



INTUITIONLABS / RESEARCH & PRACTICAL GUIDANCE

IEC 81001-5-1 Implementation: An Evidence Crosswalk

Build practical AI for pharma and biotech with IntuitionLabs. We help life-science teams turn complex information and workflows into useful software, governed knowledge systems and AI tools.

Published by IntuitionLabs · 2026-10-13 · iec 81001-5-1 implementation · iec 81001-5-1 · medical device cybersecurity · secure software development lifecycle · iec 62304 · fda cybersecurity guidance · threat modeling · sbom · cybersecurity evidence

Original article: <https://intuitionlabs.ai/articles/iec-81001-5-1-implementation-evidence-crosswalk>



In this article

1. Executive Summary
 2. Introduction and Background
 3. Key Changes
 4. Implementation Considerations and Process Changes
 5. Security Requirements, Architecture and Threat Modeling
 6. Implementation, Verification and Release
 7. Postmarket Monitoring and Vulnerability Response
 8. FDA Submission Evidence Mapping
 9. Data Analysis and Evidence
 10. Implications and Future Directions
 11. Conclusion
-

Executive Summary

Implementation of **International Electrotechnical Commission (IEC) 81001-5-1** should begin with an applicability register and an activity-to-artifact crosswalk linking lifecycle security work to owners, product configurations and retained decisions. The standard addresses development and maintenance of health software. (webstore.iec.ch) Existing **IEC 62304** processes offer a software-lifecycle foundation, while security-specific reasoning and evidence need to remain identifiable. (webstore.iec.ch) This report proposes shared records with distinct review purposes, rather than treating a safety lifecycle as sufficient cybersecurity evidence.

The version register should identify **IEC 81001-5-1:2021 with the December 2025 correction** and incorporated **Interpretation Sheet 1**. (webstore.iec.ch) The interpretation clarifies software-item applicability and risk-transfer documentation; transitional status is not a fourth software-item category. (webdesk.jsa.or.jp) **U.S. Food and Drug Administration (FDA)** guidance directs readers to the Recognized Consensus Standards Database for current editions of the standards it references. (www.fda.gov) The current final guidance is dated **February 3, 2026**. (www.fda.gov) Recognition, a declaration of conformity and the submission's documentation package therefore require separate decisions.

The recommended evidence chain connects requirements, architecture and threat-model decisions to controls, verification results, release findings and maintenance records. Threat models should evolve with the system. (cheatsheetseries.owasp.org) Dependency inventories also need configuration control: the **International Medical Device Regulators Forum (IMDRF)** recommends a new **software bill of materials (SBOM)** when device software changes. (www.imdrf.org) A current implementation should distinguish the historical **National Telecommunications and Information Administration (NTIA)** minimum-elements baseline from **Cybersecurity and Infrastructure Security Agency (CISA)'s update of July 29, 2026**, which replaces it. (www.cisa.gov) Inventory content, contextual vulnerability analysis and response procedures answer different questions, so a generated SBOM alone cannot close the security assessment.

Three working tables provide the proposed evidence crosswalk, a hypothetical control-to-test traceability example and a reader-input coverage calculation. Report development, release and maintenance separately using **implemented applicable activities divided by applicable activities**. No percentage in this report establishes conformity or an acceptable risk level; **International Organization for Standardization (ISO) 14971** does not prescribe acceptable risk levels. (www.iso.org) Before a submission or conformity declaration, quality assurance and regulatory affairs (**QA/RA**) teams should review the licensed corrected text, applicable device-specific requirements and actual records. The report's publicly verified headings support navigation and preparation, while its proposed artifacts and ownership model remain implementation recommendations.

Introduction and Background

IEC 81001-5-1 implementation means making cybersecurity activities repeatable across development and maintenance, then retaining evidence that connects those activities to the released software. The standard addresses health software lifecycle security and supports the health-software application of **IEC 62443-4-1**. Its public description covers both product cybersecurity and the security of lifecycle processes. (webstore.iec.ch) A useful implementation question is therefore: can the team explain who performed an activity, which product configuration it covered, what it concluded, and how the conclusion affected release or maintenance?

For organizations already using **IEC 62304**, the starting point is an existing software lifecycle, not an empty document library. That standard covers **medical-device software development and maintenance**, while excluding medical-device validation and final device release. (webstore.iec.ch) (webstore.iec.ch) This report proposes adding security-specific evidence to existing review, change-control and configuration workflows. Shared records should preserve the purpose of each review: a safety conclusion, a security conclusion and a submission-documentation decision are different decisions.

The audience is product-security leads, software engineering managers, quality assurance and regulatory affairs (**QA/RA**) teams, and submission owners. IntuitionLabs' stated advisory scope includes technology roadmapping and digital transformation; the perspective here is implementation governance rather than certification. (intuitionlabs.ai) The analysis does not endorse a particular development tool, assessment vendor or document-management platform.

Evidence boundary: the research used public standards descriptions, the corrected preview, the published interpretation sheet and official guidance. The preview supplies navigation headings, not complete normative clause bodies. Consequently, the matrix below is an **editorial activity-to-artifact crosswalk**, not a verified clause-by-clause conformity assessment. Before declaring conformity, the responsible organization needs the licensed corrected text, an applicability assessment and review of the actual records. The recommendations are deliberately written so that a team can use them for a gap assessment without treating suggested artifact names as mandatory document titles.

Key Changes

Corrected text and Interpretation Sheet 1

IEC identifies the publication as **IEC 81001-5-1:2021, corrected December 2025**, incorporating **Interpretation Sheet 1**; the separate interpretation-sheet record gives **December 4, 2025** as its publication date. (webstore.iec.ch) (webstore.iec.ch) Record both edition and correction status in the standards register. Avoid replacing an edition identifier with a download date.

The public scope excludes specification of accompanying-documentation contents. (webstore.iec.ch) However, the interpretation addresses essential documentation for risk transfer and security maintenance.

(webdesk.jsa.or.jp) The practical reading is to assess handover responsibilities carefully, rather than assume that the scope statement removes the need to communicate security assumptions.

The interpretation gives specific applicability clarifications: **5.2.3** applies across REQUIRED, SUPPORTED and MAINTAINED software; **6.3.1** also applies to MAINTAINED software; **6.3.2 and 6.3.3** apply only to MAINTAINED software. (webdesk.jsa.or.jp) (webdesk.jsa.or.jp) (webdesk.jsa.or.jp) Alternative internal terminology should be mapped explicitly. Transitional status describes the product, rather than a fourth software-item category. (webdesk.jsa.or.jp) (webdesk.jsa.or.jp) These statements help direct a licensed-text review; they do not reproduce the underlying requirements.

Recognition, law and recommended documentation

FDA may recognize all, part or none of a standard established by a national or international standards-developing organization. (www.fda.gov) Before relying on a declaration of conformity, consult the current database record and supplemental information for the applicable standard.

FDA's consensus-standards guidance says standard use is generally voluntary unless incorporated into a regulation. (www.fda.gov) Recognition therefore does not make every clause universally mandatory. Separately, **section 524B** imposes requirements on qualifying cyber-device submissions, including a vulnerability-response plan, processes supporting cybersecurity and patches, and a software bill of materials (**SBOM**). (www.fda.gov)

Distinguishing overlapping standards

Use each reference for its own purpose. **ISO 13485** addresses **medical-device quality management**, including installation and servicing; (www.iso.org) **ISO 14971** addresses medical-device risk management and does not prescribe acceptable risk levels. (www.iso.org) (www.iso.org) IEC 62443-4-1 addresses secure-development processes, including defect management, patching and end-of-life, for developers and maintainers. (webstore.iec.ch) (webstore.iec.ch) None of these public scope statements establishes interchangeable conformity.

As complementary references, **Association for the Advancement of Medical Instrumentation (AAMI) SW96:2023** addresses manufacturer security-risk management, while the **American National Standards Institute (ANSI)** describes its relationship to ISO 14971 and use with TIR57 and TIR97. (aami.org) (webstore.ansi.org) (webstore.ansi.org) Teams can use those references to structure decisions while maintaining a separate register of applicable obligations.

Implementation Considerations and Process Changes

Build the activity register before the document library

The recommended starting artifact is an **applicability register**. Give each activity a stable identifier, responsible role, applicability rationale, accepted evidence and review state. Use the licensed standard to determine what applies, then link to existing controlled records. The proposed register distinguishes lifecycle planning from software-item responsibilities. A record marked inapplicable should explain the product boundary or support arrangement that supports that decision.

The **National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF)** provides high-level practices that can integrate with existing software development lifecycle (SDLC) implementations. (www.nist.gov) Its examples are optional, and NIST explicitly cautions against treating the framework as a checklist. (csrc.nist.gov) (csrc.nist.gov) This makes it useful as a method-selection aid, while the organization's applicability assessment remains tied to its actual standards and obligations.

Table 1 proposes an activity-to-artifact crosswalk. Clause labels are navigation references confirmed in the public contents; artifact names, ownership and reuse suggestions are editorial choices. FDA destinations identify where relevant evidence can be assembled, without asserting that every listed record is separately required. The rows use those navigation references while distinguishing them from proposed artifacts.

IEC navigation/activity	Proposed owner	Proposed controlled evidence	FDA evidence destination	IEC 62304 workflow reuse
4.3: classification/risk transfer (webstore.iec.ch)	Product security + supplier lead	Software-item responsibility register; supplier commitments; handover assumptions	Component/s support information	Inventory and supplier records
5.1: planning (webstore.iec.ch)	Engineering manager + QA	Security development plan; role assignments; tool/environment controls	Development-process explanation	Lifecycle plan and reviews
5.2: requirements (webstore.iec.ch)	Security architect + systems lead	Versioned security requirements; rationale; acceptance criteria	Risk-control explanation	Requirements baseline
5.3: architecture (webstore.iec.ch)	Software architect	Trust-boundary model; interface assumptions; review decisions	Architecture and threat-model package	Architecture baseline
5.4: design (webstore.iec.ch)	Component lead	Control design; design-review decisions	Control implementation explanation	Detailed-design reviews
5.5: implementation/verification (webstore.iec.ch)	Development + verification leads	Review records; unit-test evidence; build provenance	Verification evidence	Unit implementation records

IEC navigation/activity	Proposed owner	Proposed controlled evidence	FDA evidence destination	IEC 62304 workflow reuse
5.6: software integration testing (webstore.iec.ch)	Integration-test lead + product security	Configuration-specific integration-test plan and results; interface and trust-boundary assumptions; finding disposition and retest links	Integration/security verification evidence	Integration-test planning and records
5.7: software system testing (webstore.iec.ch)	System-verification lead + security-test lead	Configuration-specific security-requirements, threat-mitigation, vulnerability and penetration-test reports; tester independence; finding disposition and retest links	System/security testing package	System-test planning and traceability
5.8: release (webstore.iec.ch)	Release authority + security lead	Findings disposition; tested baseline; release approval	Released configuration and test package	Software-release workflow
6.1: maintenance (webstore.iec.ch)	Product support + security	Monitoring plan; support responsibilities; response workflow	Vulnerability-management plan	Maintenance plan
7: security risk (webstore.iec.ch)	Security risk owner + safety lead	Threat/control/test traceability; residual-risk decisions	Security-risk assessment	Linked safety-risk records
8: configuration (webstore.iec.ch)	Configuration manager	Component/build baselines; artifact identifiers	Version-specific evidence index	Configuration management
9: problem resolution (webstore.iec.ch)	Problem-resolution owner	Intake, triage, disposition and closure records	Vulnerability-response evidence	Problem-resolution workflow

Read the table horizontally. The useful unit is a controlled relationship between an activity, an owner and evidence, not a folder named after a standard. A shared requirements tool may support several rows, provided the links remain reviewable for a particular release.

Establish a usable implementation checklist

The following checklist is an editorial operating sequence:

- **Scope:** identify the product, software items, external services and deployment assumptions.
- **Applicability:** record included activities and reasons for exclusions.
- **Ownership:** assign accountable reviewers and execution roles.
- **Baseline:** identify the software configuration the assessment covers.
- **Evidence:** link accepted records and identify missing decisions.
- **Change control:** define which changes reopen requirements, models and tests.
- **Review:** use a release-focused walkthrough before requesting a conformity decision.

For a small team, one person may hold several roles. The proposed safeguard is to make each approval responsibility visible and document how conflicting interests are handled. For a larger organization, the same register can make supplier, platform and product-team boundaries explicit. Neither organizational size nor the existence of a policy document answers whether an activity was actually performed.

Security Requirements, Architecture and Threat Modeling

Keep security decisions linked to safety decisions

FDA recommends a separate accompanying security-risk assessment alongside the safety assessment. (www.fda.gov) A practical implementation is to link the two assessments through shared identifiers for affected functions and controls, rather than merge all reasoning into an undifferentiated risk table. The safety reviewer should be able to understand the clinical consequence under consideration, while the security reviewer can reconstruct the attack assumptions.

Threat modeling documentation should describe what is being built, its environment, what can go wrong, the proposed response and whether that response is adequate. The **Open Worldwide Application Security Project (OWASP)** organizes its guidance around those questions and recommends showing trust boundaries, flows, stores, processes and external entities. (cheatsheetseries.owasp.org) (cheatsheetseries.owasp.org) The recommended evidence pack is:

- **System boundary:** device, services, interfaces and external dependencies.
- **Trust assumptions:** identities, privileges, network conditions and operator responsibilities.
- **Threat rationale:** the behavior being considered and affected function.
- **Control decision:** accepted mitigation, accountable owner and requirement reference.
- **Verification link:** test method, expected result and tested baseline.
- **Residual concern:** unresolved assumption and approved disposition.

OWASP recommends converting agreed mitigations into actionable security requirements and maintaining the model alongside the system. (cheatsheetseries.owasp.org) (cheatsheetseries.owasp.org) The report's recommendation is to trigger review when an interface, dependency, privilege boundary or support arrangement changes. A model saved at project initiation can be retained as history, while the release decision should reference the model that covers the released design. FDA recommends documenting the rationale for the selected threat-model methodology. (www.fda.gov)

Use taxonomies to improve traceability

MITRE Common Weakness Enumeration (CWE) supplies common terminology for weaknesses, which are underlying conditions that can lead to vulnerabilities. (cwe.mitre.org) (cwe.mitre.org) **Common Attack Pattern Enumeration and Classification (CAPEC)** describes attack patterns. (capec.mitre.org) These references can help make a threat/control discussion more precise, but assigning an identifier does not show that a particular device is affected.

Table 2 illustrates a proposed security-risk-control-to-test traceability record. This is a **Hypothetical Example**, not a validated design or a required IEC template. Its structure follows the practice of tracking security requirements, risks and design decisions described in SSDF. (csrc.nist.gov)

Hypothetical threat/control record	Proposed requirement	Verification evidence	Release decision evidence
Unauthorized update delivery	Reject packages lacking an accepted authenticity check	Positive/negative tests; package and build identifiers	Results and approved update assumptions
Excessive service privileges	Limit the service to approved operations	Permission-boundary tests; configuration baseline	Approved privilege configuration
Loss of recoverable configuration	Restore an approved operational configuration	Restore rehearsal; retained configuration identifiers	Recovery instructions and accepted limitations
Uncertain dependency applicability	Determine whether the component and vulnerable functionality are present	Dependency analysis; contextual assessment; supporting tests	Recorded disposition and review trigger

The table demonstrates how to ask for evidence, not which controls every product must implement. The recovery row is consistent with Medical Device Coordination Group (**MDCG**) guidance discussing backup and restore documentation. (health.ec.europa.eu) A useful review follows the links both ways: every accepted control has relevant evidence, and every test can be explained by a requirement or risk decision.

Implementation, Verification and Release

Preserve the configuration that was actually tested

The proposed implementation record should connect reviewed source, dependency selection, generated binaries, tests and approved release artifacts. Record tool versions and assumptions where they affect the evidence. NIST's integration-oriented SSDF supports adding security practices to the organization's existing development lifecycle. (www.nist.gov) Configuration management should make it possible to answer a narrow audit question: does this report describe the software being released?

For web-facing components, the **OWASP Application Security Verification Standard (ASVS)** can provide a basis for testing technical security controls. Version its requirement references because identifiers can change between releases. (owasp.org) Use an applicability rationale before importing a catalog of tests. A device interface, cloud service and operator application may need different evidence even when they share a repository.

FDA states that cybersecurity controls need testing beyond standard software verification and validation (**V&V**). (www.fda.gov) MDCG likewise identifies testing as the primary means of security V&V. (health.ec.europa.eu) FDA recommends penetration-test reports addressing tester independence, scope, methods and results. (www.fda.gov) These statements support examining security behavior explicitly. The proposed review should distinguish a test that checks intended operation from a test that checks resistance to an unauthorized or malformed interaction.

Make the release gate a decision record

A recommended release gate contains the following evidence:

- **Baseline identity:** released software and dependency configuration.
- **Requirements coverage:** applicable controls and linked results.
- **Threat-model currency:** reviewed assumptions for the released architecture.
- **Finding disposition:** resolved items and justified outstanding decisions.
- **SBOM alignment:** inventory corresponding to the release.
- **Update readiness:** distribution, installation and recovery evidence.
- **Approval:** accountable sign-off and retained rationale.

For dependency inventory, **SPDX** is an international open standard; its software profile supplies shared classes, properties and vocabularies. (spdx.dev) (spdx.dev) The choice of representation should support the organization's evidence workflow. An export that cannot be associated with a release should be treated as an inventory-handling gap, even when it parses correctly. IMDRF cautions that an SBOM does not itself state whether a component has a vulnerability. (www.imdrf.org)

The **International Medical Device Regulators Forum (IMDRF)** recommends capturing software changes in the SBOM and generating a new SBOM when software changes. (www.imdrf.org) (www.imdrf.org) A practical release rule is to compare the inventory against the approved baseline, document differences and retain the generation context. This rule is an editorial control proposal; it is not a claim that the standard prescribes a particular scanner or file format.

Ask the release approver to select a security control and reconstruct its history from threat to requirement, implementation, verification and disposition. That exercise tests whether the evidence is usable. It also exposes a distinction between a completed test run and a completed decision about the test's significance.

Postmarket Monitoring and Vulnerability Response

Treat maintenance as an evidence-producing workflow

The proposed postmarket workflow begins with a report or monitoring signal and ends with a documented disposition, communication and updated configuration. **Coordinated vulnerability disclosure (CVD)** synchronizes relevant information and mitigations among stakeholders; the **CERT** guide also describes stakeholder roles and disclosure phases. (www.cisa.gov) (www.sei.cmu.edu) Monitoring, engineering and customer-support responsibilities should therefore be linked explicitly. CERT describes disclosure as collecting reports, sharing relevant information and coordinating the disclosure of mitigations. (www.sei.cmu.edu)

The **Forum of Incident Response and Security Teams (FIRST)** describes vulnerability intake and triage as case management within a **product security incident response team (PSIRT)**. (www.first.org) A practical sequence is:

- **Receive:** retain the report, reporter contact and affected-product description.
- **Validate:** establish reproducibility, assumptions and duplicate status.
- **Assess:** identify affected configurations and clinical/security consequences.

- **Decide:** approve remediation, mitigation or a justified disposition.
- **Verify:** test the remedy and relevant regression behavior.
- **Communicate:** coordinate disclosure and deployment instructions.
- **Close:** retain the updated baseline, evidence and monitoring triggers.

A concrete intake-policy example is **ENISA**, the European Union Agency for Cybersecurity. Its own disclosure policy requests sufficient reproduction information and proof-of-concept (**PoC**) validation for automated-scanner reports. (www.enisa.europa.eu) (www.enisa.europa.eu) That is an example of evidence quality, not an IEC reporting mandate. Teams can adapt the idea by distinguishing an unvalidated scanner observation from a confirmed product issue.

Combine prioritization signals with product context

The **Common Vulnerability Scoring System (CVSS)** expresses severity; the **Exploit Prediction Scoring System (EPSS)** estimates exploitation probability over the next **30 days**. (www.first.org) (www.first.org) CVSS v4.0 recommends considering Threat and Environmental metrics. (www.first.org) None of those signals supplies a medical-device safety-risk conclusion.

The **Cybersecurity and Infrastructure Security Agency (CISA)** recommends its Known Exploited Vulnerabilities (**KEV**) catalog as an input to prioritization. (www.cisa.gov) **CycloneDX Vulnerability Exploitability eXchange (VEX)** communicates contextual exploitability and supports state justification. (www.cyclonedx.org) (www.cyclonedx.org) CycloneDX distinguishes severity from risk in context. (www.cyclonedx.org) The proposed triage record should explain applicability, exposure, compensating controls and uncertainty, rather than replace reasoning with a score.

FIRST recommends identifying affected versions and validating remediation across affected product versions. (www.first.org) (www.first.org) FIRST also recommends quality-assurance and security validation of the remedy. (www.first.org) Record the validation scope so that a fix to one branch does not silently close the decision for another. Retain exceptions to the normal remedy cadence and their rationale. (www.first.org) MDCG recommends explicit published manufacturer guidance for patching. (health.ec.europa.eu) Maintain separate timestamps for receipt, assessment, remedy availability and field deployment; these timestamps answer different operational questions.

FDA Submission Evidence Mapping

Separate the statutory screen from the documentation package

FDA's cyber-device definition combines sponsor-authorized software, internet connectivity capability and sponsor-authorized technological characteristics potentially vulnerable to cybersecurity threats. (www.fda.gov) For qualifying submissions, section 524B requires a vulnerability-response plan including CVD, cybersecurity-supporting processes and patches, and an SBOM covering commercial, open-source and off-the-shelf components. (www.fda.gov) The applicability decision should be documented before the team treats a standards crosswalk as its submission plan.

The current FDA final cybersecurity guidance was issued on **February 3, 2026** and supersedes the version issued **June 27, 2025**. (www.fda.gov) (www.fda.gov) Keep the statutory applicability assessment, guidance-document index and proposed conformity declaration distinct.

The recommended evidence assembly checklist is:

- **Risk package:** security-risk decisions and their links to safety records.
- **Threat-model package:** current model, assumptions and methodology rationale.
- **Architecture package:** views linked to controls and update behavior.
- **Verification package:** configuration-specific results and finding disposition.
- **Component package:** SBOM, applicability analyses and support information.
- **Maintenance package:** monitoring, response, disclosure and patch procedures.

FDA recommends **Global System, Multi-Patient Harm, Updateability/Patchability and Security Use Case** views, without expecting duplicate documentation when existing material sufficiently captures a view. (www.fda.gov) (www.fda.gov) Use an evidence index to explain reuse. Reuse is useful when the underlying record answers the requested question and covers the relevant configuration.

Package evidence for review rather than duplicating it

A submitter's use of consensus standards may not, by itself, provide a sufficient basis for a regulatory decision. (www.fda.gov) Review software lifecycle evidence alongside the cybersecurity-documentation package.

For the **electronic Submission Template And Resource (eSTAR)** package, assign a stable attachment identifier to each controlled document and verify its title, revision, scope and referenced baseline. The proposed package review should follow a control from the submitted narrative to its supporting evidence without depending on informal knowledge held by the author.

There is no device type specified in this report. The submission owner should assess product-specific guidance and special controls with qualified regulatory counsel or an appropriate regulatory professional; FDA's software-guidance navigator cautions that other guidance may apply. (www.fda.gov) The same professional review should distinguish statutory requirements, recommendations, the actual declaration scope and editorial workflow suggestions. The MDCG document used here expressly identifies its views as nonbinding; it supplies complementary practice, not an additional statutory checklist. (health.ec.europa.eu)

Data Analysis and Evidence

Quantified anchors and version control

The useful numerical evidence here concerns versions, dates, framework structure and reader-entered coverage, rather than market adoption. NIST published **SSDF v1.1 on February 3, 2022**, and describes **four** practice groups: organizational preparation, software protection, secure production and vulnerability response. (www.nist.gov) (csrc.nist.gov) These groups offer planning categories; they are not measured evidence that a device conforms. The historical NTIA report also cautions that its baseline does not create new federal requirements. (www.ntia.gov)

IMDRF identifies **three** general SBOM delivery categories: manufacturer delivery, device residence and repository access. (www.imdrf.org) The historical **NTIA 2021** SBOM report identifies **seven data fields** and **three categories** of minimum elements. (www.ntia.gov) (www.ntia.gov) However, CISA's **July 29, 2026** release updates and replaces that guidance. (www.cisa.gov) Its announced additions include **Component Hash Algorithm, Component License, SBOM Tool Name and SBOM Generation Context**. (www.cisa.gov) Therefore, a gap assessment conducted as of October 2026 should identify its chosen baseline explicitly, rather than describe the older seven-field list as the complete current baseline.

FDA's eSTAR page lists **version 7.1** templates and mandatory use for 510(k) and De Novo submissions unless exempted. (www.fda.gov) (www.fda.gov) Its **Quality Management System Regulation (QMSR)** became effective **February 2, 2026**, incorporating ISO 13485:2016 by reference. (www.fda.gov) These dates support a controlled reference register, not an inference that all earlier project records must be rewritten.

Calculate coverage without inventing conformance

The following is an **editorial reader-input calculation**:

Activity coverage = implemented applicable activities / applicable activities × 100%.

Define “implemented” before scoring, for example, performed for the relevant baseline with reviewed evidence. Record applicability before calculating coverage. Keep missing evidence separate from a reasoned inapplicability decision. ISO 14971 does not prescribe acceptable risk levels; similarly, this report supplies no standard-derived implementation percentage that establishes a pass. (www.iso.org)

Table 3 is a **Hypothetical Example** using illustrative inputs, not research measurements or an audit threshold.

Assessment area	Applicable activities	Implemented with reviewed evidence	Calculated coverage
Development	12	9	75%
Release	4	3	75%
Maintenance	8	4	50%

Each percentage is calculated solely from the displayed inputs. Identical percentages can reflect different missing activities, so the reviewer should inspect the gap register. No example value establishes conformity, acceptable residual risk or submission readiness. Separate reporting prevents development work from obscuring unresolved maintenance activities.

For operational measurement, FIRST defines time to triage from initial intake to completion of triage. (www.first.org) FDA also discusses identification-to-patch and patch-availability-to-field-implementation duration. (www.fda.gov) Treat these as different intervals. Report their definitions, included population and unresolved cases before comparing periods.

Implications and Future Directions

The proposed implementation strategy is to maintain an evidence graph through existing controlled records. Requirements, threat models, configuration baselines, inventories and release decisions should be connected through persistent identifiers. IntuitionLabs describes enterprise implementation and integration services; that adjacent advisory perspective favors practical record connections without treating an integration project as product conformity evidence. (intuitionlabs.ai) Tool selection should follow the evidence relationships the team needs to preserve.

Supplier and operator boundaries deserve particular attention. The **U.S. Department of Health and Human Services (HHS)** healthcare cybersecurity goals address prompt response to vulnerabilities in vendor-provided assets and maintenance of secure configuration baselines. ([hhsciber.hhs.gov](https://hhs.gov/hhsciber)) ([hhsciber.hhs.gov](https://hhs.gov/hhsciber)) A product team's handover package can explain configuration assumptions, update responsibilities and the channel for security communications. The receiving organization still needs its own operating decisions.

IMDRF distinguishes **Development, Support, Limited Support and End of Support** lifecycle stages, and emphasizes active communication rather than passive availability alone. (www.imdrf.org) (www.imdrf.org) IMDRF also notes that jurisdiction-dependent postmarket responsibilities may continue after support ends. (www.imdrf.org) These stages should not be substituted for IEC software-item categories. Instead, they can help a team describe its product-support policy and communication plan while preserving the terms used in its conformity assessment.

Useful next steps are to select a representative release, populate the crosswalk with actual evidence and have different owners reconstruct several decisions independently. Record where the walkthrough fails: unclear applicability, missing ownership, a stale baseline, insufficient test rationale or an unresolved support assumption. Prioritize those gaps through product-specific risk reasoning. This is more informative than counting the number of uploaded documents.

Conclusion

IEC 81001-5-1 implementation is most useful when it becomes a controlled way of performing and evidencing lifecycle security work. The crosswalk presented here organizes that work around accountable roles, configuration-specific artifacts and reviewable decisions. It preserves the distinction between software lifecycle evidence, security-risk reasoning and submission documentation.

The corrected-text review matters because the published interpretation affects how support responsibilities and software categories are read. An implementation team should preserve its edition and correction references, map internal terminology and check applicability against the licensed text before relying on a declaration. Public headings and an editorial matrix can guide preparation, but cannot substitute for that assessment.

For FDA submissions, standards recognition, statutory cyber-device obligations and guidance recommendations remain separate considerations. The practical goal is a coherent evidence package: relevant records linked to the released software, understood by their owners and assembled for the questions

a reviewer needs to answer. Reusing existing records is appropriate when their scope and content support the relevant decision.

Finally, activity coverage is a planning measure. The proposed calculation should expose missing evidence separately for development, release and maintenance, without creating an invented pass percentage. A defensible next action is to complete the applicability register, test the traceability of a representative release and resolve the documented gaps through the existing quality system. That produces a concrete implementation plan while leaving conformity and regulatory conclusions to their proper, product-specific assessment.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. <https://webstore.iec.ch/en/publication/63293>
2. <https://webstore.iec.ch/en/publication/6792>
3. <https://webdesk.jsa.or.jp/link/Cor/IEC/iec81001-5-1-i1%7Bed1.0%7Den.pdf>
4. <https://www.fda.gov/media/119933/download>
5. https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html
6. <https://www.imdrf.org/sites/default/files/2023-04/Principles%20and%20Practices%20for%20Software%20Bill%20of%20Materials%20for%20Medical%20Device%20Cybersecurity%20%28N73%29.pdf>
7. <https://www.cisa.gov/resources-tools/resources/2026-minimum-elements-software-bill-materials-sbom>
8. <https://www.iso.org/standard/72704.html>
9. <https://intuitionlabs.ai/articles/iec-62304-medical-device-software-life-cycle>
10. <https://intuitionlabs.ai/>
11. <https://webstore.iec.ch/en/publication/108664>
12. <https://www.fda.gov/medical-devices/premarket-submissions-selecting-and-preparing-correct-submission/division-standards-and-conformity-assessment>
13. <https://www.fda.gov/media/71983/download>
14. <https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs>
15. <https://intuitionlabs.ai/articles/what-is-iso-13485>
16. <https://www.iso.org/standard/59752.html>
17. <https://webstore.iec.ch/en/publication/33615>
18. <https://aami.org/standard/ansi-aami-sw962023-pdf/>
19. <https://webstore.ansi.org/standards/aami/ansiaamsw962023>
20. <https://www.nist.gov/publications/secure-software-development-framework-ssdf-version-11-recommendations-mitigating-risk>
21. <https://csrc.nist.gov/Projects/ssdf>
22. https://webstore.iec.ch/en/iec_catalog/product/preview/?id=L3B1Yi9wZGYvcHJldmldy9pbmZvX2llyZgxMDAxLTUtMXtIZDEuMH1iLnBkZg%3D%3D

23. <https://cwe.mitre.org/about/faq>
24. <https://capec.mitre.org/>
25. https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf
26. <https://owasp.org/projects/asvs>
27. <https://spdx.dev/use/specifications/>
28. <https://spdx.dev/learn/areas-of-interest/software/>
29. <https://www.cisa.gov/coordinated-vulnerability-disclosure-process>
30. <https://www.sei.cmu.edu/library/the-cert-guide-to-coordinated-vulnerability-disclosure-2/>
31. https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1-1
32. <https://www.enisa.europa.eu/responsible-disclosure-policy>
33. <https://www.first.org/epss/>
34. <https://www.first.org/cvss/v4.0/specification-document>
35. <https://www.cyclonedx.org/use-cases/vulnerability-exploitability/>
36. <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-management-system-considerations-and-content-premarket>
37. <https://www.fda.gov/medical-devices/regulatory-accelerator/medical-device-software-guidance-navigator>
38. https://www.ntia.gov/sites/default/files/publications/sbom_minimum_elements_report_0.pdf
39. <https://www.cisa.gov/news-events/news/cisa-and-partners-unveil-updated-software-bill-materials-resource-improves-transparency-security-and>
40. <https://www.fda.gov/medical-devices/how-study-and-market-your-device/estar-program>
41. <https://www.fda.gov/medical-devices/postmarket-requirements-devices/quality-management-system-regulation-qmsr>
42. <https://hhscyber.hhs.gov/cybersecurity-performance-goals.html>
43. https://www.imdrf.org/sites/default/files/2023-04/IMDRF%20Principles%20and%20Practices%20of%20Cybersecurity%20for%20%20Legacy%20Medical%20Devices%20Final%20%28N70%29_1.pdf

THE PUBLISHER

About IntuitionLabs

IntuitionLabs is an AI consulting, custom software development and data engineering firm serving pharmaceutical, biotechnology, medical-device and other life-science organizations. We work with clinical, regulatory, medical-affairs, commercial, quality and IT teams to connect technology decisions with the work people need to accomplish.

AI consulting and adoption

Our AI enablement services cover readiness assessments, use-case selection, governance and policies, team workshops, adoption measurement and ongoing advisory support. We help organizations structure the information layer behind AI: source material, context, permissions and maintained knowledge that make generated answers useful and reviewable. Private LLM inference and hosted AI options support teams evaluating how to operate AI with appropriate control over their data and infrastructure.

Software, data and life-science workflows

IntuitionLabs develops custom software for pharma and biotech, integrates enterprise systems, and builds data engineering and business intelligence solutions. Areas of focus include AI agents, regulatory research, medical writing, medical affairs, CMC information, competitive intelligence and clinical-document workflows. Our eTMF intelligence work includes cross-system reconciliation and inspection-readiness support.

Enterprise platforms and regulated delivery

We provide Veeva services, application support, managed services, integrations and custom applications, alongside enterprise content work involving platforms such as Egnyte. For regulated workflows, our services include GxP enablement, computer-system validation and software development addressing 21 CFR Part 11 requirements. The applicable controls, validation responsibilities and acceptance criteria are defined for each engagement.

Work with IntuitionLabs

Explore [AI enablement](#), [pharma and biotech software development](#), [data engineering and BI](#), and [Veeva services](#). [Contact IntuitionLabs](#) to discuss your workflow, information sources and implementation needs.

IntuitionLabs publishes educational research to help life-science teams make informed technology decisions. Coverage of a product or organization does not imply a client relationship, endorsement or partnership.

Website: <https://intuitionlabs.ai>

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.