GUIDE

MedTech Cybersecurity Vendor Evaluation Grid

MedTech Cyber Vendor Evaluation Grid A scoring grid for cybersecurity firms tailored to MedTech regulatory needs.

MedTech Cyber Vendor Evaluation Grid A scoring grid for cybersecurity firms tailored to MedTech regulatory needs.

MedTech Cybersecurity Vendor Evaluation Grid

Free Guide · Blue Goat Cyber · Updated 2026

WORKSHEET · VENDOR EVALUATION GRID

MedTech Cyber Vendor Evaluation Grid A scoring grid for cybersecurity firms tailored to MedTech regulatory needs.

250+ 0 6-10 wk FDA submissions supported Cybersecurity rejections Class II eSTAR cyber pack

SINCE 2014 TRACK RECORD TYPICAL TIMELINE

Scoring categories (out of 5)

- FDA submission experience (weight 3×).
- Pen-test independence (weight 3×).
- Deliverable quality and eSTAR fit (weight 2×).
- Post-market support (weight 2×).
- Communication cadence and responsiveness (weight 1×).
- Pricing model clarity (weight 1×).

How to use the score

Sum the weighted scores. A vendor scoring above 35/60 typically meets the bar for a Class II software-enabled device. Below 25/60 is a meaningful risk to first-review clearance.

Auto-disqualifying answers

- No FDA submissions in the last 24 months.
- Same engineer signs threat model and pen test.

- Refuses to share sample sanitized eSTAR cyber package.
- No post-market offering.

When to use this guide

This guide is most useful in one of the following situations. If none of them describe your team, the resources index has a better fit.

- You are a Class II software-enabled MedTech preparing for a 510(k), De Novo, or PMA submission.
- You are mid-development and need the cybersecurity story to land in the eSTAR without rework.
- RA/QA owns the submission but cybersecurity work is spread across engineering, with no clear ownership.
- You have read Section 524B and the Feb 3 2026 final guidance and want a practical operating model.

Operating framework

The framework below sequences the work this guide describes against the four TPLC phases used in the Feb 3 2026 final guidance. Use it to locate the activities that apply to your team this quarter.

| TPLC phase | Activities relevant to this guide | Primary artifact | | --- | --- | --- | | Concept / design | Architecture diagram, trust boundaries, initial STRIDE pass | Threat model v0 | | Development | SBOM in CI, SAST/DAST, secure-coding evidence | SBOM (CycloneDX/SPDX) | | V&V | Independent pen test, fuzz, vuln scan, SPDF documentation | SPDF + pen-test report | | Submission | eSTAR cyber package, labelling, CVD plan | eSTAR section + CVD plan | | Post-market | Vuln monitoring, SBOM refresh, re-test, CVD operations | Annual cyber report |

Step-by-step playbook

1. Confirm Section 524B applicability. Apply the three-part test (software + connectivity + exploitable characteristic). Most software-enabled Class II devices meet it. The cost of getting this wrong is a Refusal-to-Accept - clarify it now.

2. Inventory existing cyber artifacts. Pull what you have: architecture diagram, SBOM, any threat model, prior pen tests, risk file. Most teams have more than they think - what they lack is traceability between artifacts.

3. Map artifacts to the Feb 3 2026 final guidance. For every artifact the guidance expects (SBOM, threat model, risk assessment, security testing, SPDF, labelling, CVD), note 'have', 'partial', or 'gap'. The gap list is your scope.

4. Sequence the gap list against TPLC phase. Don't try to fix everything in parallel. Sequence by what unblocks the next phase gate, not by what is easiest. The threat model usually has to land first because everything else traces to it.

5. Stand up post-market processes before they are needed. Post-market cyber is not a launch-day activity

- it is a day-zero activity that has to be operating before the first sale, with evidence reviewers can audit.

Worked example - a typical Class II MedTech

Setup

A typical Class II software-enabled device team: 8-15 engineers, mid-development, planned 510(k) submission in 4-6 months, no prior FDA cyber experience on the team.

Walk-through

We apply the operating framework. Architecture and SBOM exist; threat model is informal; pen test was done a year ago against an older build; SPDF documentation does not exist. We rebuild the threat model against the current architecture, regenerate SBOM in CI, schedule independent pen testing for the V&V build, and draft the SPDF in parallel. Every cyber control is linked to an existing ISO 14971 hazard.

Outcome

Submission ships on the original date. The eSTAR clears the RTA screen on first review. The team carries the operating model forward as the QMS-default for every subsequent product line.

Standards crosswalk

The work this guide describes does not live inside any single standard. The crosswalk below shows how each artifact ties to the regulatory text and the consensus standards a reviewer expects you to cite. Use it when you are asked, mid-review, 'where does this come from?'

| Artifact | Primary regulatory anchor | Consensus standard | | --- | --- | --- | | SBOM | Section 524B(b)(3) | NTIA / CycloneDX / SPDX | | Threat model | Feb 3 2026 final guidance §V | AAMI TIR57, STRIDE | | Cyber risk assessment | Feb 3 2026 final guidance §V | AAMI TIR57 + ISO 14971 | | Security testing | Feb 3 2026 final guidance §VI | AAMI SW96, IEC 62443-4-1 | | SPDF documentation | Feb 3 2026 final guidance §IV | IEC 62443-4-1, AAMI SW96 | | Cybersecurity labelling | Section 524B(b)(2)(A) | Feb 3 2026 final guidance §VII | | CVD plan | Section 524B(b)(1) | ISO/IEC 29147 + 30111 |

HOW TO USE THIS IN A REVIEW MEETING

When a reviewer or an internal stakeholder challenges an artifact, do not defend it on its own merits - point to the row in this crosswalk. Every artifact in your eSTAR cyber package should sit on top of both a statutory anchor and a consensus standard.

Reviewer lens - what FDA actually looks for

Reviewers do not score artifacts on weight or polish. They score them on traceability, independence, and whether the cyber story matches the safety story. The bullets below are what an experienced reviewer scans for first.

- Traceability - every cyber control must trace back to a specific hazard in the ISO 14971 risk file.
- Independence - the engineer who built the system did not also test it.

- Currency - the SBOM and threat model reflect the build that is actually being submitted, not last sprint's.
- Coverage - the threat model addresses every trust boundary shown on the architecture diagram.
- Disclosure - a coordinated vulnerability disclosure (CVD) plan exists, with a published intake path.
- Labelling - end-user cybersecurity content (intended use, controls, residual risks) is in the IFU.

What 'evidence-grade' looks like

Reviewers are not impressed by length. They are impressed by traceability. The four characteristics below are what separates an evidence-grade cyber package from one that draws an Additional Information letter.

1. Versioned Every artifact carries a version, a date, and a commit/build identifier. The SBOM in your eSTAR matches the build under review, not last sprint's.

2. Linked Threat-model entries link to risk-file hazards. Pen-test findings link to threat-model entries. Mitigations link to design controls. The reviewer can walk any chain end-to-end without leaving the package.

3. Independent Testing was performed by an engineer who did not write the code. The org chart in the SPDF documentation makes that visible.

4. Operational Post-market processes (vuln monitoring, CVD intake, patch validation) exist as live processes with named owners - not as procedures that will be 'stood up at launch'.

Pitfalls we see in the wild

- Treating cybersecurity as a pre-submission task instead of a TPLC obligation.
- Assuming a single pen test satisfies the eSTAR cyber package - it does not.
- Letting developers run their own pen test, then losing the independence argument with the reviewer.
- SBOM generated once, never refreshed before submission, missing the build that ships.
- Threat model and risk file maintained in different tools, with no link between cyber controls and ISO 14971 hazards.
- Coordinated vulnerability disclosure deferred until after clearance - then scrambled together post-launch.

Frequently asked questions

How does this fit Section 524B? Section 524B of the FD&C Act, in force since March 29, 2023, makes cybersecurity content a refusal-to-accept item for any 'cyber device'. The Feb 3, 2026 final guidance, Cybersecurity in Medical

Devices, defines what that content looks like in practice: SBOM, threat model, risk assessment, security testing evidence, SPDF documentation, labelling, and a coordinated vulnerability disclosure plan.

Everything in this guide is written to land cleanly inside that package.

What if our device isn't a 'cyber device'? The Section 524B test is broad: software + connectivity (even transient, even via a phone) + any exploitable technological characteristic. Most software-enabled Class II devices meet it. Even when they don't, the FDA can still ask for cyber content under its general safety-and-effectiveness authority, and a right-sized threat model is the cheapest insurance you can buy against an Additional Information letter.

Action checklist

Use this checklist to confirm the artifacts and decisions covered in this guide are in place before any premarket conversation.

Section 524B applicability documented. Architecture diagram with all trust boundaries labelled. SBOM generated in CI, in CycloneDX or SPDX format. Threat model (typically STRIDE) covers every trust boundary. Cybersecurity risk assessment linked to ISO 14971 hazards. Independent pen test scheduled or complete on the V&V build. SPDF documentation drafted before eSTAR build starts. CVD intake live before first commercial sale. Post-market vuln monitoring process assigned and documented.

What to do this week

Before any partner conversation, do three things this week: (1) pull the current architecture diagram and confirm every trust boundary is labelled, (2) export the latest SBOM (CycloneDX or SPDX) for the build you intend to submit, and (3) note the TPLC phase you are in. With those three inputs, a good cyber partner can scope a right-sized engagement in 20 minutes - without them, every conversation re-starts from zero.

NEXT STEP

Book a 20-minute discovery call

We'll map your device, your submission timing, and the artifacts FDA expects, and you'll leave with a one-page plan you can share with your team. No deck, no obligation.

(844) 939-4628 (GOAT) ·

go.bluegoatcyber.com/meetings/blue-goat-cyber/discovery-session Scan the QR code to book instantly →

Talk to us

This guide is part of Blue Goat Cyber's MedTech cybersecurity library. To apply it to your device program, book a 30-minute strategy session - no cost, no obligation. Or browse all guides.

Ready to talk through your roadmap?

Book a Strategy Session →

Source guide: vendor-evaluation-grid. For the most current version, visit bluegoatcyber.com/guides/vendor-evaluation-grid.