GUIDANCE NOTE

Integrating Premarket Cybersecurity Deliverables Into Your Quality Management System

How the FDA premarket cybersecurity artifacts Blue Goat produces enter, and are governed by, your ISO 13485 / QMSR quality system, as controlled records you own rather than documents that sit outside your file.

Prepared by	Blue Goat Cyber · bluegoatcyber.com · info@bluegoatcyber.com · (844) 939-4628
Document ID	BGC-GUIDE-QMS-001
Version	Rev A, 260723
Audience	Client Quality and Regulatory Affairs teams evaluating how outsourced premarket cybersecurity deliverables integrate into an established QMS
Scope	US QMSR (21 CFR Part 820, effective Feb 2, 2026) incorporating ISO 13485:2016 by reference; FDA premarket cybersecurity guidance of Feb 3, 2026. EU MDR and IEC 62304 noted where relevant.
Status	Informational. Not regulatory or legal advice; not a guarantee of clearance.

The short answer

These deliverables are not a parallel body of work that sits beside your quality system. They *are* quality-system outputs. The FDA guidance that governs them is titled *"Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions."* Every artifact Blue Goat authors is designed to drop into a specific home in your QMS (your design history file, your risk management file, your purchasing records, your labeling) as a version-controlled record that you own and that an auditor can trace. This note shows exactly where each one lands.

1. Why this question comes up, and the reframe

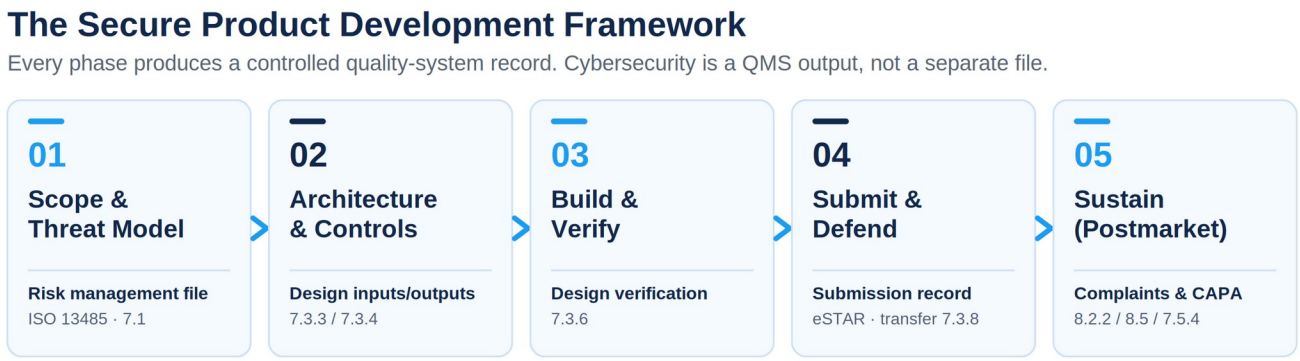
Quality and regulatory teams are right to scrutinize anything that touches the design history file. The concern usually takes one of two forms. The first is that a specialist firm's deliverables will arrive as a separate stack of PDFs that live outside the quality system: not under document control, not traceable in the risk management file, and awkward to defend in an audit or an FDA review.

The second is subtler, and it is the one mature quality teams tend to raise: a premarket submission is a point-in-time snapshot, so how do you know the cybersecurity work runs on the same repeatable system you have to operate for the life of the device, rather than a one-off package you cannot reproduce or maintain? If the method behind the submission is not something your quality system can carry forward, a clearance today does little to help you manage the device tomorrow.

Both worries rest on a premise that the current FDA framework has retired. Cybersecurity is no longer a bolt-on to the submission; it is an output of the quality system itself. The submission is a snapshot drawn from a living system, not the system itself, and because the deliverables are authored as your controlled records, the method and the evidence behind them persist and repeat through updates, design changes, and postmarket, for the life of the device.

The controlling guidance, issued February 3, 2026, is titled *Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions*. FDA's own words: documentation outputs "related to the ongoing requirements of the QMSR may be one source of documentation to include as part of the premarket submission," and the guidance explains "how the QMSR can be leveraged to demonstrate these performance outputs." In other words, the artifacts are meant to be QMS records first and submission attachments second.

The framework makes the point visually. Every phase of secure product development produces a record that already belongs to your quality system:



So the integration question has a clean answer: these deliverables do not need to be forced into your QMS after the fact, because they are authored as QMS records to begin with. What follows shows the governing framework, then maps every deliverable to its exact home.

Scope note: this guidance covers how the premarket cybersecurity deliverables integrate into your quality management system. The methodology behind the cybersecurity risk assessment, including how security risk is evaluated and bridged to patient-safety risk, is addressed in a separate Blue Goat note.

2. The governing framework

On February 2, 2026, FDA's final rule amending 21 CFR Part 820 took effect. The revised Part 820, the **Quality Management System Regulation (QMSR)**, incorporates the 2016 edition of ISO 13485 by reference. For a US medical device manufacturer, ISO 13485:2016 and the QMSR are now effectively one framework, and ISO 13485 threads risk management through its requirements. The QMSR keeps ISO 13485 as the core of the quality system and retains only a few FDA-specific sections on top of it, notably §820.35 (control of records) and §820.45 (device labeling and packaging); the former standalone design-controls section, §820.30, is now satisfied through ISO 13485 Clause 7.3.

Three anchor points in that framework carry almost the entire cybersecurity file:

- **Design and development, ISO 13485 Clause 7.3 (incorporated by QMSR §820.10).** Design inputs, outputs, review, verification, validation, transfer, and change control. The home for security requirements, architecture, and testing.
- **Risk management, ISO 13485 Clause 7.1 with ISO 14971.** The home for the threat model, the cybersecurity risk assessment, and residual-risk decisions.
- **Measurement, analysis and improvement, Clause 8 (complaints 8.2.2, CAPA 8.5, servicing 7.5.4).** The home for the postmarket management plan and coordinated disclosure.

FDA ties these together through the **Secure Product Development Framework (SPDF)**, a set of processes that reduce vulnerabilities across the lifecycle and that, in FDA's words, "can be integrated with existing processes for product and software development, risk management, and the quality system at large." An SPDF is one recognized way to satisfy the QMSR. Blue Goat delivers against that framework, which is precisely why the outputs fit your quality system rather than competing with it.

The work is built to the recognized consensus standards a reviewer expects: **ISO 14971, AAMI SW96, AAMI TIR57, IEC 81001-5-1, and IEC 62304**, so the artifacts speak the same language as the rest of your technical file.

3. Deliverable-to-QMS map

Every premarket cybersecurity deliverable has a defined home in an ISO 13485 / QMSR quality system. At a glance, the design history file and the risk management file do most of the work, with purchasing and the device master record picking up the rest:

Every deliverable has a home in your quality system

Design History File (DHF)

- **Security Requirements & Control** Coverage
- **Security Architecture Views**
- **Static Application Security** Testing (SAST)
- **Penetration Test: Plan, Cases,** Report
- **Assessment of Unresolved Anomalies**

Risk Management File

- **Threat Model**
- **Cybersecurity Risk Assessment**
- **Interoperability Risk Assessment**
- **Risk Management Report (umbrella)**

Device Master Record / Purchasing

- **SBOM (statutory)**
- **Component Support & End-of-Support**
- **MDS2**
- **Cybersecurity & Interoperability** Labeling

Traceability Matrix: carried by the Risk Management Report
Threat → **Control** → **Test** → **Residual risk**

The spine an auditor follows, filed in your risk management file

The table states the home, the governing clause, and the role for each of the eighteen deliverables. Items marked statutory are required under Section 524B of the FD&C Act with no justification path.

Deliverable	Where it lives in your QMS	ISO 13485:2016 clause (via QMSR §820.10)	What it satisfies
Risk Management Report	Risk management file (umbrella); indexed in the DHF	7.1 Risk management; 4.2.5 Records	The traceable spine of the cybersecurity file; ties threats to controls to tests to residual risk
Threat Model	Risk management file plus design inputs in the DHF	7.1; 7.3.3 Design inputs	Identifies security risks that become design inputs
Cybersecurity Risk Assessment	Risk management file	7.1; ISO 14971 by reference	Scores patient-safety and residual risk (CVSS 4.0 / ISO 14971)
Software Bill of Materials (SBOM), statutory	Design outputs plus purchasing / supplier records	7.3.4 Design outputs; 7.4 Purchasing	Component inventory; supports supplier and vulnerability control
Component Support and End-of-Support	Purchasing / supplier records; risk management file	7.4 Purchasing; 7.1	Support status and EOS dates feed lifecycle risk
Assessment of Unresolved Anomalies	Design verification records; risk management file	7.3.6 Design verification; 8.3 Nonconforming product	Documents open items and their risk justification
Measures and Metrics	Measurement, analysis and improvement records	8.2.5 / 8.4 Analysis of data	Objective evidence the security program performs over time
Security Requirements and Control Coverage	Design inputs to design outputs in the DHF	7.3.3 Design inputs; 7.3.4 Design outputs	Security controls as traceable design requirements
Security Architecture Views	Design outputs in the DHF	7.3.4 Design outputs	Global, multi-patient-harm, updateability, security-use-case views
Static Application Security Testing (SAST)	Design verification records	7.3.6 Design verification	Verification evidence against security requirements
Penetration Test Plan	Design verification planning	7.3.6; 7.3.2 D&D planning	Planned, documented

Deliverable	Where it lives in your QMS	ISO 13485:2016 clause (via QMSR §820.10)	What it satisfies
			verification arrangement
Penetration Test Cases	Design verification records	7.3.6 Design verification	Traceable test register: case to threat to requirement
Penetration Test Report	Design verification records; feeds CAPA	7.3.6; 8.5 Improvement	Independent test evidence; findings drive remediation
Cybersecurity Labeling	Device master record (DMR) / labeling	7.3.4 outputs; 7.5.1 labeling control	Security labeling and informed-consent content
MDS2	DMR / labeling; procurement disclosure	7.3.4; 7.5.1	Standardized security disclosure to healthcare providers
Cybersecurity Management Plan, statutory	Postmarket / servicing and CAPA procedures	7.5.4 Servicing; 8.2.2 Complaints; 8.5 CAPA	Postmarket monitoring and coordinated disclosure plan
Interoperability Risk Assessment	Risk management file	7.1; ISO 14971	Risk of connected / interoperable use
Interoperability Labeling	DMR / labeling	7.3.4; 7.5.1	Interoperability information for users

Reading the map: requirements, architecture, and controls are design inputs and outputs; SAST and penetration testing are design verification; the threat model and risk assessments populate the risk management file; labeling and MDS2 belong to the device master record.

4. Ownership and control of the records

A guidance artifact only integrates if you own it and can keep it controlled over the life of the device. Blue Goat authors each deliverable so that ownership transfers cleanly and then behaves like the rest of your controlled documents:

- **Stable identifiers, authored to your file structure.** Each deliverable carries a fixed Blue Goat document ID and a revision-and-date indicator, and is written to sit as a design input, design output, verification record, or risk management file entry, the categories your QMS already defines, rather than as a free-form report.
- **Submission- and audit-ready.** Artifacts are formatted to the eSTAR structure and drop into the submission as is, while the same record satisfies the underlying QMSR design-control or risk-management requirement.
- **Client-controlled after transfer.** On delivery you apply your approval signatures, effective dates, and retention. From that point they are your controlled records, governed by your document control (§4.2.4) and records control (§4.2.5) procedures, with access limited and the cybersecurity file's confidentiality markings respected.
- **Versioned and retained.** Revisions are reissued at a new indicator and date and re-approved; superseded versions are retained rather than deleted (§4.2.5). Records are kept for the life of the device plus your defined period, so the SBOM, threat model, and test evidence stay retrievable for inspection and for your next submission.
- **Living documents, not static PDFs.** The threat model, risk assessment, and SBOM are reviewed on a defined cadence and whenever the device, its environment, or the threat landscape changes, and the Risk Management Report's traceability matrix is updated with each change so the threat to control to test to residual-risk chain stays intact.

The practical result: an auditor or reviewer sees cybersecurity evidence living inside the design history file and risk management file under your control, as living records with a clear authorship trail, not a detached bundle from a vendor.

5. Who does what

Because Blue Goat produces records that enter your design and risk management files, your quality system treats this as a controlled, outsourced activity, and it fits your existing purchasing and supplier-control procedures (ISO 13485 §7.4 and §4.1.5) with nothing new to invent. For supplier-qualification evidence, Blue Goat provides a separate Supplier Qualification Package.

The division of responsibility is simple: Blue Goat authors, and your team approves and owns.

Responsibility	Blue Goat	Your team
Author the threat model, risk assessment, testing, and labeling artifacts	Leads and authors	Provides device inputs; reviews
Approve security requirements as design inputs (§7.3.5)	Advises and supports	Approves and signs
Accept test results as verification evidence	Provides independent evidence	Accepts at design-verification review
Register and control each record (§4.2.4)	Delivers with stable IDs and editable source	Registers, owns, and retains

Responsibility	Blue Goat	Your team
Maintain the traceability matrix	Delivers and updates it	Files in the risk management file
Qualify the supplier and hold the agreement (§7.4.1)	Provides qualification evidence	Evaluates, approves, and documents
Postmarket monitoring and disclosure	Runs monitoring (GoatWatch) and advises	Owns the obligation; executes CAPA

6. How integration works in practice

Bringing the deliverables into your QMS follows five steps that map onto processes you already run:

- **1. Intake as controlled records.** Each deliverable arrives with a stable Blue Goat document ID and a revision indicator. On receipt, you register it under your document-control procedure (ISO 13485 §4.2.4) so it carries your record ID, approval, and effective date. This is the same intake path you already use for any supplier-authored design record.
- **2. Route to its QMS home.** Using the mapping table above, each artifact is filed to its home: threat model and risk assessment into the risk management file; security requirements, architecture views, and controls into the DHF as design inputs and outputs; SAST and penetration testing into design verification; labeling and MDS2 into the DMR.
- **3. Review and approve through design controls.** The artifacts are presented at your design reviews (§7.3.5). Security requirements are approved as design inputs; test results are accepted as verification evidence. Your existing review, approval, and signature workflow governs them, so nothing new is invented.
- **4. Trace end to end.** The Risk Management Report carries the traceability matrix that links every threat to its control, its test, and its residual-risk decision. This is a named FDA documentation element and the spine an auditor follows; it plugs directly into your risk management file.
- **5. Carry into postmarket.** The Cybersecurity Management Plan connects to your complaint handling (§8.2.2), CAPA (§8.5), and servicing (§7.5.4) procedures, so coordinated vulnerability disclosure and SBOM/VEX upkeep run as extensions of processes you already operate.

Traceability is the connective tissue. FDA names traceability as a documentation element (Appendix 4) that runs across every deliverable. The Risk Management Report carries the matrix that links each threat to its control, its test, and its residual-risk decision. That matrix is the single artifact an auditor can follow from a hazard all the way to the evidence it was handled, and it lives in your risk management file.

A worked example

Take a connected infusion pump. Blue Goat's threat model flags a spoofing risk on the pump's wireless channel. That risk enters your quality system as a design input, so your team approves a matching security requirement, mutual authentication, at the design-input review. The requirement traces to a control in the security architecture views (a design output), then to a penetration test case that exercises it. The test report, accepted as verification evidence at your design-verification review (§7.3.5), records the result and any residual risk, which is scored in the cybersecurity risk assessment and carried in the Risk Management Report's traceability matrix. One thread, filed across your design history file and risk management file, that an auditor can follow from hazard to evidence.

7. The tie into postmarket

Clearance is not the finish line. Section 524B and the QMSR both impose ongoing cybersecurity obligations, and the premarket file is what those obligations run on. The same records you filed become the backbone of your postmarket program, a single continuous file rather than a fresh start.



The Cybersecurity Management Plan is the operating document. Required under Section 524B(b)(1), it defines monitoring, coordinated disclosure, and update cadence, and it links to your complaint handling (§8.2.2), CAPA (§8.5), and servicing (§7.5.4).

- **SBOM and VEX upkeep.** The SBOM is maintained as components change and vulnerabilities emerge, with VEX statements recording exploitability.
- **KEV and threat monitoring.** Continuous monitoring against the CISA KEV catalog and new advisories feeds triage. Blue Goat runs this through GoatWatch, its postmarket surveillance service.
- **Coordinated vulnerability disclosure.** A defined intake and disclosure path, set by the management plan, for reports from researchers and users.
- **Feedback into the design and risk management files.** A postmarket finding that changes risk flows back through design change control (§7.3.9) into the threat model and risk assessment, with re-verification where needed, so premarket and postmarket remain one file.
- **Reporting.** Reportable cybersecurity events tie into your existing MDR and complaint processes.

Because the premarket deliverables were authored as QMS records, the postmarket program is continuous rather than a restart. The management plan, SBOM, and risk management file simply keep running.

8. Common concerns, answered

Q. "Our QMS does not have a cybersecurity process. Do we need to write one?"

A. You do not need a separate parallel process. Cybersecurity activities attach to the procedures you already have: design controls (7.3), risk management (7.1), purchasing (7.4), and CAPA and complaints (8.x). The SPDF is designed to integrate with existing product-development, risk, and quality processes. Where a light procedural hook is useful, for example referencing the threat model as a design input or the management plan in your complaint-handling SOP, Blue Goat identifies exactly where, so the change is a cross-reference rather than a new quality system.

Q. "Are these records subject to FDA inspection?"

A. Yes. Once filed in your DHF and risk management file, they are part of your quality records and are inspectable like any design or risk record under the QMSR. That is the point of authoring them as controlled records: they hold up under inspection because they carry approval, versioning, and traceability. Blue Goat writes them to that standard from the start.

Q. "What happens to these when we make a design change after clearance?"

A. Post-clearance design changes run through your design-change process (ISO 13485 §7.3.9). A change that touches the attack surface triggers a review of the threat model and risk assessment, and re-verification where needed, while the management plan and SBOM are updated in postmarket. Because the cybersecurity artifacts already live in the design and risk management files, the change process reaches them automatically rather than leaving them stale.

Q. "Does this trigger software re-validation?"

A. Only where a change affects validated software behavior, the same as any design change. Cybersecurity testing (SAST and penetration testing) is verification evidence; it feeds, but does not replace, your software validation under §7.3.7. Blue Goat scopes re-testing to the change so you are not re-validating the whole device for a targeted fix.

Q. "We also market in the EU. Does this still work?"

A. Yes. ISO 13485:2016 is the common QMS backbone for both the US QMSR and EU MDR, so the same design-control and risk management file placement holds. The threat model and risk work also support EU MDR Annex I security requirements and IEC 62304 and IEC 81001-5-1 software-lifecycle expectations. The artifacts are built to serve a dual US and EU file rather than a US-only one.

9. How Blue Goat supports the handoff

Integration is part of the engagement, not an afterthought. Every package is led by senior staff who have supported 275+ FDA submissions with no cybersecurity-related rejections to date, and each deliverable is written to land in your quality system:

- A deliverable-to-eSTAR and guidance map so each artifact's regulatory home and QMS home are both explicit.
- Submission-ready artifacts formatted to the eSTAR structure that drop in as is.
- A traceability matrix that serves as the spine of the risk management file and the audit trail.
- A plain-English record of decisions so QA, RA, and engineering stay aligned.
- Postmarket continuity (coordinated disclosure, SBOM/VEX upkeep, and KEV monitoring) tied back into your complaint and CAPA processes.

If it would help, Blue Goat can walk your quality team through the mapping against your specific SOP set and identify the small number of cross-references worth adding, typically a 30-minute conversation.

10. Glossary

Common terms and acronyms used in this note.

Term	Meaning
CAPA	Corrective and Preventive Action (ISO 13485 §8.5)

Term	Meaning
CVD	Coordinated Vulnerability Disclosure
DHF	Design History File: the compiled record of a device's design and development
DMR	Device Master Record: the specifications and procedures for the finished device
eSTAR	Electronic Submission Template And Resource, FDA's 510(k) and De Novo template
KEV	Known Exploited Vulnerabilities, the CISA catalog
MDS2	Manufacturer Disclosure Statement for Medical Device Security
QMSR	Quality Management System Regulation, the revised 21 CFR Part 820
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SPDF	Secure Product Development Framework
VEX	Vulnerability Exploitability eXchange

References

FDA, Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions (February 3, 2026), which supersedes the June 27, 2025 version.

21 CFR Part 820, Quality Management System Regulation (QMSR), effective February 2, 2026; incorporating ISO 13485:2016 by reference (89 FR 7496).

Section 524B, Federal Food, Drug, and Cosmetic Act. ISO 14971 risk management. eSTAR v7.0 submission template.

This guidance note is informational and reflects the current FDA guidance and QMSR as of the version date. It is not regulatory or legal advice and is not a guarantee of clearance. Confidential and proprietary, prepared by Blue Goat Cyber.