



Top FDA Cybersecurity Deficiencies

What 30+ FDA letters raised most

Actual report frequencies. Anonymized actual deficiencies.

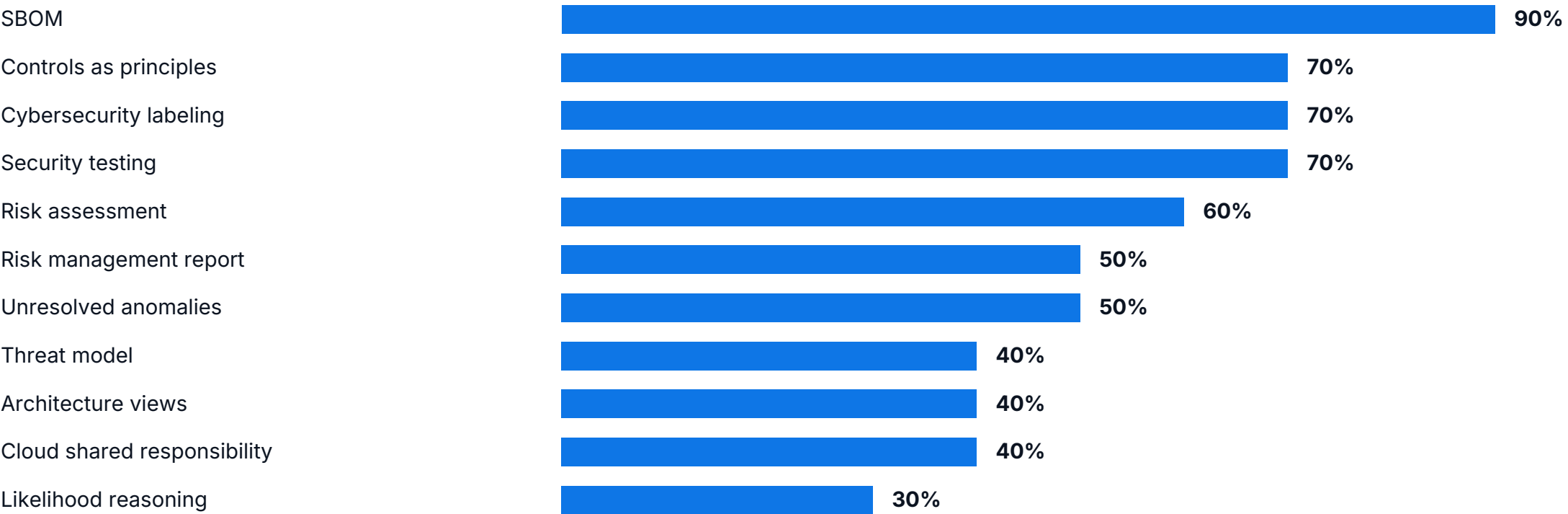
One slide per category, with actual reviewer concerns and the same security and safety matrices as the client risk deck.

Documentation gaps do not establish a vulnerability vector or patient-harm severity. Actual deficiencies are not rated without device-specific evidence.

Actual-deficiency revision | 23 October 2026



How often each issue appeared



Share of more than 30 letters reviewed, through August 2026. Each issue counted once per letter; categories overlap. Not rates across all submissions or exact counts.



Frequency is not risk

OBSERVED REPORT DATA

Percentages describe issues raised in reviewed letters. They do not measure exploitability, patient-harm severity, or a category's risk.

ACTUAL DEFICIENCIES

Concerns are anonymized paraphrases of the source report. Its aggregate descriptions do not supply validated CVSS inputs or manufacturer harm severities.

SCORING METHOD

STRIDE classifies, never scores. AV, PR, and UI determine matrix exploitability; security impact is the highest of the six CIA metrics.

DECISION BOUNDARY

The CVSS v4.0 base score is recorded separately, not used in either matrix. Safety needs manufacturer hazard evidence; acceptance remains manufacturer-owned.



Security matrix | every finding

Exploitability ↑	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

Security impact → Highest of VC, VI, VA, SC, SI, SA: H = High; L = Medium; all N = Low.

Risk is a table lookup, not score multiplication. Highest risk is upper-right.



Safety matrix | patient-affecting findings

Exploitability ↑	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

Manufacturer-assigned harm severity → Negligible through Catastrophic.

PHI disclosure alone does not establish patient harm. An unclear pathway needs manufacturer review.

01 | SBOM

90% of reviewed letters

Actual deficiency | anonymized paraphrase

SBOMs lacked component-level support and end-of-support information, identifiers, dependencies, or vulnerability mapping. Some inventories omitted the deployment environment or listed no findings without enumerating components.

Source: BGC-ANL-260828, page 2

Security risk: Not scored

Validated exploitability and CIA-impact inputs are not supplied in the aggregate report.

Safety risk: Not scored

Patient pathway and manufacturer-assigned harm severity need device-specific evidence. This is not a finding of no patient risk.

Evidence to check: Reconcile shipped components and deployment scope; document support, vulnerability applicability, and evidence.

An FDA reviewer concern is not a universal requirement or an automatic risk rating.

02 | Controls as principles

70% of reviewed letters

Actual deficiency | anonymized paraphrase

Controls were described without testable specifications: password rules, TLS cipher suites, or signature curve and hash details were missing. Requirement identifiers and verification traceability were incomplete.

Source: BGC-ANL-260828, page 2

Security risk: Not scored

Validated exploitability and CIA-impact inputs are not supplied in the aggregate report.

Safety risk: Not scored

Patient pathway and manufacturer-assigned harm severity need device-specific evidence. This is not a finding of no patient risk.

Evidence to check: Define testable control requirements, link verification evidence, and retest failed controls.

An FDA reviewer concern is not a universal requirement or an automatic risk rating.

03 | Cybersecurity labeling

70% of reviewed letters

Actual deficiency | anonymized paraphrase

User-facing instructions omitted secure configuration, ports, credential reset, updates, recovery, logging, or support information. A submission labeling plan did not establish delivery of the information to users.

Source: BGC-ANL-260828, page 2

Security risk: Not scored

Validated exploitability and CIA-impact inputs are not supplied in the aggregate report.

Safety risk: Not scored

Patient pathway and manufacturer-assigned harm severity need device-specific evidence. This is not a finding of no patient risk.

Evidence to check: Confirm the delivered labeling explains configuration, updates, recovery, logging, and support responsibilities.

An FDA reviewer concern is not a universal requirement or an automatic risk rating.

04 | Security testing

70% of reviewed letters

Actual deficiency | anonymized paraphrase

Vulnerability scanning was offered instead of penetration testing. A hosting-provider responsibility model was used to justify omitting application testing. Other concerns included incomplete scope and an unaddressed finding the manufacturer's report rated medium.

Source: BGC-ANL-260828, page 3

Security risk: Not scored

Validated exploitability and CIA-impact inputs are not supplied in the aggregate report.

Safety risk: Not scored

Patient pathway and manufacturer-assigned harm severity need device-specific evidence. This is not a finding of no patient risk.

Evidence to check: Test device-specific application and system boundaries; document tester independence, methods, findings, and retest evidence.

An FDA reviewer concern is not a universal requirement or an automatic risk rating.

05 | Risk assessment

60% of reviewed letters

Actual deficiency | anonymized paraphrase

Risk methodology and exploitability levels were undefined. Initial and residual assessments, implemented mitigation evidence, patient-harm analysis, or consistent traceability were missing.

Source: BGC-ANL-260828, page 3

Security risk: Not scored

Validated exploitability and CIA-impact inputs are not supplied in the aggregate report.

Safety risk: Not scored

Patient pathway and manufacturer-assigned harm severity need device-specific evidence. This is not a finding of no patient risk.

Evidence to check: Record the method, assessed inputs, manufacturer hazard evidence, implemented controls, and residual decisions.

An FDA reviewer concern is not a universal requirement or an automatic risk rating.

06 | Risk management report

50% of reviewed letters

Actual deficiency | anonymized paraphrase

Reports referenced supporting documents without summarizing their results, performed mitigations, or residual-risk conclusions. Cross-document traceability was incomplete.

Source: BGC-ANL-260828, page 4

Security risk: Not scored

Validated exploitability and CIA-impact inputs are not supplied in the aggregate report.

Safety risk: Not scored

Patient pathway and manufacturer-assigned harm severity need device-specific evidence. This is not a finding of no patient risk.

Evidence to check: Summarize actual assessment and mitigation outcomes and trace them to supporting records.

An FDA reviewer concern is not a universal requirement or an automatic risk rating.

07 | Unresolved anomalies

50% of reviewed letters

Actual deficiency | anonymized paraphrase

Statements of no cybersecurity issues replaced evaluation of retained software defects. Listed anomalies lacked security assessment, safety/effectiveness evaluation, root cause, or deferral rationale.

Source: BGC-ANL-260828, page 4

Security risk: Not scored

Validated exploitability and CIA-impact inputs are not supplied in the aggregate report.

Safety risk: Not scored

Patient pathway and manufacturer-assigned harm severity need device-specific evidence. This is not a finding of no patient risk.

Evidence to check: Assess retained anomalies and document their impact, investigation, disposition, and risk-file links.

An FDA reviewer concern is not a universal requirement or an automatic risk rating.

08 | Threat model

40% of reviewed letters

Actual deficiency | anonymized paraphrase

Threat models omitted hostile-network assumptions, lifecycle phases, or infrastructure boundaries. Some omitted AI-specific threats or failed to carry threats into the risk assessment.

Source: BGC-ANL-260828, page 4

Security risk: Not scored

Validated exploitability and CIA-impact inputs are not supplied in the aggregate report.

Safety risk: Not scored

Patient pathway and manufacturer-assigned harm severity need device-specific evidence. This is not a finding of no patient risk.

Evidence to check: Cover applicable lifecycle and infrastructure boundaries and trace threats into evidence-based risk assessment.

An FDA reviewer concern is not a universal requirement or an automatic risk rating.

09 | Architecture views

40% of reviewed letters

Actual deficiency | anonymized paraphrase

A single diagram and prose left relevant architecture information incomplete. Trust boundaries, authentication/session details, operational states, or SBOM traceability were missing; excluding multi-patient harm lacked supporting analysis.

Source: BGC-ANL-260828, page 4

Security risk: Not scored

Validated exploitability and CIA-impact inputs are not supplied in the aggregate report.

Safety risk: Not scored

Patient pathway and manufacturer-assigned harm severity need device-specific evidence. This is not a finding of no patient risk.

Evidence to check: Provide applicable architecture views and justify scope with supporting risk analysis.

An FDA reviewer concern is not a universal requirement or an automatic risk rating.

10 | Cloud shared responsibility

40% of reviewed letters

Actual deficiency | anonymized paraphrase

Cloud service models and the manufacturer/provider split of control ownership were undocumented. Supplier assurance and testing evidence were incomplete, cloud-unavailability procedures were missing, or cloud and on-premise configurations were not assessed separately.

Source: BGC-ANL-260828, page 5

Evidence to check: Assign control ownership; document supplier evidence, application testing, outage procedures, and configuration-specific controls and risks.

An FDA reviewer concern is not a universal requirement or an automatic risk rating.

Security risk: Not scored

Validated exploitability and CIA-impact inputs are not supplied in the aggregate report.

Safety risk: Not scored

Patient pathway and manufacturer-assigned harm severity need device-specific evidence. This is not a finding of no patient risk.

11 | Likelihood reasoning

30% of reviewed letters

Actual deficiency | anonymized paraphrase

Attack probability, intentions, physical barriers, or controlled environments were substituted for exploitability analysis without addressing actual attack paths. A low physical-vector CVSS label was treated as the risk conclusion.

Source: BGC-ANL-260828, page 5

Security risk: Not scored

Validated exploitability and CIA-impact inputs are not supplied in the aggregate report.

Safety risk: Not scored

Patient pathway and manufacturer-assigned harm severity need device-specific evidence. This is not a finding of no patient risk.

Evidence to check: Assess defined exploitability factors and control evidence; do not substitute unlikely-attack arguments for risk assessment.

An FDA reviewer concern is not a universal requirement or an automatic risk rating.



Verified controls change the inputs

A documented responsibility split is evidence, not a risk score.

Cloud-provider controls do not replace device-specific application testing. Assign control ownership, document supplier evidence, and assess cloud failure paths.

Where a confirmed vulnerability exists, record its initial CVSS inputs and manufacturer hazard evidence. Verify implemented controls before calculating residual risk.

The source report does not provide before-and-after vectors. No claimed Critical-to-Medium reduction is carried into this actual-deficiency deck.

The manufacturer owns risk decisions

CONTROL STRATEGIES

Eliminate, mitigate, accept, then transfer as a justified last resort.

SECURITY PRIORITIES

Low: record. Medium: track remediation or document acceptance rationale. High: fix before release or on a defined postmarket timeline. Critical: fix immediately.

SAFETY REVIEW

Connect findings to hazard analysis. Assess initial risk, verified controls, residual risk, and benefit-risk reasoning where applicable.

CHANGED EVIDENCE

KEV records known exploitation (E:A); it does not automatically change matrix exploitability. Re-score when evidence changes AV, PR, UI, or impact.

These are BGC conventions, not mandated FDA ratings or deadlines. A score is not risk acceptance.



Sources and presentation limits

Report data

Blue Goat Cyber. (2026). Top FDA Cybersecurity Deficiencies: What 30+ FDA Letters Raised Most. <https://bluegoatcyber.com/research/fda-medical-device-cybersecurity-deficiencies-2026>

More than 30 letters reviewed through August 2026; selected BGC engagements, not a random sample. Percentages are reported aggregates, not exact counts. Categories are BGC groupings.

Scoring basis

BGC-RISK-GUIDE-EXEC-260924 Rev H and BGC-GUIDE-RISK-001 Rev P: exploitability, security/safety matrices, patient pathway, and control review. CVSS v4.0 vector and base score are separate records.

The February 3, 2026 FDA premarket cybersecurity guidance is nonbinding guidance. Reviewer requests in individual letters are not universal legal requirements.

Present with Blue Goat Cyber attribution. Anonymized paraphrases omit identifiers; distribution still requires clearance of confidential or open matters.