



BLUE GOAT CYBER
Medical Device Cybersecurity

MEDICAL DEVICE CYBERSECURITY GUIDE

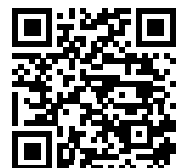
IEC 81001-5-1 Security Lifecycle Evidence Table

Practical IEC 81001-5-1 evidence mapping: lifecycle activities, artifact owners, review questions, and a worked traceability example for health software.

Reviewed 2026-10-18

bluegoatcyber.com

Book a free discovery call
30 minutes with a senior expert
bluegoatcyber.com/discovery-call



IN BRIEF

IEC 81001-5-1:2021 defines lifecycle requirements for the development and maintenance of health software to support conformance to IEC 62443-4-1, with health-software-specific needs taken into account. Organize evidence around secure development, risk management, testing, release, and vulnerability handling. Identify the exact edition and applicable interpretation sheet before performing a conformity assessment.

[Download the matching IEC lifecycle evidence PDF.](#)

The [official IEC catalogue](#) lists the corrected December 2025 version of IEC 81001-5-1:2021, including Interpretation Sheet 1. This is not a new 2025 edition. The standard excludes specification of accompanying documentation contents. Instructions-for-use requirements should be traced to applicable device law rather than attributed to this standard.

What this table does and does not establish

The table below is Blue Goat Cyber's practical evidence planning aid. It paraphrases lifecycle work and offers example artifacts, owners, and review questions. It does not reproduce the licensed standard, certify conformity, or assert that each named artifact is a mandatory standalone document. Clause-level assessment requires the licensed text, applicable interpretations, product scope, and your chosen conformity method.

IEC 81001-5-1 is not an amendment to IEC 62304. A manufacturer can integrate the security activities into an existing software lifecycle and QMS, but the standards have different scopes. Do not infer that conformity with IEC 62304 automatically establishes security lifecycle conformity.

Lifecycle activity to evidence table

Lifecycle work	Example controlled evidence	Manufacturer owner and review question
Security governance and development planning	Security development plan, defined product scope, roles, competency records, and lifecycle review criteria	Engineering / QA: Are responsibilities and review criteria established before work begins?
Security risk management	Security risk plan, asset/threat analysis, risk assessment, control decisions, and safety links where relevant	Product security / risk management: Are risks assessed in the intended environment and approved by authorized people?
Security requirements	Device-specific requirements with traceability to threats, risks, and applicable external requirements	Engineering / product security: Can each requirement be tested and traced to its reason for existing?
Secure architecture and design	Trust boundaries, data flows, threat model, control allocation, and design rationale	System engineering: Are attack surfaces and security assumptions explicit, including connected systems?

Lifecycle work	Example controlled evidence	Manufacturer owner and review question
Implementation and component management	Secure coding practices, review records, component inventory or SBOM, and supplier/component assessments	Software engineering: Are implementation and dependency risks controlled for the released configuration?
Security verification and testing	Security requirement tests, appropriate vulnerability/abuse-case testing, penetration test evidence, finding disposition, and retest records	Product security / engineering: Does evidence demonstrate the controls and account for test limitations?
Release and configuration control	Versioned evidence index, release configuration, unresolved issue rationale, and authorized release/risk decisions	QA / release authority: Do the assessed build and evidence match what is released?
Maintenance and security updates	Change impact assessment, updated threat/risk records, patch test evidence, and controlled release records	Maintenance engineering: Is each change assessed for security and relevant safety effects?
Vulnerability intake and problem resolution	Security contact/intake process, triage records, coordinated disclosure decisions, remediation tracking, and closure evidence	Product security / PSIRT: Can a reported vulnerability be tracked through assessment, action, and closure?
Lifecycle monitoring and improvement	Monitoring records, recurring issue analysis, process changes, and updated evidence	Product security / QA: Do new threats and field findings feed back into development and maintenance?

Some records can be combined. A security development plan may reference controlled QMS procedures rather than copy them. An SBOM can support component management without replacing supplier assessment or vulnerability analysis. A test report does not approve residual risk; that remains a manufacturer decision.

Confirmed standard areas and interpretation notes

The official IEC preview confirms the following process headings. Evidence examples remain our planning suggestions, not quotations of the normative requirements.

IEC area	Practical evidence focus
4: General requirements	QMS integration, responsibilities, competence, supplier controls, and security issue handling
4.3: Software-item classification relating to risk transfer	MAINTAINED, SUPPORTED, and REQUIRED classifications, responsibilities, and support arrangements
5: Software development process	Plans, threats, requirements, architecture, implementation, verification, and release evidence
6: Software maintenance process	Monitoring, impact assessment, security updates, and associated testing and communication

IEC area	Practical evidence focus
7: Security risk-management process	Risk analysis, controls, verification, and reassessment after changes
8: Software configuration-management process	Baselines, version identification, and controlled change records
9: Software problem-resolution process	Investigation, vulnerability disposition, correction, and closure evidence
Annex F: Transitional health software	Applicable whole-product transitional assessment, not a fourth software-item category or a regulatory exemption

[Interpretation Sheet 1](#) clarifies software-item categories and risk-transfer activities, vulnerability severity versus risk, monitoring, and update responsibilities. Maintain the classification rationale and reassess it when support arrangements change. The exclusion of accompanying-documentation contents does not mean there are no documentation-related activities: the interpretation sheet also clarifies security-guideline documentation. Use the licensed corrected text for the exact requirements.

How IEC 62304, SW96, and ISO 14971 relate

Reference	Main purpose	Practical connection
IEC 62304	Medical device software lifecycle processes	Integrate security activities at existing development, maintenance, configuration, and problem-resolution checkpoints; assess each standard separately
IEC 81001-5-1	Security lifecycle activities for health software	Organize secure development and maintenance activities with controlled evidence
ANSI/AAMI SW96:2023	Medical device security risk management	Apply a security risk management method alongside lifecycle activities; it is not replaced by a lifecycle evidence table
ISO 14971:2019	Medical device risk management	Link security findings to hazardous situations and harm where relevant; security-specific methods and scales may remain distinct

No one-to-one equivalence should be assumed between all clauses of these standards. Check the exact editions and any applicable regulatory recognition or harmonization. Recognition of a standard is not the same as a blanket legal mandate to use it.

Worked traceability example: a software update path

This fictional example is not a client case or evidence of a regulator's acceptance. A connected device receives software updates through a maintenance service.

Link	Example record	What to check
Threat	TM-14: an unauthorized actor supplies a modified update	Architecture identifies the update source, trust boundary, credentials, and delivery path
Security requirement	SEC-22: the device authenticates and checks update integrity before installation	Requirement describes rejection behavior and the supported configuration
Implementation	DES-22: verification control and protected trust material	Design accounts for key management, failure handling, and deployment assumptions
Security evidence	TEST-22: altered and unauthorized packages are rejected in the assessed build	Test environment, inputs, results, limitations, and build identifiers are retained
Finding disposition	FIND-08: an alternative service path bypasses the control	Manufacturer remediates or documents a justified risk decision; linked retest evidence records the outcome
Release and maintenance	REL-07 and CHG-09 reference the approved evidence set	Released versions and later update-path changes are covered by the correct assessment

Whether exploitation could create a hazardous situation depends on the device and clinical use. Link to the safety risk analysis when relevant; do not infer patient risk or acceptability from a vulnerability score alone.

How the evidence supports regional files

For the [EU MDR/IVDR evidence crosswalk](#), reference lifecycle records against the applicable GSPRs and technical-documentation sections. For [Japan](#), assess the applicable Japanese requirements and JIS mapping. For the [UK](#), distinguish Great Britain from Northern Ireland before choosing legal anchors.

For the US, the [FDA February 3, 2026 premarket cybersecurity guidance](#) explains expected cybersecurity content. A lifecycle table can organize supporting evidence, but does not substitute for guidance-specific content or applicable Section 524B obligations. Do not claim that using this table alone produces an acceptable submission.

Practical gap review

1. Define health-software scope, product versions, and applicable standards/interpretations.
2. Map lifecycle activities to existing QMS processes without duplicating procedures.
3. Index actual artifacts with revisions, build IDs, owners, and approval status.
4. Follow a sample threat through requirements, design, test, disposition, and release.
5. Confirm component changes and new vulnerability reports trigger reassessment.
6. Record evidence gaps and assign corrective work, rather than marking a document title as complete.
7. Obtain manufacturer approval for risk and release decisions.

Typical gaps include a threat model that predates the released architecture, component data with no vulnerability follow-up, tests that cannot be tied to the released build, and risk decisions with no authorized approver.

How Blue Goat Cyber helps

We support cybersecurity gap reviews, threat modeling, security risk assessment, SBOM evidence, penetration testing, and scoped cybersecurity QMS integration. General software verification and validation, QMS ownership, certification, and regulatory approval remain outside that cybersecurity service scope. The manufacturer retains risk and release authority. See [premarket cybersecurity support](#) or [book a discovery call](#).

FAQ

Is IEC 81001-5-1 just a risk assessment standard?

No. It addresses security activities across health-software development and maintenance. Risk management is part of that lifecycle, not the complete scope.

Is this a clause-by-clause conformity checklist?

No. It is a practical activity-to-evidence table. Use the licensed standard and applicable interpretation sheet for a formal clause-level assessment.

Does IEC 81001-5-1 specify IFU contents?

No. The IEC catalogue explicitly states that specification of accompanying documentation contents is excluded. Trace IFU duties to applicable regulation and use guidance to explain implementation.

Does it replace SW96 or ISO 14971?

No. Those references serve related but distinct risk management purposes. Integrate evidence and safety links where relevant without assuming identical scope or rating scales.

Is the corrected December 2025 version a new edition?

No. The IEC catalogue still identifies IEC 81001-5-1:2021, edition 1.0, with the corrected version incorporating Interpretation Sheet 1 from December 2025.

Sources and primary references

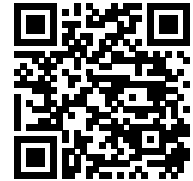
- [IEC 81001-5-1:2021, corrected version and Interpretation Sheet 1 information](#)
- [IEC 62304:2006 with Amendment 1:2015](#)
- [ANSI/AAMI SW96:2023](#)
- [ISO 14971:2019](#)

- [The FDA: February 3, 2026 premarket cybersecurity guidance](#)
- [European Commission: harmonized standards for medical devices](#)

Current web guide: bluegoatcyber.com/guides/security-risk-assessment-iec-81001-5-1

Talk to a senior medical device cybersecurity expert

Book a free 30-minute discovery call. Scan the code or visit bluegoatcyber.com/discovery-call. You get a written quote within 24 hours.



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