

Medical Device Cybersecurity Due Diligence Checklist

Reviewed 2026-10-19 | A cybersecurity due diligence checklist for investors and acquirers reviewing a medical device company: regulatory status, submission evidence, testing, SBOM, postmarket readiness, and red flags.

Investors and acquirers should check five areas: whether the device is a cyber device under FDA Section 524B, what cybersecurity evidence supports the marketing submission, whether independent penetration testing covered the current build, whether the SBOM and vulnerability process are maintained, and whether a working postmarket plan exists. Ask for the underlying documents and treat gaps as cost and schedule risk to price in.

This checklist is for venture investors, private equity teams, corporate development groups, and boards reviewing a connected medical device company. It is a practical starting point for the questions to ask and the documents to request. It is not legal advice and does not replace a review of the target's actual evidence.

Why this matters

Cybersecurity is now part of whether a connected device reaches the US market on schedule. Section 524B of the FD&C Act requires specific cybersecurity content in marketing submissions for cyber devices, and the FDA's February 3, 2026 premarket cybersecurity guidance explains what the agency expects to see. A company that has not planned for this work can face a refuse-to-accept decision, a deficiency letter, or months of rework. Those outcomes affect launch dates, burn rate, and valuation, which is why they belong in diligence.

1. Regulatory status and scope

- [] Confirm whether the device meets the three-part [cyber device definition](#): it includes software, can connect to the internet, and has characteristics that could be vulnerable to cybersecurity threats.
- [] Identify the submission pathway (510(k), De Novo, or PMA) and its planned or actual filing date.
- [] Ask whether any submission received a cybersecurity deficiency letter or refuse-to-accept decision, and request the letter and the response.
- [] For devices sold outside the US, ask which markets apply, such as the [EU](#), [UK](#), or [Canada](#).

2. Premarket cybersecurity evidence

Request the documents themselves. A summary slide that says "cybersecurity complete" tells you little.

- [] Threat model with data flow diagrams and trust boundaries.
- [] Cybersecurity risk assessment that links threats to patient harm.
- [] Security architecture views.
- [] Software bill of materials (SBOM) with support status and end-of-support dates for components.

- [] Cybersecurity management plan for postmarket vulnerabilities.
- [] Traceability from threats to controls to tests.

The [premarket deliverables map](#) lists every document the FDA expects and where it goes in eSTAR.

3. Security testing

- [] Ask for the most recent penetration test report and confirm it covered the build that was or will be submitted or sold.
- [] Confirm the testers were independent of the development team.
- [] Check that findings have documented fixes, retest results, or risk rationales.
- [] Ask whether testing covered every interface: wireless, mobile app, cloud, and physical ports.

[KEY REQUIREMENT] The FDA's guidance recommends testing performed by testers independent of the developers. A pen test on an old build, or one limited to a web portal while the device itself goes untested, leaves real gaps.

See [penetration testing for medical devices](#) for what full coverage looks like.

4. SBOM and vulnerability management

- [] Confirm the SBOM is kept up to date with each release, not produced once for the submission.
- [] Ask how new vulnerabilities in third-party components are found, assessed, and fixed.
- [] Request the list of known unpatched vulnerabilities and the rationale for each.
- [] Check for end-of-life operating systems or libraries with no update path.

5. Postmarket readiness

- [] Look for a published coordinated vulnerability disclosure policy and a way for researchers to report issues.
- [] Ask how updates and patches reach fielded devices, and how long that takes.
- [] Ask whether the team has run an incident response or [tabletop exercise](#).
- [] Check whether cybersecurity is part of the quality management system, with named owners.

6. People and budget

- [] Identify who owns product cybersecurity and what their experience is.
- [] Check whether outside consultants or testers are engaged, and for what scope.
- [] Confirm the remaining cybersecurity work is in the budget and the launch timeline. Our guide to [medical device cybersecurity cost](#) explains what drives that budget.

Red flags

- No threat model, or one created after the design was finished with no updates since.

- Penetration testing done only by the development team, or not at all.
- No SBOM, or an SBOM with no support status for components.
- An open cybersecurity deficiency letter with no response plan.
- Hardware or software with no way to update devices in the field.
- "We will handle cybersecurity after clearance."

What to do with gaps

A gap is not automatically a reason to walk away. Most missing evidence can be produced. The question is how long it takes and what it costs. Turn each gap into a work item with an owner, an estimated duration, and a budget line, then check whether the company's runway and launch plan account for it.

Frequently asked questions

When should cybersecurity diligence happen?

Before the term sheet is final or during confirmatory diligence, while findings can still shape terms, milestones, or use of funds.

Does a cleared device still need cybersecurity diligence?

Yes. Clearance does not end cybersecurity duties. Section 524B also requires a plan to monitor and address postmarket vulnerabilities, and each new device version may need its own submission.

Can a company's own team produce the evidence?

Much of it, yes. The FDA recommends that penetration testing be done by testers independent of the developers, so that piece usually involves an outside team.

How long does an outside cybersecurity diligence review take?

Our [investor cybersecurity due diligence](#) review typically takes about two weeks, starts from \$7,500 at a fixed fee after scoping, and begins with a signed NDA.

Related resources

- [Download this checklist as a PDF](#)
- [Investor cybersecurity questions for medtech founders](#)
- [Sample due diligence executive summary](#)
- [Funding and cybersecurity budgets by stage](#)
- [FDA cybersecurity requirements buyer's guide](#)
- [Early-stage cybersecurity readiness checklist](#)

How Blue Goat Cyber helps

We review a target's cybersecurity evidence against Section 524B and the FDA's February 3, 2026 guidance, then report the gaps, their likely cost and timeline, and the questions to put to management. We have supported more than 275 devices. See [investor cybersecurity due diligence](#) or [view the sample summary](#).

Sources and primary references

- [FDA: Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions, February 3, 2026](#)
- [21 U.S.C. 360n-2: FD&C Act Section 524B](#)

Current web guide:

<https://bluegoatcyber.com/guides/medical-device-cybersecurity-due-diligence-checklist>

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