicit MDR/IVDR statutory requirement.

[IEC 81001-5-1](#) provides health-software security lifecycle activities. It does not specify the contents of accompanying documentation. Attribute IFU duties to the regulations. Check the European Commission's current harmonized-standard lists before claiming any presumption of conformity, including the exact edition, restrictions, and covered requirements. An EN designation alone does not establish harmonization.

Evidence ownership and change triggers

Evidence	Manufacturer owner	Reassess when
System boundary and threat model	Product security with system engineering	Interfaces, trust boundaries, deployment, intended use, or connected services change
Security risk assessment and safety links	Product security and risk management; authorized manufacturer approver accepts risk	New threats, vulnerabilities, control failures, or clinical impact information arise
Component inventory / SBOM	Software configuration management	Released dependencies, firmware, platform components, or supplier information change
Security requirements and test traceability	Engineering and product security, with QA-controlled records	Requirements, control implementations, test configuration, or exposure change
IFU and deployment security baseline	Manufacturer labeling / RA/QA	Tested environment, user responsibilities, patch process, or support information changes
Vulnerability handling and PMS records	Product security / PSIRT, RA/QA, and complaint handling	A report arrives, exploitation is identified, an update is released, or reporting criteria may be met

A document title is not enough. Record the artifact ID, revision, build/configuration, approval status, storage location, open gap, and remediation owner. Keep detailed findings in controlled records rather than putting confidential vulnerability details in public instructions.

Worked example: connected IVD analyzer

This is fictional and illustrates evidence linkage, not a client outcome or an accepted submission. An analyzer sends patient results to a laboratory information system through middleware. A maintenance interface also permits software updates.

Concern	Evidence chain	IVDR file reference
An attacker alters a result in transit	Threat TM-07 links to integrity requirement SEC-12, protocol/authentication design, negative-test result TEST-12, and safety analysis HAZ-04 for wrong or delayed treatment	13.2(d), 16.2; Annex II 5 and 6
A service account can install unauthorized software	Threat TM-11 links to SEC-19, update authorization/integrity controls, security test evidence, and manufacturer residual risk disposition	16.2 and 16.4; Annex II 5 and 6
Hospital configuration differs from the tested baseline	IFU requirements identify supported network and access settings; deployment evidence records the tested configuration and remaining responsibilities	16.4 and 20.4.1(ah); Annex II 2
A dependency vulnerability is disclosed after release	Versioned component inventory identifies affected builds; triage assesses exploitability and clinical consequences; PMS and vigilance procedures determine the next actions	Articles 78-84; Annex III

Result integrity, availability, confidentiality, and delayed reporting can all matter. Do not decide clinical risk from a CVSS score alone or assume that every IVD vulnerability changes a test result.

Postmarket reporting: use device law, not CRA clocks

The [Cyber Resilience Act](#), Article 2(2)(a) (MDR) and (b) (IVDR), exclude products to which the MDR or IVDR applies. Do not import its reporting clocks into a medical-device vigilance table. Separately regulated non-device products may require their own assessment.

For device serious incidents, MDR Article 87 and IVDR Article 82 set reporting duties, including immediately and no later than two days for a serious public health threat; immediately and no later than ten days for death or unanticipated serious deterioration in health; and the general maximum of fifteen days, subject to the applicable awareness and causality criteria. A vulnerability alone is not automatically a serious incident. Assess reportability and field safety corrective action under the applicable regulation and authority instructions; do not wait for a scheduled PMS review.

Readiness review

- Confirm regulation, intended purpose, product boundary, and assessment route.
- Use the correct MDR or IVDR numbering in the GSPR checklist.
- Connect each applicable row to controlled, build-specific evidence and a manufacturer owner.
- Link security findings to safety analysis where exploitation could contribute to harm.
- Resolve gaps in control testing and record manufacturer risk decisions.
- Check that the IFU agrees with deployment assumptions used in testing.
- Connect vulnerability handling to PMS, complaint handling, corrective actions, and vigilance.
- Reassess the mapping after a material product or regulatory change.

How Blue Goat Cyber helps

We support threat modeling, security risk assessment, SBOMs, penetration testing, and cybersecurity documentation mapping. The manufacturer owns its QMS, approves labeling and risk decisions, and determines regulatory submissions and reportability. See [EU MDR cybersecurity support](#) or [book a discovery call](#).

FAQ

Is an SBOM explicitly mandatory under the MDR or IVDR?

Neither regulation names an SBOM as a universal deliverable. A controlled component inventory or SBOM can support lifecycle security and vulnerability management. Explain how it supports the applicable requirements and assessment rather than citing the CRA as the device's legal basis.

Can I copy the MDR checklist into an IVDR file?

No. Many security activities are reusable, but the legal references and device risks differ. Use IVDR 16.2 and 16.4 for software lifecycle and minimum IT security requirements, and 20.4.1(ah) for the corresponding IFU provision.

Does a penetration test establish conformity?

No. It is one part of the evidence, with scope, limitations, findings, remediation, and traceability. It does not replace risk management, secure development, IFU requirements, or postmarket responsibilities.

Where does MDC Crosswalk fit?

Use [MDC Crosswalk](#) for companion multi-market mapping. Verify legal claims against the primary authorities and retain your own controlled, product-specific evidence index.

Related regional evidence

- [Japan PMDA cybersecurity guide](#)
- [UK MHRA cybersecurity guide](#)

- [IEC 81001-5-1 evidence table](#)
- [EU MDR vs FDA comparison](#)

Sources and primary references

- [Regulation \(EU\) 2017/745, MDR: Annexes I-III and Articles 83-89](#)
- [Regulation \(EU\) 2017/746, IVDR: Annexes I-III and Articles 78-84](#)
- [European Commission: MDCG 2019-16 Rev.1 cybersecurity guidance](#)
- [European Commission: harmonized standards for medical devices](#)
- [IEC 81001-5-1:2021 catalogue, corrected December 2025 version](#)
- [Regulation \(EU\) 2024/2847, CRA: Article 2\(2\)\(a\) and \(b\)](#)

Current web guide: <https://bluegoatcyber.com/guides/eu-mdr-ivdr-cybersecurity-evidence-crosswalk>

Informational material. Confirm requirements for your device and market. The manufacturer owns risk decisions, QMS approvals, and regulatory submissions. No regulatory outcome is promised.