A Framework for Digitalized Quality Management in Cybersecurity Testing Laboratories: Integrating ISO/IEC 17025:2017 Requirements into Automated Workflows

Aymen Gatri *, David Lübeck, Mukayil Kilic

Posted Date: 25 February 2026

doi: 10.20944/preprints202602.1450.v1

Keywords: ISO/IEC 17025; cybersecurity testing; conformity assessment; decision rules; traceability; IEC 62443; cyber resilience act; radio equipment directive; EN 18031; ETSI EN 303 645

 doi:10.20944/preprints202602.1450.v1

Article

A Framework for Digitalized Quality Management in Cybersecurity Testing Laboratories: Integrating ISO/IEC 17025:2017 Requirements into Automated Workflows

Aymen Gatri[1,2,*], David Lübeck [1] and Mukayil Kilic [1]

1 Digital Business University of Applied Sciences, Berlin, Germany
2 TELIGENCIA Labs SARL, Tunis, Tunisia
* Correspondence: aymen.gatri@dbuas.de

Abstract

Industrial maintenance is increasingly software defined and interconnected through the internet of things, which forces a redefinition of uptime as cyber incidents begin to behave like unplanned downtime as per International Electrotechnical Commission (IEC) [1]. ISO/IEC 17025:2017 is a widely used standard for demonstrating laboratory competence in testing and evaluation across many industrial areas and disciplines [2]. Despite its long-standing and broad use, it remains under-documented and challenging when applied to cybersecurity testing. This is due in part to the nature of the business, which is highly fragmented and unique and must be treated differently from traditional laboratory activities. Cybersecurity testing has its own specific characteristics, in which software, hardware, cloud services and other components are tested individually or as integrated systems and solutions.

Keywords: ISO/IEC 17025; cybersecurity testing; conformity assessment; decision rules; traceability; IEC 62443; cyber resilience act; radio equipment directive; EN 18031; ETSI EN 303 645

1. Introduction

Cybersecurity is no longer an isolated field, especially in industrial, quality-driven environments. Downtime and uptime have long been key metrics for maintenance-quality management, with methods such as reliability-centred maintenance, risk-based maintenance and predictive maintenance still forming the basis for planning preventive and planned maintenance activities [3]. The rapid growth of IoT and IIoT in industry requires a rethinking of the boundaries of uptime metrics and incident management for industrial assets [4]. What fundamentally changes the picture is not digitalisation alone, but the rapid expansion of cybersecurity exposure across these environments.

Cybersecurity requirements [5] are being embedded into product regulation and certification schemes, and testing laboratories must demonstrate competence and repeatability. They are often a key driver for industrial companies starting their cybersecurity journey. One of the main challenges, however, is how to navigate this journey across new and evolving European and international cybersecurity regulations [5-11] that are still under progressive development and implementation.

To date, most testing laboratories have been accredited under ISO/IEC 17025 [2] for a wide range of industrial testing activities. When the focus shifts to software-, system- and solution-driven business, this accreditation can become too generic. Cybersecurity testing involves qualitative judgements, dynamic systems and tool-based measurements, and existing laboratory guidance is often limited [12].

 doi:10.20944/preprints202602.1450.v1

The resulting gap concerns how cybersecurity testing performed under ISO/IEC 17025, and the associated test outputs [13], can support a measurable cyber-maintenance plan and key performance indicators for cyber-driven maintenance strategies [14,15]. The contribution of this paper is a crosswalk that applies ISO/IEC 17025 accreditation to cybersecurity testing laboratories, including risk-based methods [16], workflow verification and validation, and the treatment of decision rules for cybersecurity conformity. Lessons learned from accreditation-style implementation case studies are also discussed, together with how these elements can support cybersecurity-driven maintenance strategies for industrial assets [17].

The paper is organised as follows. First part presents the background and related work on major industrial cybersecurity standards and their mapping to ISO/IEC 17025. Second section describes the research methods and data used in the study. Thirds section depicts the results, and finally the fourth part summarizes the results analysis and the outcomes as well as lessons learned from the work and future works in section five.

1.1. Background and Related Work

1.1.1. Maintenance Engineering, Quality and Resilience

Classical maintenance engineering treats availability as an outcome of structured failure management, where functions are defined, failure modes are analysed, and maintenance tasks are selected and periodically re-optimised based on consequences and operating context. Reliability-centred maintenance (RCM) techniques formalises this logic and is explicitly described as a guideline for developing failure-management policies and maintenance programmes (including feedback and continuous improvement) in IEC 60300-3-11 [18]. Risk-based maintenance and inspection methods extend the same principle by prioritising tasks applying a probability–consequence view of failure, allocating scarce inspection/maintenance resources to the highest-risk assets first [19]. In Maintenance 4.0 approach, this planning is increasingly coupled to Industrial IoT data streams and analytics (predictive maintenance, condition monitoring), with recent reviews emphasising both the opportunity (earlier detection, reduced unplanned stops) and the limitations (data quality, model drift, integration into operations) [20]. The recent Maintenance 5.0 discourse further shifts the focus toward resilience and recovery capacity (not only prediction), adding sustainability and human-centricity as explicit design constraints for maintenance systems [21]. This paper leverages that lineage by treating cybersecurity incidents as a new class of “unplanned downtime” for connected industrial assets [22], and by interpreting laboratory governance controls (risk review, corrective actions, evidence traceability) as measurable maintenance-like signals—an interpretation consistent with the risk and review gaps observed in the TELIGENCIA Labs assessment summary (e.g., incomplete cyber-specific risks, limited residual-risk treatment, and non-periodic risk review).

1.1.2. Industrial Cybersecurity Standards: IEC 62443 Series

Industrial cybersecurity practice is frequently structured around the ISA/IEC 62443 series, which defines lifecycle requirements and stakeholder-specific responsibilities for securing Industrial Automation and Control Systems (IACS), spanning governance, system design, and component/product assurance. Within that series, IEC 62443-4-1 [23] specifies secure product development lifecycle requirements and explicitly covers activities that matter for post-market security sustainment, including defect handling, patch management, and end-of-life practices. Complementing this, IEC TR 62443-2-3 [24] addresses patch management in the IACS environment and describes requirements for asset owners and product suppliers who establish and maintain a patch management program, an area where operational constraints (availability, safety, legacy platforms) often make “IT-style” patching infeasible without compensating controls. In practice, these standards create a direct pull for cybersecurity testing laboratories because demonstrating conformance (or supporting regulatory conformity evidence) requires repeatable, auditable test

 doi:10.20944/preprints202602.1450.v1

outcomes, and traceable handling of vulnerabilities and updates across product versions, conditions that are governance-heavy even when the underlying tests are highly technical.

1.1.3. EU Cyber Resilience Act and Regulatory Context

The EU Cyber Resilience Act (Regulation (EU) 2024/2847) establishes horizontal cybersecurity requirements for "products with digital elements" and explicitly frames the policy problem as widespread vulnerabilities and inconsistent security updates across the market [25]. The European Commission's implementation material indicates that the CRA entered into force on 10 December 2024; the main obligations apply from 11 December 2027; and reporting obligations apply earlier, from 11 September 2026 [26]. From a vulnerability-handling perspective, the CRA operationalises two evidence expectations that affect testing and assessment work: (i) manufacturers must handle vulnerabilities throughout the product lifecycle, and (ii) for actively exploited vulnerabilities and severe incidents, manufacturers must report via a Single Reporting Platform using short timelines (early warning within 24 hours and full notification within 72 hours, with a final report following corrective measures) [27]. This shifts conformity evidence away from a single "point-in-time" report toward a lifecycle argument: test evidence, vulnerability triage artefacts, update/support commitments, and reporting/communication records become part of what regulators and market surveillance authorities may expect to see as credible proof of ongoing compliance.

1.1.4. ISO/IEC 17025 in Cybersecurity Testing

ISO/IEC 17025 [2] is widely used to demonstrate laboratory competence, but cybersecurity testing stresses parts of the standard that are less dominant in classical measurement labs: qualitative outcomes, expert judgement, and rapidly changing toolchains. In such contexts, decision rules become central because conformity statements can no longer be defended by numerical uncertainty alone; instead, the laboratory must specify what evidence is sufficient, how exceptions are treated, and who carries the risk of false accept/reject. ILAC G8 was written explicitly to support laboratories implementing ISO/IEC 17025:2017 requirements on decision rules and statements of conformity [28]. The TELIGENCIA Labs assessment summary illustrates why this matters in cybersecurity: the contract review and reporting process (procedure TL-P-7.1 rev1 and template TL-P-7.1-1 rev2) contained a decision-rule field, yet the assessment noted that clients were "self-declaring" compliance via checklists in a way that is not equivalent to an ISO/IEC 17025 laboratory declaration, and recommended alignment with ILAC G8.

A second recurring issue in non-traditional domains is the misfit of conventional "measurement validity" mechanisms when results are qualitative. TELIGENCIA's procedure for ensuring validity (TL-P-7.7 rev2) applied the normalised error (En) as a performance criterion [29], even though the lab's cybersecurity results were qualitative (PASS/FAIL) and did not require uncertainty estimation; the same assessment record references a bilateral inter-laboratory comparison (Eurofins Germany, Nov 2023) that used PASS/FAIL as the evaluation criterion and also noted the absence of a participation plan for proficiency testing/comparisons. This points to a practical research gap: cybersecurity labs need fit-for-purpose inter-comparison designs, repeatability targets, and validity criteria that respect judgement-based met auditable.

Finally, competence and method control are amplified in cybersecurity because "methods" include tools, configurations, and environments that evolve continuously. ENISA has published EUCC-related guidance describing how ISO/IEC 17025 is interpreted for IT Security Evaluation Facilities (ITSEFs), recognising that additional interpretation is needed when applying 17025 to security evaluation [30]. In the TELIGENCIA assessment, "points sensibles" explicitly recommend structured competence evidence (including training aligned with ISO/IEC 19896-3 [31] for security testers/evaluators) and retaining proper competence and test-domain expertise; the same record highlights document control weaknesses (revision status not systematically identified) and risk-rating method gaps (undefined scoring criteria), which are directly relevant to toolchain baselining, method validation/verification, and the traceability of cybersecurity test conclusions over time.

 doi:10.20944/preprints202602.1450.v1

2. Materials and Methods

2.1. Research Design

This work follows a case-study research design based on accreditation-style implementation evidence from an operational cybersecurity testing laboratory. The unit of analysis is the laboratory's governance and technical record artefacts used to substantiate ISO/IEC 17025 conformity, complemented by anonymised project datasets aligned with ETSI EN 303 645 [32] and IEC 62443-related assurance activities. The study combines artefact analysis with a mixed quantitative–qualitative evaluation of assessment outcomes to identify how decision rules, method governance, and traceable records reduce ambiguity in conformity statements.

2.2. Data Analysis

2.2.1. Dataset Preparation and Anonymization

The case study dataset comprises (i) project-level cybersecurity assessment artefacts and (ii) laboratory governance artefacts used to demonstrate ISO/IEC 17025 conformity in a cybersecurity testing context. To preserve confidentiality, client/product identifiers were removed and replaced with neutral labels (e.g., Client A, Product Family A). Requirement identifiers (e.g., "5.3-11") were retained because they are standard-defined and needed for traceability and reproducibility.

The analyzed evidence included:

- ETSI TS 103 701 assessment workbook [33] (EN 303 645 aligned), including an Implementation Conformance Statement (ICS) view, an assessment view with verdicts per test case and per test group, and a reviewed "final review" version.
- IEC 62443 program audit action plan: a nonconformity-driven improvement log (NCR-based) capturing findings and corrective actions related to methodology completeness, TRF/report integrity, and evidence traceability.
- ISO/IEC 17025 internal audit report: internal audit scope, nonconformities, corrective actions, and closure dates used as a proxy for management-system "maintenance" responsiveness.
- Laboratory method and toolchain governance artefacts (ISO/IEC 17025 clause instantiations), including a method selection/verification/validation procedure, a method validation form, a controlled list of cybersecurity test methods, and a Used Computer Master List supporting controlled toolchains.

Together these artefacts represent the "scope-design artefacts" referenced in the proposal and enable analysis across planning, execution, checking, and corrective-action stages.

2.2.2. Quantitative Analysis

Quantitative analysis focused on verdict stability, ambiguity reduction, and scope discipline. The ETSI assessment workbook provides a natural before/after structure because it contains both a draft assessment state and a reviewed assessment state.

Unit of analysis (ETSI dataset): a "test group" / "provision" row (e.g., 5.6-3). Variables extracted included:

- applicability/claim status (Claimed: Yes/No/blank for conditional not applicable),
- requirement type (Mandatory vs Recommended; Conditional flags),
- support indicator (evidence present vs not),
- verdict at test group level (PASS / FAIL / INCONCLUSIVE / NO / NA),
- reviewer comment presence (notes and review columns).

The primary quantitative indicators computed were:

- **Conformity Statement Ambiguity Index (CSAI)**: measures how often a conformity statement cannot be made because decision rules and evidence are insufficient [34].

 doi:10.20944/preprints202602.1450.v1

- **Verdict transition counts (draft → reviewed)**: a transition matrix capturing how many provisions changed from INCONCLUSIVE/FAIL to PASS (or remained unresolved).
- **Evidence traceability ratio (ETSI review items)**: proportion of reviewer-flagged items where the final review explicitly references concrete evidence artefacts (e.g., document references, captures) [35].

For the IEC 62443 audit action plan, the unit of analysis was an action item row. Rows were forward filled by NCR identifier (to group multi-row NCRs) and then categorised by theme (scope definition, TRF/report integrity, evidence traceability, methodology/work instruction completeness). Counts were computed per NCR and per theme.

2.2.3. Qualitative Analysis

Qualitative analysis used directed thematic coding [36] aligned with ISO/IEC 17025 technical and management requirements and the proposed Assurance Maintenance Loop (Plan–Do–Check–Act) [37].

Two coding frames were applied:

ISO/IEC 17025 clause-oriented frame (operationalisation lens):

- Method governance & validation depth (method selection, verification, validation, deviations)
- Technical records & traceability (what evidence supports each verdict, how it is referenced)
- Reporting integrity & decision rules (how verdicts are derived and stated)
- Nonconforming work / corrective action (how gaps are tracked and closed)

Assurance Maintenance Loop frame (maintenance lens):

- Plan: scope definition, requirement selection, decision rules, milestones
- Do: controlled execution, toolchain baselines, evidence collection
- Check: peer review, consistency checks, re-evaluation triggers
- Act: corrective actions, template updates, governance refinements

Reviewer notes in the ETSI workbook and NCR texts in the 62443-action plan were coded to identify recurring causes of ambiguity and to characterise which PDCA stage produced (or resolved) them.

3. Results

3.1. Coverage of ISO/IEC 17025 Requirements with Cybersecurity Artefacts

The analysed artefact set proves that ISO/IEC 17025 requirements can be instantiated into cybersecurity-specific records without forcing cybersecurity testing into a purely "measurement uncertainty" model. Key operationalisations observed in the case laboratory include:

- **Method identification and control**: a controlled List of Methods assigns internal identifiers to cybersecurity activities (e.g., ETSI/RED-aligned testing, IEC 62443 process/product assessments, vulnerability testing/pentesting). This supports repeatability by anchoring each project to a defined method baseline rather than relying on informal "test approach" narratives.
- **Method verification/validation governance**: a formal method procedure explicitly requires validation depth proportional to changes in scope and deviations and recognizes performance characteristics relevant to cybersecurity testing (e.g., robustness, repeatability/reproducibility, and uncertainty in results interpretation).
- **Toolchain control**: the presence of a Used Computer Master List and authorised usage records provides a lightweight mechanism to document test environment identity and software update state—critical in cybersecurity testing where scanner versions, firmware images, and tool configurations can change outcomes.
- **Project workflow integration**: the RED/ETSI/IEC 62443 work instruction includes explicit steps from application evaluation to conformity assessment, report packaging, and technical

 doi:10.20944/preprints202602.1450.v1

review/closeout. This creates a direct governance bridge between ISO/IEC 17025 management controls and cybersecurity assurance deliverables.

These artefacts collectively enable a clause-to-record "crosswalk" in practice: ISO/IEC 17025 requirements become concrete cybersecurity records (ICS/IXIT completion, evidence packages, controlled templates, review logs, and corrective actions).

3.2. ETSI TS 103 701 (EN 303 645 Aligned) Assessment Outcomes

3.2.1. Dataset Structure

The ETSI assessment workbook contains 68 provision-level test groups. Applicability is expressed through "Claimed" states and conditional logic:

- Applicable/claimed: 40 provisions
- Not claimed: 6 provisions
- Blank/not applicable (conditional not met / out of scope): 22 provisions

The ICS view shows that provisions span mandatory and recommended requirements with a high share of conditional requirements, reflecting the fragmented applicability typical of industrial IoT components.

3.2.2. Draft vs. Reviewed Verdict Distributions

The draft assessment state exhibited a high reliance on INCONCLUSIVE outcomes, while the reviewed state produced a substantially higher share of PASS outcomes.

Table 1. Verdict distribution before and after review (ETSI assessment, n = 68 provisions).

Verdict category	Draft assessment	Reviewed assessment
PASS	0	38
INCONCLUSIVE	40	2
FAIL	1	1
NO (explicit "not claimed")	0	5

When restricted to claimed/applicable provisions, the change is more pronounced:

Draft (claimed = 41): 40 INCONCLUSIVE, 1 FAIL

Reviewed (claimed = 40): 38 PASS, 2 INCONCLUSIVE

This demonstrates that the review cycle (and associated evidence/decision-rule refinement) converts many "cannot conclude" outcomes into determinate conformity outcomes.

3.2.3. Verdict Transition Analysis

A transition analysis from a draft to reviewed format shows the mechanism of improvement:

Non-applicable items mostly remained non-applicable (NA → NA), with some clarified as explicitly unclaimed (NA → NO).

Table 2. Verdict transition counts (draft → reviewed).

Transition	Count
INCONCLUSIVE → PASS	37
FAIL → PASS	1
INCONCLUSIVE → INCONCLUSIVE	2
INCONCLUSIVE → FAIL	1
NA → NA	22
NA → NO	5

 doi:10.20944/preprints202602.1450.v1

This pattern indicates that ambiguity was primarily caused by documentation/evidence sufficiency and decision-rule clarity, rather than by discovery of new technical nonconformities late in the process.

3.2.4. Ambiguity Reduction Indicator

Using CSAI (INCONCLUSIVE rate among claimed/applicable items):
Draft CSAI: 40 / 41 = 0.976
Reviewed CSAI: 2 / 40 = 0.050
This reduction signals a shift from "assessment in progress" to "assessment capable of producing conformity statements," consistent with the proposal's claim that formal decision rules and controlled records reduce ambiguity.

3.2.5. Reviewer Comments and Evidence Traceability

In the reviewed assessment, 12 provisions contained explicit reviewer notes requiring clarification (e.g., increased detail, missing evidence, or scope justification). In the final review notes for these items:

- ~75% referenced IXIT updates (documentation additions to support repeatable testing), and
- ~83% referenced specific evidence artefacts (e.g., named documents, captures), indicating strengthened traceability.

Two items remained INCONCLUSIVE because the review identified evidence gaps that were documented but not closed within the dataset snapshot, illustrating the governance value of preserving "inconclusive" as a controlled outcome rather than forcing a pass/fail judgement.

One item became FAIL because a mandatory expectation was incorrectly treated as "not claimed," demonstrating the importance of explicit decision rules for when "not applicable" is permitted.

3.3. IEC 62443 Audit Action Plan Results

The IEC 62443 action plan following the IECEE CB Scheme, an international system for mutual recognition of product safety test reports and certificates for electrical and electronic components, equipment, and products [38], contains 26 corrective-action rows grouped into four NCR clusters (NCR 2, 3, 4, 5). The findings are strongly concentrated in governance and reporting controls rather than technical vulnerability discovery.

Dominant themes include:

- **Methodology/workflow incompleteness (NCR 3 dominant)**: The methodology was in draft status and missing explicit steps (e.g., identifying requirements in scope and maturity level for the chosen certification scenario).
- **Scope and scenario definition errors (NCR 4 dominant)**: Plan of Evaluation contained incorrect/ambiguous certification scenarios, indicating insufficient control of the "Plan" stage and its downstream impact on reporting and conformity interpretation.
- **TRF/report integrity issues (NCR 4 and NCR 5 dominant)**: Report numbering conflicts, combining multiple certification scenarios into one report, and modifying template sections not intended for modification—directly affecting comparability and credibility of conformity statements.
- **Evidence traceability requirements**: Repeated emphasis that evidence must be described with sufficient metadata (type/version/chapter/date), consistent with ISO/IEC 17025 expectations for technical records and reproducibility.

Overall, the action plan supports the claim that cybersecurity assurance quality is often constrained less by the absence of security expertise and more by the absence of structured conformity evidence discipline (scope, decision rules, evidence referencing, and reporting integrity).

3.4. ISO/IEC 17025 Internal Audit Findings as Governance "Maintenance" Signals

 doi:10.20944/preprints202602.1450.v1

ISO/IEC 17025 internal audits can be interpreted as periodic governance "maintenance" events: they detect early drift in confidentiality, authorisation, and documentation controls before such drift propagates into invalid test outcomes or the exposure of sensitive client information. In the case-study laboratory, the internal audit cycle recorded minor nonconformities in (i) confidentiality governance (e.g., incomplete coverage of employee non-disclosure agreements) and (ii) the timely update of documented responsibilities and authorisations when personnel roles change. Corrective actions were assigned with explicit due dates and were tracked to closure in the audit log.

Although these items are not "cyber-technical" vulnerabilities, they are material in cybersecurity testing laboratories because confidentiality, integrity of authorisation, competence continuity, and traceability are prerequisites for trustworthy security results and for protecting client artefacts (e.g., firmware images, vulnerability details, and proprietary interfaces). Consistent with this pattern, the 2025 assessment dataset shows that governance-centric deviations tend to cluster around management-system controls rather than test execution. Reported minor findings include: incomplete specification of responsibilities and authorities for report signatories and supervision (Clause 6.2.4); incomplete records for externally provided cloud services (Clause 6.6.2); mis-specified performance comparison criteria and lack of a participation plan for inter-laboratory comparisons for qualitative security outcomes (Clause 7.7.2); report templates containing inapplicable elements for qualitative cybersecurity tests and unclear terminology around outsourced/subcontracted work (Clause 7.8.3); ambiguity in contract review and reporting regarding decision rules and conformity statements, with an explicit recommendation to align with ILAC G8 [28] (Clauses 7.1.3 and 7.8.6); insufficient traceability when amending or re-issuing reports (Clause 7.8.8); and an under-specified risk-and-opportunity register and review cadence, including residual-risk treatment (Clause 8.5). Additional minor governance gaps noted in the dataset relate to the handling of internal nonconformities (Clause 7.10), the clarity of test-request templates to avoid confusion between testing and product certification (Clause 7.1), and the completeness of equipment registers for standard-specific tooling (Clause 6.4).

Framed through an industrial maintenance lens, each minor nonconformity functions as a leading indicator of governance degradation. Tracking recurrence, clause concentration, and mean time-to-closure provides measurable "cyber-maintenance indicators" [39] that complement technical test KPIs and support sustained comparability and defensibility of conformity statements in fast-evolving security test domains.

4. Discussion

4.1. Why the Results Support ISO/IEC 17025 Operationalisation for Cybersecurity Testing

Cybersecurity testing differs from traditional laboratory testing because it combines:

- tool-driven measurements (scanner outputs, captures, logs),
- expert judgement (triage, exploitability interpretation, applicability decisions),
- rapidly changing methods (tool versions, threat patterns),
- conditional applicability (requirements depend on architecture, configuration, and interfaces).

Across the case evidence, the limiting factor for defensible conformity statements is rarely "test execution capability" alone; it is the governance layer that makes qualitative security results auditable, repeatable, and comparable. This is consistent with the 2025 accreditation/assessment findings, where recorded nonconformities were minor yet concentrated in management-system controls that directly shape test trustworthiness—e.g., incomplete definition of signatory authorities and supervision responsibilities (Clause 6.2.4), incomplete control records for externally provided services such as cloud hosting (Clause 6.6.2), a missing fit-for-purpose approach to proficiency testing / inter-laboratory comparisons for qualitative PASS/FAIL outcomes (Clause 7.7.2), report template misalignment with qualitative testing (Clause 7.8.3), ambiguity around decision rules and conformity

 doi:10.20944/preprints202602.1450.v1

statements (Clauses 7.1.3 and 7.8.6), weak amendment traceability when reports are re-issued (Clause 7.8.8), and an under-specified risk/opportunity register and review mechanism (Clause 8.5).

These findings support the paper's central claim: ISO/IEC 17025 can govern cybersecurity testing effectively only when clauses are translated into cybersecurity-native artefacts (e.g., ICS/IXIT, controlled method lists, evidence packages with versioned toolchains, decision-rule catalogues, review logs, and re-issuance traceability records). In the ETSI-aligned dataset discussed earlier in the paper, the main barrier to issuing conformity statements was not "technical failure," but insufficiently structured evidence and decision rules, visible in the initial dominance of INCONCLUSIVE outcomes. After review and evidence integration, most outcomes became determinable (PASS), demonstrating that ambiguity is reducible through governance—not through additional testing alone.

4.2. Decision Rules as the Primary Lever for Ambiguity Reduction

The largest measurable effect remains the reduction in INCONCLUSIVE outcomes among claimed provisions (CSAI from ~0.98 to ~0.05 in the paper's dataset). This aligns with ILAC-style logic: if evidence is incomplete, a laboratory should either (a) declare the result inconclusive with documented rationale, or (b) apply a predefined decision rule for sufficiency, acceptance, and treatment of uncertainty/limitations.

The 2025 assessment findings strengthen this point by showing that decision-rule weaknesses surface early and are auditable. Specifically, the assessment highlights ambiguity where a client "self-declares" compliance using checklists while the ISO/IEC 17025 report must provide a laboratory-controlled declaration of conformity and a documented decision rule, with an explicit recommendation to align with ILAC G8 (Clauses 7.1.3 and 7.8.6). This is not a clerical concern: it defines who owns the conformity claim, what evidence is sufficient, and how exceptions are handled.

This is not a clerical concern: it defines who owns the conformity claim, what evidence is sufficient, and how exceptions are handled.

Two discussion implications follow:

1. "Inconclusive" is not a failure of testing; it is a controlled quality state: Where evidence expectations are recognised but not met, preserving an inconclusive outcome prevents false passes and enables later reassessment without reconstructing context.
2. "Not applicable" and "not claimed" require strict constraints. Mandatory expectations cannot be de-risked by re-labelling them as "unclaimed." This boundary condition is precisely where formal decision rules add value: they make the line between "out of scope" and "nonconforming" explicit and auditable. In practice, this argues for a decision-rule structure that is standard-aware (ETSI/EN 303 645, EN 18031, IEC 62443) and interface-aware (ICS/IXIT conditions), and that explicitly encodes when NA is permissible.

4.3. Traceability and Comparability: Why Controlled Toolchains and Evidence Packages Matter

The IEC 62443 action-plan issues highlighted earlier—scenario selection errors, mixed scenarios in one report, incomplete TRF fields, inconsistent report numbering, and insufficient evidence metadata—are not "mere documentation problems." They determine whether two laboratories (or two assessments at different times) can be compared and whether a regulator can treat the report as credible compliance evidence.

The 2025 assessment dataset adds concrete, clause-linked examples of comparability failure modes that are governance-driven:

- Report template misfit for qualitative cybersecurity tests (e.g., references to uncertainty estimation where qualitative PASS/FAIL is used; confusion between outsourced vs externalised work terminology), which can introduce interpretive noise and inconsistent reporting expectations (Clause 7.8.3).

 doi:10.20944/preprints202602.1450.v1

- Weak amendment and re-issuance traceability, where a re-issued report retains the original identifier instead of using a unique identifier and explicit linkage, reducing auditability over time (Clause 7.8.8).
- Incomplete governance records for external service providers, notably cloud hosting, which creates both confidentiality risk and reproducibility ambiguity when the execution environment is externalised (Clause 6.6.2).
- Document control sensitivity points, including periodic review and consistent revision-state identification, which directly affects whether a given test was executed under the correct controlled method and template revision (Clauses 8.2/8.3 – points sensibles).

In cybersecurity testing, "toolchain control" is not only version pinning. It is evidence interpretability: the environment state, tool versions, configuration, and artefact provenance must be sufficiently specified so that results remain meaningful as tools evolve. Evidence packages (captures, logs, configuration snapshots, versioned scripts, controlled templates) therefore function as repeatability scaffolding for qualitative verdicts.

4.4. The Assurance Maintenance Loop as a Cyber-Maintenance Control System

Interpreting the empirical findings through the proposed PDCA loop clarifies how ISO/IEC 17025 governance behaves like an industrial maintenance system—detecting, correcting, and preventing "assurance downtime" (ambiguous or non-defensible conformity outcomes):

- Plan (scope, decision rules, risk model): Assessment findings show that when decision rules are underspecified and conformity statements are blurred with client self-declarations, the entire assurance chain becomes fragile (Clauses 7.1.3 and 7.8.6). The same applies to risk and opportunity management: missing cyber-specific risks (e.g., IT system operational blockage, data quality/non-quality, external equipment integrity/security) and the absence of residual-risk treatment or periodic re-evaluation limit the management system's ability to anticipate and prevent governance failures (Clause 8.5).
- Do (controlled execution and technical records): Execution quality depends on controlled templates, fit-for-purpose reporting for qualitative outcomes, controlled external-provider interfaces (including cloud services), and disciplined technical records. The findings around reporting content and external provider records indicate that "doing" in cyber labs includes maintaining the trust boundary around tooling, environments, and outsourced/externalised components.
- Check (review, internal audit, inter-lab validity mechanisms): The ETSI dataset demonstrates that completeness checks and peer review materially change outcomes (INCONCLUSIVE → PASS) by resolving ambiguity rather than by adding tests. The assessment dataset reinforces that "Check" must also include fit-for-purpose validity mechanisms: qualitative PASS/FAIL domains require different inter-lab comparison criteria than quantitative measurement domains, and a participation plan is expected (Clause 7.7.2). Additionally, competence assurance in this stage includes demonstrable auditor competence and relevant cybersecurity-testing expertise for the internal audit function (Clause 8.8.2 – point sensible).
- Act (corrective actions as governance maintenance actions): Nonconformity action plans (programme-level) and internal audit corrective actions are the "maintenance actions" that update procedures, templates, decision rules, competence records, and risk registers. The key maintenance property is closure with verification—the governance analogue of restoring availability after downtime. The assessment process also makes closure timeliness explicit (action plan submission and evidence windows), which can be treated as a measurable maintenance parameter

4.5. Proposed Measurable Cyber-Maintenance Indicators

Building on the observed patterns (ETSI/IEC 62443 dataset behaviour + 2025 assessment findings), the following indicators are proposed for accredited cybersecurity laboratories and asset owners:

 doi:10.20944/preprints202602.1450.v1

- Conformity Statement Ambiguity Index (CSAI): rate of INCONCLUSIVE outcomes among claimed items. Interpretation: evidence/decision-rule maturity; reflects "assurance uptime."
- Scope Misclassification Count: number of mandatory requirements incorrectly marked NA/unclaimed (or moved outside scope without an auditable rule). Interpretation: decision-rule boundary failures with direct compliance impact.
- Decision Rule Coverage Ratio: share of projects/reports in which the decision rule is explicitly documented, traceable to the applicable specification, and applied consistently across provisions (contract review → report). Motivation: assessment findings explicitly flag decision-rule ambiguity and the need to align conformity reporting with ILAC-style expectations (Clauses 7.1.3 and 7.8.6).
- Evidence Traceability Ratio: share of provisions whose verdict includes explicit references to versioned artefacts (captures/logs/config snapshots/tool versions). Interpretation: reproducibility and audit readiness; predictor of comparability across labs/time.
- Report Amendment Integrity Rate: proportion of amended/re-issued reports that use a unique identifier and explicit linkage to the original report they replace. Motivation: assessment findings show that weak amendment traceability degrades longitudinal comparability and audit defensibility (Clause 7.8.8).
- External Service Governance Coverage: share of externally provided services (including cloud hosting) with documented evaluation, risk treatment, and retained records. Motivation: assessment findings show governance records may omit cloud providers despite their security and confidentiality implications (Clause 6.6.2).
- Corrective Action Lead Time: time from NCR creation to verified closure (internal audit + programme action plans). Interpretation: governance MTTR; measures how quickly the lab restores "assurance availability."

Together, these metrics connect cybersecurity testing quality to maintenance-quality management and enable asset owners to incorporate cybersecurity assurance capacity into broader uptime/resilience planning.

5. Conclusions

The case study is derived from a single laboratory's artefact set and a limited number of project datasets. While this supports deep operational insight, broader generalisation requires:

- Multi-lab inter-comparison designs for qualitative cybersecurity outcomes, including performance criteria that are meaningful for PASS/FAIL and mixed judgement/evidence methods (explicitly motivated by Clause 7.7.2 findings on unsuitable quantitative criteria and missing participation planning).
- Longitudinal tracking of toolchain drift (tool versions, rulesets, cloud environments) and its effect on verdict reproducibility and evidence interpretability.
- Expanded decision-rule engineering for mixed judgement/evidence-driven methods, with explicit acceptance criteria, treatment of partial evidence, and strict NA constraints, aligned with ILAC-style conformity logic (motivated by Clauses 7.1.3 and 7.8.6).
- Strengthened governance instrumentation, including: formal amendment traceability for re-issued reports (Clause 7.8.8), systematic document revision control (Clauses 8.2/8.3 – points sensibles), and explicit cyber-risk scoring scales/residual-risk treatment and periodic review triggers (Clause 8.5).
- Competence frameworks tailored to cybersecurity testing, leveraging competence guidance (e.g., ISO/IEC 19896-3 is flagged as a training recommendation in the assessment points sensibles) and ensuring internal auditors can audit both management-system and cyber-testing specifics.

Future work should validate the proposed cyber-maintenance indicators against operational outcomes (reduced rework, faster determinable conformity decisions, improved audit performance, and improved confidentiality assurance), and test whether indicator trends predict accreditation risk or conformity-statement instability across tool and threat evolution.

 doi:10.20944/preprints202602.1450.v1

Author Contributions: Conceptualization, A.G., D.L., and M.K.; methodology, A.G., D.L., and M.K.; formal analysis, A.G., D.L., and M.K.; investigation, A.G., D.L., and M.K.; resources, A.G., D.L., and M.K.; data curation, A.G., D.L., and M.K.; writing—original draft preparation, A.G.; writing—review and editing, D.L. and M.K.; supervision, D.L.; project administration, A.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets and laboratory artefacts analysed in this study are not publicly available due to confidentiality obligations with clients and third parties. Anonymised excerpts or derived indicators may be made available on reasonable request, subject to contractual and legal constraints.

Acknowledgments: The authors acknowledge the laboratory personnel and assessment reviewers whose governance and technical record-keeping practices informed the case study and thank the peer reviewers for their constructive feedback during manuscript development.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

Abbreviation	Definition
CRA	Cyber Resilience Act
RED	Radio Equipment Directive
IEC	International Electrotechnical Commission
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ILAC	International Laboratory Accreditation Cooperation
ETSI	European Telecommunications Standards Institute
IACS	Industrial Automation and Control Systems
IoT	Internet of Things
IIoT	Industrial Internet of Things
PDCA	Plan–Do–Check–Act
RCM	Reliability-Centered Maintenance
ICS	Implementation Conformance Statement
IXIT	Implementation eXtra Information for Testing
NCR	Nonconformity Report
TRF	Test Report Form
ITSEF	IT Security Evaluation Facility
EUCC	European Cybersecurity Certification Scheme

References

1. International Electrotechnical Commission (IEC). Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels (IEC 62443-3-3:2013), Edition 1.0; IEC: Geneva, Switzerland, 2013.
2. ISO. ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories; International Organization for Standardization: Geneva, Switzerland, 2017. Available online: https://www.iso.org/standard/66912.html (accessed on 15 February 2026).
3. Smith, A., & Hinchcliffe, G. R. *RCM3: Risk-Based Reliability Centered Maintenance*. Momentum Press, 2014.
4. Molęda, M., Małysiak-Mrozek, B., Ding, W., Sunderam, V., & Mrozek, D. (2023). From Corrective to Predictive Maintenance—A Review of Maintenance Approaches for the Power Industry. Sensors, 23(13), 5970. https://doi.org/10.3390/s23135970.

 doi:10.20944/preprints202602.1450.v1

5. National Institute of Standards and Technology (NIST). *Guide to Operational Technology (OT) Security (SP 800-82 Rev. 3)*; NIST: Gaithersburg, MD, USA, 2023. https://doi.org/10.6028/NIST.SP.800-82r3.
6. International Electrotechnical Commission (IEC). IEC 62443-2-1:2010 Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program; IEC: Geneva, Switzerland, 2010.
7. International Society of Automation (ISA). ISA/IEC 62443 Series of Standards. Available online: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (accessed on 15 February 2026).
8. European Union. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment (Radio Equipment Directive). Official Journal of the European Union, 2014. Available online: https://eur-lex.europa.eu/eli/dir/2014/53/oj/eng (accessed on 15 February 2026).
9. European Commission. Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU with regard to the application of the essential requirements referred to in Article 3(3)(d), (e) and (f). Official Journal of the European Union, 2022. Available online: https://eur-lex.europa.eu/eli/reg_del/2022/30/oj/eng (accessed on 15 February 2026).
10. European Commission. Commission Implementing Decision (EU) 2025/138 of 28 January 2025 amending Implementing Decision (EU) 2022/2191 as regards harmonised standards in support of the essential requirements of Directive 2014/53/EU that relate to cybersecurity. Official Journal of the European Union, 2025. Available online: https://eur-lex.europa.eu/eli/dec_impl/2025/138/oj/eng (accessed on 15 February 2026).
11. European Union. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union, 2024. Available online: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (accessed on 15 February 2026).
12. Hall, T.; Nicholson, K.J.; Rogers, D.J. Cybersecurity Testing—Good Practice Guide; National Physical Laboratory (NPL): Teddington, UK, 2018.
13. IntuitionLabs. ISO/IEC 17025: A Complete Guide to Lab Accreditation; IntuitionLabs, 2025. Available online: https://intuitionlabs.ai/pdfs/iso-iec-17025-a-complete-guide-to-lab-accreditation.pdf (accessed on 15 February 2026).
14. SentinelOne. Cybersecurity Metrics & KPIs: What to Track in 2026; SentinelOne, 2026. Available online: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-metrics/ (accessed on 15 February 2026).
15. LLumin. Cybersecurity Best Practices for Maintenance Systems; LLumin, 2025. Available online: https://llumin.com/blog/cybersecurity-best-practices-for-maintenance-systems/ (accessed on 15 February 2026).
16. Information Risk Analysis in Laboratories Complying with ISO/IEC 17025 Standard. ResearchGate, 2025. Available online: https://www.researchgate.net/publication/396118377_Information_Risk_Analysis_in_Laboratories_Complying_with_ISOIEC_17025_Standard (accessed on 15 February 2026).
17. Industrial Cyber. Cybersecurity Best Practices in the Manufacturing Sector; Industrial Cyber, 2024. Available online: https://industrialcyber.co/manufacturing/cybersecurity-best-practices-in-the-manufacturing-sector/ (accessed on 15 February 2026).
18. IEC. IEC 60300-3-11:2009. Dependability management - Part 3-11: Application guide - Reliability centred maintenance; International Electrotechnical Commission: Geneva, Switzerland, 2009.
19. Towards Maintenance 5.0: Resilience-Based Maintenance in AI; Preprints.org, 2025. Available online: https://www.preprints.org/manuscript/202507.0345 (accessed on 15 February 2026).
20. Werbińska-Wojciechowska, S.; Winiarska, K. Maintenance Performance in the Age of Industry 4.0: A Bibliometric Performance Analysis and a Systematic Literature Review. Sensors 2023, 23, 1409. https://doi.org/10.3390/s23031409

 doi:10.20944/preprints202602.1450.v1

21. Cortés-Leal, A.; Cárdenas, C.; Del-Valle-Soto, C. Maintenance 5.0: Towards a Worker-in-the-Loop Framework for Resilient Smart Manufacturing. Appl. Sci. 2022, 12, 11330. https://doi.org/10.3390/app122211330
22. ABS Group. How Cybersecurity Drives Reliability and Maintenance Performance; ABS Group: Spring, TX, USA, 2026. Available online: https://www.abs-group.com/Knowledge-Center/Insights/How-Cybersecurity-Drives-Reliability-and-Maintenance-Performance/ (accessed on 15 February 2026).
23. International Electrotechnical Commission (IEC). IEC 62443-4-1:2018 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements; IEC: Geneva, Switzerland, 2018.
24. International Electrotechnical Commission (IEC). IEC TR 62443-2-3:2015 Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment; IEC: Geneva, Switzerland, 2015.
25. European Parliament and Council. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act); Official Journal of the European Union: Brussels, Belgium, 2024; L_202402847.
26. European Commission. Cyber Resilience Act; European Commission: Brussels, Belgium, 2024. Available online: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (accessed on 15 February 2026).
27. Hogan Lovells. EU Cyber Resilience Act: Key 2026 milestones toward CRA compliance; Hogan Lovells: London, UK, 2026. Available online: https://www.hoganlovells.com/en/publications/eu-cyber-resilience-act-getting-ready-for-cra-compliance-in-2026 (accessed on 15 February 2026).
28. International Laboratory Accreditation Cooperation (ILAC). ILAC-G8:09/2019 Guidelines on Decision Rules and Statements of Conformity; ILAC, 2019. Available online: https://www.iasonline.org/wp-content/uploads/2021/03/ILAC_G8_09_2019.pdf (accessed on 15 February 2026).
29. ISO/IEC. ISO/IEC 13528:2022 Statistical methods for use in proficiency testing by interlaboratory comparison; International Organization for Standardization: Geneva, Switzerland, 2022.
30. European Commission. Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC); Official Journal of the European Union: Brussels, Belgium, 2024; L_202400482.
31. ISO/IEC. ISO/IEC 19896-3:2018 IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators; International Organization for Standardization: Geneva, Switzerland, 2018.
32. ETSI. ETSI EN 303 645 V2.1.1 (2020-06) Cyber Security for Consumer Internet of Things: Baseline Requirements; ETSI, 2020. Available online: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (accessed on 15 February 2026).
33. ETSI. ETSI TS 103 701 V1.1.1: Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements; European Telecommunications Standards Institute: Sophia Antipolis, France, 2021.
34. JCGM. JCGM 106:2012 Evaluation of measurement data – The role of measurement uncertainty in conformity assessment; Joint Committee for Guides in Metrology: Sèvres, France, 2012.
35. ISO. ISO 9000:2015 Quality management systems — Fundamentals and vocabulary; International Organization for Standardization: Geneva, Switzerland, 2015.
36. Kuckartz, U.; Rädiker, S. Qualitative Content Analysis: Methods, Practice and Software; SAGE Publications: London, UK, 2023.
37. ISO/IEC. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements; International Organization for Standardization: Geneva, Switzerland, 2022.
38. IECEE. *IECEE 02:2023 System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE System) - Rules of Procedure*; International Electrotechnical Commission: Geneva, Switzerland, 2023.

 doi:10.20944/preprints202602.1450.v1

39. ISO/IEC. ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation; International Organization for Standardization: Geneva, Switzerland, 2016. (Note: ISO/IEC 27004 provides the formal framework for assessing the performance of information security management systems through measurable indicators, perfectly supporting your KPI argument).