WHAT FDA ACTUALLY WROTE

Eight Cybersecurity Deficiencies, Taken From the Letters

MTEC Webinar | Wednesday, September 23, 2026 | 1:00 PM ET

Christian Espinosa
Founder and CEO, Blue Goat Cyber

CHRISTIAN ESPINOSA

Founder and CEO
Blue Goat Cyber

THE PERSON AND THE FIRM BEHIND THIS ANALYSIS

CHRISTIAN

U.S. Air Force veteran

Military-grade rigor and discipline, carried into how Blue Goat reads a submission.

Host, Med Device Cyber Podcast

A recurring voice in medical device cybersecurity, working through FDA patterns with the community.

30+ deficiency letters reviewed

Career review experience spans well beyond the ten letters formally analyzed for this talk's ranking.

BLUE GOAT CYBER

SDVOSB

Service-Disabled Veteran-Owned Small Business, focused exclusively on medical device cybersecurity and FDA clearance support.

275+ submissions supported

Fixed fee. Deficiencies on our submissions resolved at no extra cost.

Startups to enterprise

Premarket, postmarket and penetration testing for device makers of every size.

"A medical device saved my life in 2022. Now I secure them."

What we'll cover

The basis for this talk

What the analysis is built on, and what it isn't.

How often each one shows up

The ranking, before we go finding by finding.

The eight findings

What the FDA wrote, the root cause, and the artifact that closes it.

How to close most of this before FDA sees it

Five checks to run before a submission goes out.

Get help with your own letter

How to reach us if you're holding a deficiency letter right now.

What you'll walk away with

- Recognize the eight FDA cybersecurity findings that account for most deficiency letters, not a generic list, ranked by how often each one actually shows up.
- Know the specific artifact that closes each one, not just the general principle FDA is checking for.
- Leave with a five-point checklist to run against your own submission before it goes out the door.
- Know exactly how to get direct help if you're holding a deficiency letter right now.

The basis for this talk

- A frequency count across FDA Additional Information (AI) letters Blue Goat has reviewed in full.
- The corpus spans software-only devices, AI-enabled devices, cloud and on-premise deployments, capital equipment, wearables, and vital signs monitors, across both CDRH and CBER.
- The ranking below is the percentage of our sample letters that raised each issue, not a percentage of all submissions industry-wide, and not a claim about any single client or device.
- Client names, device names, and submission numbers are excluded from this material.

Four categories account for most of what FDA sends back: SBOM, control traceability, labeling, and testing. A pre-release check against those four catches the majority of what would otherwise come back as a deficiency.

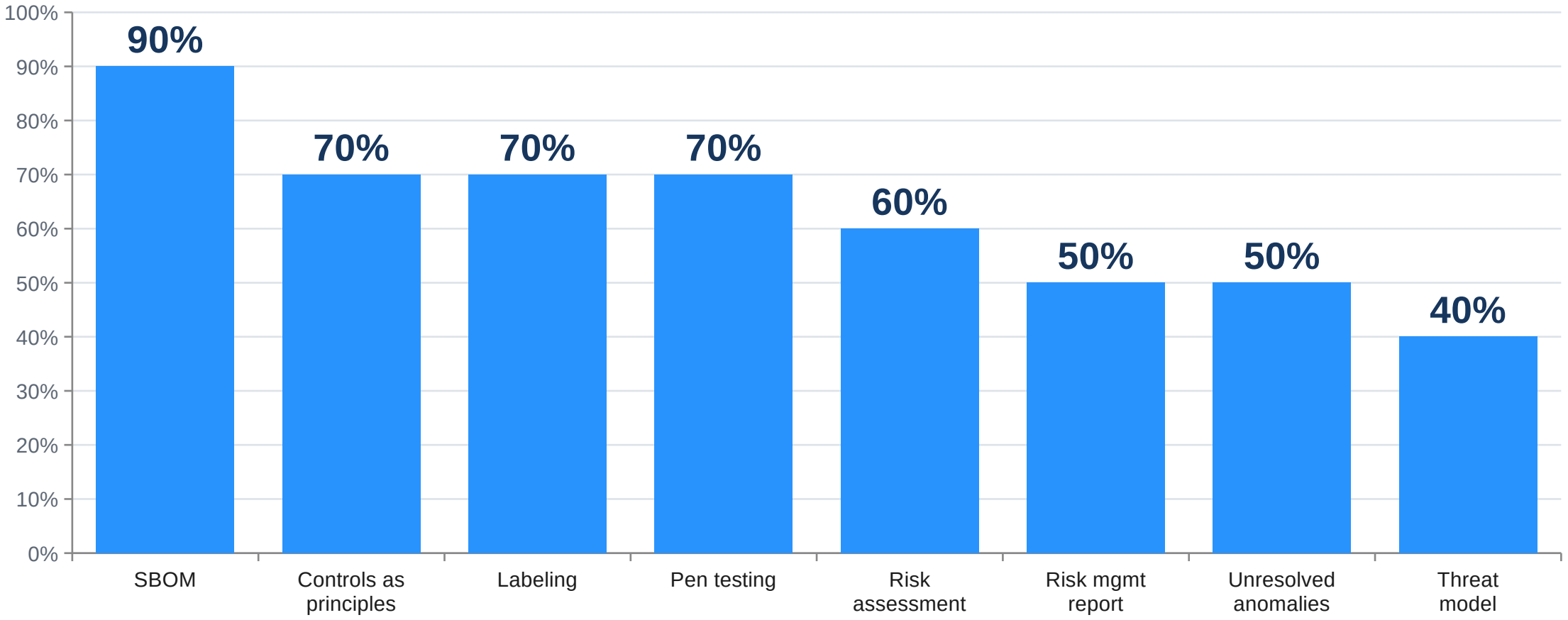
Before I show you the data

Which of these do you think shows up most often? Drop your guess in chat.

- SBOM
- Controls as principles
- Labeling
- Pen testing
- Risk assessment
- Risk mgmt report
- Unresolved anomalies
- Threat model

How often each one shows up

Percentage of our sample letters that raised each finding



The same eight findings, in roughly this order, recur across Christian's broader career review of 30+ FDA cybersecurity letters.

1

SBOM

Most common finding by a wide margin

WHAT THE FDA WROTE (PATTERN)

The SBOM does not carry the data FDA asked for. It is rarely that an SBOM is missing outright.

ROOT CAUSE IN THE SUBMISSION

Support-status tiers missing, end-of-support dates missing or undated, format not machine-readable (a PDF SBOM does not satisfy the requirement), NTIA minimum elements missing, and no per-component vulnerability mapping to NVD or the CISA Known Exploited Vulnerabilities catalog.

ILLUSTRATIVE EXAMPLE

One letter named components 10 and 16 years past end-of-life, with CVE scores of 7.5 and 7.8 and no compensating-control justification.

THE ARTIFACT THAT CLOSES IT

A machine-readable SBOM (SPDX or CycloneDX) with three-tier support status per component, dated end-of-support, NTIA minimum elements, and a per-component vulnerability assessment against NVD and CISA KEV.

What a closed SBOM entry actually looks like

Illustrative example, not real device data

Component	Support status	End-of-support	Format	Vulnerability check
OpenSSL 3.0.12	Actively maintained	N/A	SPDX, JSON	No known CVEs (NVD, CISA KEV checked)
libpng 1.6.37	No longer maintained	2023-01-15	SPDX, JSON	CVE-2023-XXXXX, CVSS 7.5
Legacy RTOS module	Abandoned	2019-06-01	SPDX, JSON	***Not assessed, flagged as a gap***

Notice the third row. A machine-readable SBOM doesn't hide the gap, it names it. “Not assessed” with a flag is defensible. A blank cell, or an SBOM that only lists the top-level package and omits this module entirely, is what actually draws the finding.

2

Security controls written as principles

Largest category by raw count of individual findings

WHAT THE FDA WROTE (PATTERN)

Only a high-level description was provided, so the adequacy of the control cannot be determined.

ROOT CAUSE IN THE SUBMISSION

Controls stated as goals, not specification-level detail: passwords required but no password policy stated, TLS 1.2 named but not the cipher suites, ECDSA cited but not the curve or hash function.

ILLUSTRATIVE EXAMPLE

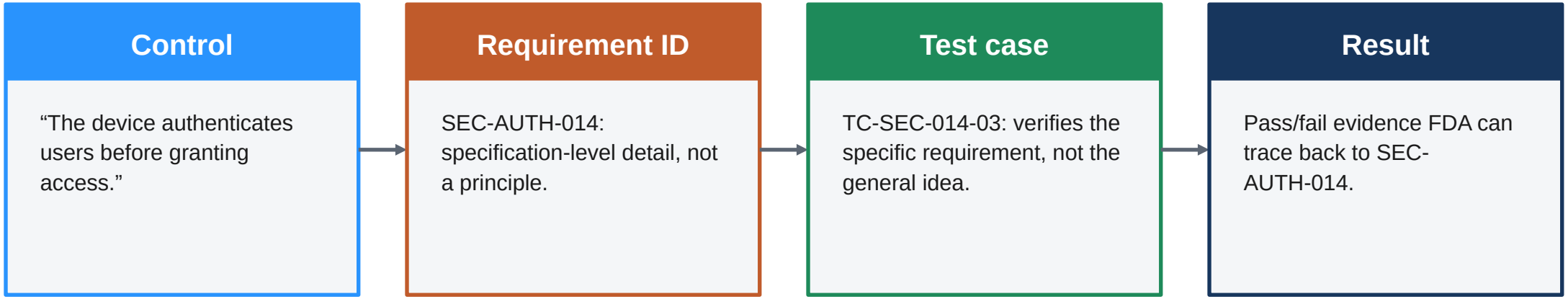
One letter raised this same finding nine separate times against nine different controls in a single submission.

THE ARTIFACT THAT CLOSES IT

Every control given a unique requirement identifier at specification level, traceable to the specific test case that verified it.

What traceability actually looks like

The chain FDA expects behind every control, illustrative example



A principle (“the device authenticates users”) can't be tested. A requirement with an ID can. That's the entire gap FDA is pointing at in this finding.

3

Cybersecurity labeling

Same missing-element checklist recurs almost verbatim

WHAT THE FDA WROTE (PATTERN)

The submission's labeling plan is not labeling. Does the content actually reach the customer?

ROOT CAUSE IN THE SUBMISSION

A recurring, near-identical list of missing elements: network ports and interfaces, secure configuration of shipped devices, update notification, anomalous-condition behavior, backup and restore, forensic evidence capture, a machine-readable SBOM for users, and end-of-life/decommissioning.

ILLUSTRATIVE EXAMPLE

One letter enumerated fourteen separate missing labeling elements against a single device.

THE ARTIFACT THAT CLOSES IT

A labeling checklist mapped one-to-one against FDA's expected element list, verified against the customer-facing document itself, not the submission narrative describing it.

4

Security and penetration testing

Richest category in the corpus

WHAT THE FDA WROTE (PATTERN)

Vulnerability scanning is not a substitute for penetration testing. A scan identifies known vulnerabilities, a penetration test demonstrates impact.

ROOT CAUSE IN THE SUBMISSION

Scope gaps (a bridging component or local agent left out of scope), risk-based justifications for skipping testing altogether, and missing independence between testers and the design team.

ILLUSTRATIVE EXAMPLE

One letter cited a local agent bridging the browser to physical scales and label printers that was left out of test scope entirely.

THE ARTIFACT THAT CLOSES IT

A full-system-scope penetration test report carrying all five required elements: tester independence and expertise, scope, duration, methods, and results and findings.

5

Cybersecurity risk assessment

A methodology problem more often than a missing document

WHAT THE FDA WROTE (PATTERN)

No stated methodology or acceptance criteria; impact written as a system effect rather than patient harm.

ROOT CAUSE IN THE SUBMISSION

Exploitability claimed without defining it against attack vector, complexity, privileges, and user interaction; risk identifiers that don't match across tables; no traceability from a risk to a requirement identifier.

ILLUSTRATIVE EXAMPLE

One letter named full system control rated Medium impact as a specific case where impact was written as a system effect, not a patient-harm outcome.

THE ARTIFACT THAT CLOSES IT

A documented risk methodology (CVSS, AAMI TIR57, or ANSI AAMI SW96) with matched risk IDs, pre- and post-mitigation levels both shown, and a cross-reference against NVD and CISA KEV.

The two risk matrices

From Blue Goat's risk management methodology (ANSI/AAMI SW96, ANSI/AAMI/ISO 14971)

SW96 SECURITY RISK MATRIX

Exploitability × Security Impact

	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

↑ *Exploitability* *Security impact* →

ISO 14971 SAFETY RISK MATRIX

Exploitability × Severity of Harm

	Negligible	Minor	Serious	Critical	Catastrophic
High	Medium	High	High	Very High	Very High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Low	Medium	Medium

↑ *Exploitability* *Severity of harm* →

Same exploitability axis, two different second factors. Security impact (device confidentiality, integrity, availability) drives the SW96 matrix; severity of patient harm, fixed by the ISO 14971 safety file, drives the safety matrix. A catastrophic harm never scores below Medium, even at Low exploitability; a negligible harm never rises above Medium, however exploitable.

The SW96 bridge: how one threat flows through

Exploitability is scored once and feeds both matrices; only the safety-side result transfers to ISO 14971

EXPLOITABILITY (CVSS v4.0)

Substitutes for probability, shared by both formulas below

ISO 14971 · SAFETY RISK
Severity of Harm × Exploitability

Severity of harm: ISO 14971's scale, Negligible to Catastrophic. Fixed by the device's safety assessment. Does not change when a security control is applied.

SW96 · SECURITY RISK
Security Impact × Exploitability

Security impact: effect on the device's own confidentiality, integrity, and availability. Low, Medium, or High. Not a patient-harm judgment, used only on this matrix.

GATE: could exploitation affect patient safety?

If yes, the threat is also scored on the safety matrix above.

Stays on the security track (its own action table). Not transferred below unless the gate above is also met.

ISO 14971 RISK MANAGEMENT FILE

Residual patient-harm risk transferred in · combined benefit-risk determination · a security-only finding with no safety gate stays on the security track and is not transferred here.

6

Cybersecurity risk management report

About half of letters reviewed

WHAT THE FDA WROTE (PATTERN)

The report points at other documents instead of standing on its own.

ROOT CAUSE IN THE SUBMISSION

Summarizing the scope of each supporting document, instead of summarizing its outcome and the residual risk conclusion.

ILLUSTRATIVE EXAMPLE

Several letters flagged that no security risk management process ran parallel to the safety risk process at all.

THE ARTIFACT THAT CLOSES IT

One report that states risk evaluation methods, the residual risk conclusion, and the mitigation activities actually performed, with traceability across the threat model, risk assessment, SBOM, and testing.

7

Unresolved anomalies

Consistently misread by submission teams

WHAT THE FDA WROTE (PATTERN)

Answering that there are no unresolved cybersecurity issues is not responsive. FDA means known software defects deliberately left in the product.

ROOT CAUSE IN THE SUBMISSION

Functional bugs listed with no security-impact assessment attached; anomalies assessed in isolation rather than against the risk management file.

ILLUSTRATIVE EXAMPLE

The mirror-image mistake shows up repeatedly: functional bugs listed with no security-impact assessment attached at all.

THE ARTIFACT THAT CLOSES IT

An anomaly-by-anomaly write-up: description, how it was found, root cause, impact on safety and effectiveness, and a risk-based rationale for not fixing it.

8

Threat model

Usually incomplete at the edges, rarely absent

WHAT THE FDA WROTE (PATTERN)

The assumption that the network is hostile is not stated.

ROOT CAUSE IN THE SUBMISSION

Supply chain, decommissioning, and end-to-end infrastructure left out; for AI-enabled devices, data poisoning, model inversion, and model evasion not identified.

ILLUSTRATIVE EXAMPLE

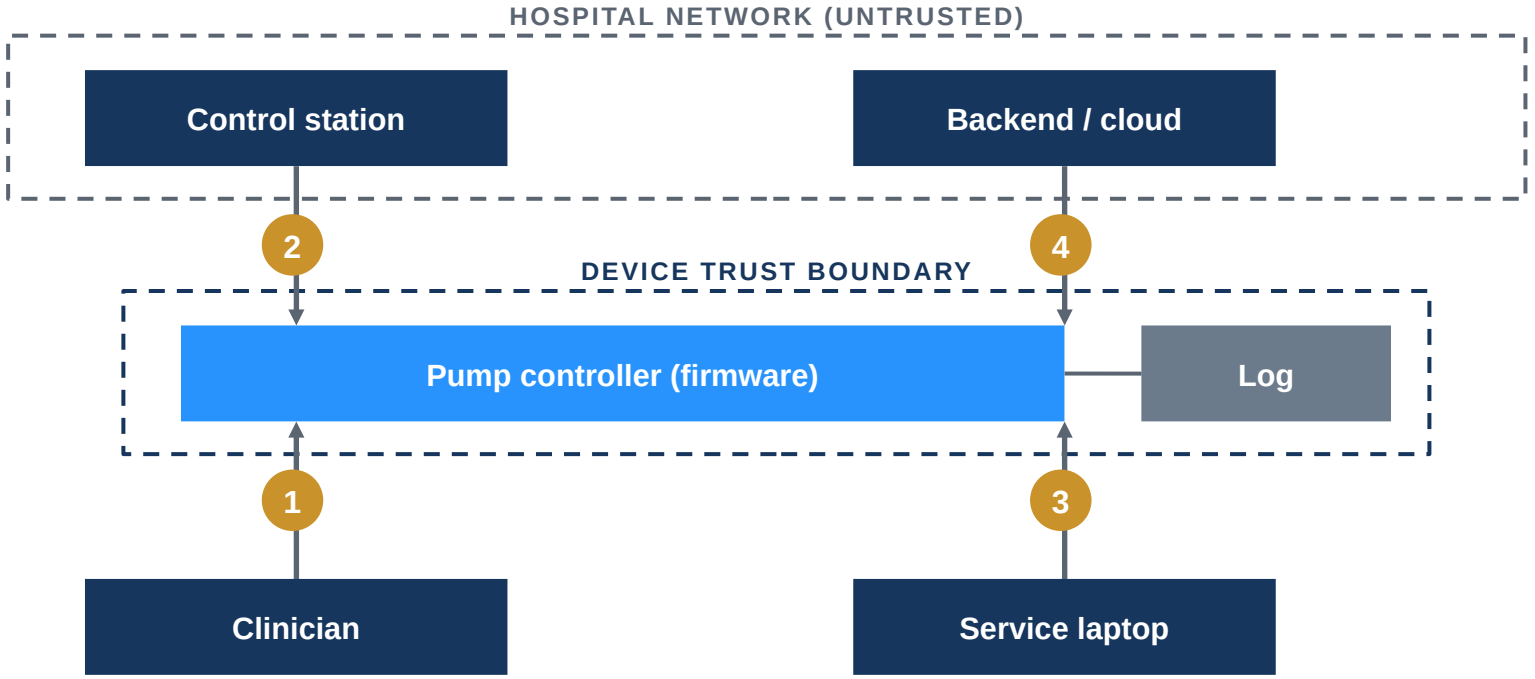
Across the AI-enabled devices in the set, data poisoning, model inversion, and model evasion were consistently absent from the threat model.

THE ARTIFACT THAT CLOSES IT

A threat model that states the hostile-network assumption explicitly, covers the full device lifecycle, and, for AI-enabled devices, names AI-specific threats, with pre- and post-mitigation scores carried through to the risk assessment.

Modeling the system: a data flow diagram

A wireless infusion pump in DFD3 notation, illustrative example from Blue Goat's methodology



EP	Interface	Description	Assets reachable
1	Touchscreen	Local operator input at the bedside	Dose settings, device configuration
2	Wi-Fi control channel	Wireless link to the control station	Infusion commands, device status
3	USB service port	Wired service and firmware-update port	Firmware, configuration, logs
4	Backend API	Network link to the backend / cloud service	Infusion orders, telemetry, PHI

How to close most of this before FDA sees it

Five checks that catch the majority of what would otherwise come back as a deficiency

Gate the SBOM before it ships

No package ships without three-tier support status, dated end-of-support per component, a machine-readable format, NTIA minimum elements, and a per-component vulnerability assessment against NVD and CISA KEV.

Treat labeling as a checklist, not prose

The same missing-element list recurs almost verbatim across letters. Map it one to one instead of describing it in narrative form.

Trace every control to a test case

Every control gets a unique requirement identifier, traceable to the test case that verified it, before the independent reviewer gate.

Confirm full-system penetration test scope

Bridging components and local agents included, and all five required report elements present: independence, scope, duration, methods, results and findings.

Grep for likelihood language before release

Search every submission for “likelihood,” “probability,” and “unlikely.” FDA assesses cybersecurity risk on exploitability, not likelihood.

The eight, at a glance

1 SBOM 

2 Security controls written as principles 

3 Cybersecurity labeling 

4 Security and penetration testing 

5 Cybersecurity risk assessment 

6 Cybersecurity risk management report 

7 Unresolved anomalies 

8 Threat model 

IF YOU REMEMBER ONE THING

SBOM. Traceability. Labeling. Testing.

Four categories account for most of what FDA sends back. A pre-release check against those four catches the majority of what would otherwise come back as a deficiency.

Notice the thread running through today's examples: a control traced to a requirement ID, a threat traced through pre- and post-mitigation scores, a risk traced to a test case. That's not three separate topics. Traceability is the spine of the deliverable set, and a gap in it runs through most of the findings above.

Three things before we go

Have a deficiency letter? We can help.

Send it to christian@bluegoatcyber.com, anonymized if you'd like. We'll take a look and follow up directly.

Take the deliverables map

Blue Goat's map of the 18 premarket cybersecurity deliverables against the current final guidance and eSTAR v7.0: bluegoatcyber.com/guides/fda-premarket-cybersecurity-deliverables-estar-map

Book a discovery session

Scan to grab time on our calendar, or reach the team directly at info@bluegoatcyber.com.

Christian Espinosa · Founder and CEO, Blue Goat Cyber · christian@bluegoatcyber.com · info@bluegoatcyber.com