Journal of *Cybersecurity and Privacy*

MDPI

Article

Digitalized Quality Management for Cybersecurity Conformity Assessment: ISO/IEC 17025-Based Automated Workflows, Evidence Analytics, and EN 18031 Readiness for the Radio Equipment Directive

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

[1] Department of Cybersecurity and AI Defense, Digital Business University of Applied Sciences, 10999 Berlin, Germany; david.luebeck@dbuas.de (D.L.); mukayil.kilic@dbuas.de (M.K.)
[2] Teligencia Labs SARL, Tunis 1080, Tunisia
* Correspondence: aymen.gatri@dbuas.de

Abstract

Cybersecurity conformity assessment is increasingly shaped by the Radio Equipment Directive (RED) delegated act, the EN 18031 harmonized standards, the Cyber Resilience Act, and industrial standards such as International Electrotechnical Commission (IEC) 62443. ISO/IEC 17025:2017 provides a general laboratory competence framework, but its application to qualitative cybersecurity testing, rapidly changing toolchains, and automation-assisted evidence workflows remains under-specified. This paper proposes a digitalized quality-management framework that translates ISO/IEC 17025 clauses into cybersecurity-native controls for scope definition, method governance, toolchain control, evidence traceability, decision rules, technical review, and corrective-action feedback. An accreditation-style single-laboratory case study integrates a European Telecommunications Standards Institute (ETSI) TS 103 701 assessment workbook, an IEC 62443 corrective-action dataset, ISO/IEC 17025 internal audit findings, and laboratory governance records. In the ETSI workbook, the Conformity Statement Ambiguity Index (CSAI) decreases from 0.976 in the draft state to 0.050 after review, with 37 previously inconclusive provisions moving to PASS. This result is interpreted as improved determinability within the assessed workflow, not as cross-laboratory validation. The study contributes a clause-to-workflow operationalization of ISO/IEC 17025, an analytic design for heterogeneous assurance artefacts, and an EN 18031 evidence-mapping approach for Radio Equipment Directive readiness.

Keywords: cybersecurity conformity assessment; ISO/IEC 17025; workflow automation; evidence traceability; decision rules; EN 18031; Radio Equipment Directive; Cyber Resilience Act; IEC 62443; AI-assisted assurance

Check for updates

Academic Editor: Shay Gueron

Received: 5 March 2026
Revised: 10 May 2026
Accepted: 26 May 2026
Published: 30 June 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Cybersecurity can no longer be treated as a peripheral information-technology issue. For connected products and industrial systems, cybersecurity requirements are now embedded in regulation, product assurance, procurement decisions, and post-market governance. In the European Union, the Radio Equipment Directive cybersecurity delegated act and the Cyber Resilience Act [1–3] have increased expectations for secure-by-design products, vulnerability handling, and traceable conformity evidence. The EN 18031 series [4–6] further raises the evidentiary bar by requiring laboratories to justify determinations under

Articles 3(3)(d), 3(3)(e), and 3(3)(f) of the Directive with repeatable and auditable evidence. As a result, isolated point-in-time assessments are no longer sufficient; evidence must remain reviewable, reproducible, and meaningful across the product lifecycle [7–10].

ISO/IEC 17025:2017 is widely used to demonstrate competence in testing and calibration laboratories [11,12]. Cybersecurity testing, however, places unusual pressure on this framework. Outcomes are often qualitative: a requirement may pass, fail, remain inconclusive, or be outside the applicable scope. Applicability can depend on product architecture, deployment mode, enabled interfaces, or user roles. Toolchains also change quickly. A defensible verdict therefore depends less on classical measurement uncertainty than on clear decision rules, sufficient evidence, and a traceable chain from observation to conclusion. For a cybersecurity laboratory, method control must therefore include scanner versions, scripts, container images, target configurations, report templates, and review logic, not only written procedures.

The research problem addressed in this paper is the lack of a practical operational model that translates ISO/IEC 17025 requirements into automation-ready, cybersecurity-specific workflow controls while also providing measurable indicators for assurance quality [13–15]. Existing work often treats laboratory competence, cybersecurity testing practice, and compliance automation as separate topics. Less attention has been paid to how these elements can be combined into a coherent quality-management architecture for qualitative cybersecurity conformity assessment, particularly under emerging European product-security regulation.

This paper develops and examines a digitalized quality-management framework for cybersecurity conformity assessment. The study is intentionally framed as a single-laboratory case study. Its purpose is not to claim universal validation across all laboratories, but to show, in operational detail, how ISO/IEC 17025 clauses can be instantiated into concrete governance artefacts, automated evidence workflows, and review controls, and how those controls affect ambiguity within one real assessment process.

The paper makes four concrete contributions:

- It translates ISO/IEC 17025 clauses into cybersecurity testing workflow controls covering scope management, method governance, technical records, decision rules, toolchain control, and technical review.
- It proposes an analytic design that integrates heterogeneous evidence sources, including ETSI assessment records, IEC 62443 [16–20] corrective-action logs, internal audit findings, and governance documents, into one case study protocol.
- It introduces practical indicators for ambiguity, evidence traceability, and governance maintenance, anchored by the Conformity Statement Ambiguity Index (CSAI).
- It connects EN 18031 restriction logic and Radio Equipment Directive implications to laboratory evidence packages so that regulatory readiness is considered during quality planning rather than only at the reporting stage.

The remainder of the manuscript is organized as follows. Section 2 provides the standards background needed for the study, while Section 3 presents the regulatory context. Section 4 reviews related work and motivates the analytical framing. Section 5 describes the materials and methods. Section 6 reports the case study results. Section 7 discusses the findings, automation implications, and limitations. Section 8 concludes.

2. Background and Standards Context

This section introduces the standards landscape on which the framework is built. Three areas are especially relevant: ISO/IEC 17025 as the core competence framework for laboratories, IEC 62443 as a lifecycle-oriented industrial cybersecurity standard family,

and the specific interpretation challenges that arise when ISO/IEC 17025 is applied to qualitative cybersecurity testing.

2.1. ISO/IEC 17025 and the Specificity of Cybersecurity Testing

ISO/IEC 17025 covers impartiality, competence, methods, technical records, result validity, reporting, and management-system control [11]. In cybersecurity testing, these requirements need domain-specific interpretation. Unlike many calibration activities, cybersecurity assessments frequently produce PASS, FAIL, INCONCLUSIVE, or NOT APPLICABLE verdicts rather than numerical results with directly calculable uncertainty bounds. The path from raw evidence to verdict involves expert judgement, decision rules, and scope decisions that may depend on enabled interfaces, deployment mode, and user roles. Toolchains also evolve quickly, so the context in which evidence was produced must be recorded. Laboratories therefore need ISO/IEC 17025 controls that address decision rules, evidence sufficiency thresholds, traceability chains, and disciplined method change management.

2.2. IEC 62443 and Lifecycle-Oriented Assurance Demands

The ISA/IEC 62443 family organizes industrial cybersecurity across governance, system, and component/product levels. IEC 62443-4-1 [21] addresses secure product development lifecycle requirements, including defect handling and patch-related practices, while IEC TR 62443-2-3 covers patch management in industrial automation and control settings [16–19]. For laboratories, these standards have a practical consequence: evidence must remain intelligible and defensible across software versions, product updates, and corrective-action cycles. Quality management therefore cannot be organized only around individual test executions; evidence needs to be packaged in a way that remains useful throughout the product lifecycle [22–26].

2.3. Applying ISO/IEC 17025 to Cybersecurity Testing

ISO/IEC 17025 is well established in calibration and testing laboratories, but cybersecurity testing requires additional interpretation. Because the work relies on expert judgement, toolchain-dependent observations, and PASS/FAIL/INCONCLUSIVE verdicts, the standard's classical mechanisms for managing measurement validity do not map directly. Decision rules become central: since conformity statements cannot be justified by numerical uncertainty alone, laboratories must specify what counts as sufficient evidence, how exceptions are handled, and how false-accept and false-reject risk is allocated. Interlaboratory comparison schemes also require a fit-for-purpose design for qualitative domains rather than simple transfer from calibration practice. Method control becomes more demanding once the method is understood to include specific tool versions, configurations, and environments that may change between projects.

3. Regulatory Context

This section separates the regulatory context from the technical standards background. It explains why Radio Equipment Directive cybersecurity requirements, EN 18031 restrictions, and the Cyber Resilience Act increase the need for repeatable and auditable laboratory evidence.

3.1. The Radio Equipment Directive, EN 18031, and the Cyber Resilience Act

For radio equipment in the scope of the delegated act supplementing Directive 2014/53/EU, cybersecurity essential requirements are increasingly operationalized through the EN 18031 standards series [4–9,27]. Commission Implementing Decision (EU) 2025/138 adds EN 18031-1:2024, EN 18031-2:2024, and EN 18031-3:2024 to the harmonized standards

framework, with restrictions that affect the presumption of conformity under specific conditions [9]. Laboratories must therefore be able to record when a restriction-triggering condition is present and how that condition changes the evidence package, the conformity route, or the expected depth of assessment.

In parallel, Regulation (EU) 2024/2847, the Cyber Resilience Act, has shifted expectations from point-in-time conformity evidence toward lifecycle-oriented cybersecurity governance. The Act entered into force on 10 December 2024; reporting obligations begin on 11 September 2026; and the main obligations apply from 11 December 2027 [10]. For laboratories, the practical implication is that evidence packages increasingly need to support ongoing claims about vulnerability handling, update practices, and the continuity of security-relevant controls rather than only a single pre-market decision.

3.2. Harmonized Cybersecurity Standards for the Radio Equipment Directive: The EN 18031 Series

For radio equipment within the scope of the Radio Equipment Directive cybersecurity delegated act, harmonized standards define a common testable baseline for essential requirements related to network protection, protection of personal data and privacy, and fraud protection. Commission Implementing Decision (EU) 2025/138 adds the EN 18031 series as harmonized standards to support these essential cybersecurity requirements for the equipment categories listed in Delegated Regulation (EU) 2022/30 [7–9].

EN 18031 is structured into three parts that align with Radio Equipment Directive Article 3(3)(d), 3(3)(e), and 3(3)(f), respectively. From a laboratory perspective, this structure supports risk-based scoping and evidence planning: mechanisms such as access control, authentication, secure update, secure communication, logging, and resilience can be traced to specific essential requirements and tested with repeatable procedures [4–6].

The EN 18031 standards have been published with restrictions that can affect the presumption of conformity and can trigger additional assessment expectations depending on product design choices. For cybersecurity laboratories, this implies that decision rules and evidence packages must explicitly capture restricted conditions and document compensating controls or additional test depth where needed. Section 7.11 returns to these implications and provides a mechanism-oriented mapping to evidence considerations [9,27].

4. Related Work and Analytical Framing

This section positions the proposed framework in relation to recent work on cybersecurity governance, internal audit, continuous compliance, and AI-assisted evidence handling. It also introduces a literature-informed baseline comparison used to contextualize the case study findings.

4.1. Cybersecurity Governance, Internal Audit, and Assurance Monitoring

Prior work has emphasized that cybersecurity governance increasingly relies on structured audit and assurance activities, but it also shows persistent difficulty in translating high-level governance frameworks into operational testing practice. Research on cyber-risk governance [28] and internal-audit functions highlights the value of independent review, metrics, and continuous monitoring, yet also notes gaps in standardization, terminology, and data-driven continuous auditing [29,30]. These findings are consistent with the present study's focus on governance-native signals such as report integrity, decision-rule clarity, and corrective-action closure.

4.2. Automated Compliance and Continuous Compliance Architectures

Recent work on compliance automation and continuous compliance moves beyond manual, checklist-style evidence collection. A recent data-centric reference architecture for continuous compliance in DevSecOps pipelines argues that snapshot-in-time audits

struggle to capture the dynamics of continuously delivered systems and proposes embedded validation in the delivery pipeline [31]. Recent empirical work on automated endpoint compliance monitoring similarly reports operational advantages from centralized, automated evidence collection and remediation workflows, though those studies focus more on infrastructure monitoring than on laboratory conformity statements [32]. Broader compliance framework research also points toward integrated governance structures that connect legislation, risk management, and technical controls rather than treating them as separate silos [33].

4.3. AI-Assisted Evidence Handling and the Remaining Gap

AI-assisted compliance is increasingly discussed in relation to machine-readable evidence, automated requirement mapping, and data-centric orchestration, and early work suggests that such approaches can reduce friction in compliance operations [31–33]. However, the literature has not yet fully addressed how this automation should be governed inside a formal laboratory competence framework when the output is not a configuration score but a qualitative conformity statement that may be reviewed by regulators or accreditation bodies. The key gap is therefore not only technical feasibility, but also auditability: when evidence is aggregated, transformed, or prioritized automatically, the resulting record must remain reviewable, reproducible, and attributable to authorized personnel.

Table 1 summarizes the most relevant streams of prior work and their limitations relative to the present study. The gap that remains is a laboratory-centred operationalization of ISO/IEC 17025 for qualitative cybersecurity assessment that links method governance, evidence traceability, decision rules, and regulatory readiness in one quality-management design.

Table 1. Selected related work and the remaining gap addressed by this study.

Study/Stream	Primary Focus	Method/Evidence Base	Main Value	Remaining Limitations for This Paper's Problem
Cybersecurity governance and internal-audit literature [29,30]	Control monitoring, governance, continuous audit	Framework and interview-driven studies	Shows need for data-driven review and clear audit roles	Does not operationalize ISO/IEC 17025 for lab-issued conformity statements
Integrated compliance framework literature [33]	Integrated security and regulatory compliance management	Framework-oriented synthesis	Connects legislation, controls, and governance	Less specific to laboratory evidence workflows and decision rules
Continuous compliance in DevSecOps [31]	Pipeline-embedded compliance validation	Reference architecture	Shows how continuous validation can reduce compliance drift	Targets software delivery environments rather than laboratory testing and report issuance
Automated endpoint-compliance monitoring [32]	Operational benefits of automated evidence collection and monitoring	Empirical implementation study	Demonstrates practical value of automation for monitoring and remediation	Does not address qualitative conformity-statement logic

4.4. Literature-Informed Baseline Comparison

Reviewer comments asked for a clearer baseline comparison as induced in Table 2. Because the present study does not contain a controlled experiment comparing manual and automated workflows, we do not present that comparison as an empirical result of the case study. Instead, we introduce a literature-informed baseline framework that contrasts manual evidence handling with automation-assisted evidence handling across four operational domains: evidence collection, toolchain control, decision-rule application, and audit readiness. This baseline comparison serves as a structured discussion device and as a direction for future controlled evaluation rather than as a claimed experimental result of the present case.

Table 2. Literature-informed baseline comparison between manual and automation-assisted evidence workflows.

Operational Domain	Typical Manual Workflow	Automation-Assisted Workflow	Expected Effect
Evidence collection	Retrospective gathering of screenshots, logs, and narrative notes	Structured ingestion of evidence with timestamps, version context, and manifests	Lower omission risk and faster review
Toolchain control	Version context tracked inconsistently or late	Controlled inventories, baseline capture, and explicit change records	Higher reproducibility and interpretability
Decision-rule application	Rules dispersed across reviewer judgement and report text	Rules encoded in templates, review gates, and workflow logic	Lower ambiguity and better consistency
Audit readiness	Report assembly is late-stage and labour-intensive	Evidence packages are kept closer to audit-ready state throughout the workflow	Lower rework and improved traceability

5. Materials and Methods

This section describes the single-laboratory case study design, the artefacts used as data sources, the quantitative and qualitative analytical procedures, and the workflow models used to operationalize ISO/IEC 17025 for cybersecurity conformity assessment.

5.1. Research Design and Boundaries of Inference

This exploratory single-case study is based on one operational cybersecurity testing laboratory. The case study approach was selected because the objective was not to generate statistical estimates across laboratories, but to examine in practical detail how ISO/IEC 17025 requirements become cybersecurity-native artefacts and workflow controls inside a working laboratory. The unit of analysis is not a product under test, but the laboratory's evidence-production and governance system as reflected in project artefacts, corrective-action records, internal audit findings, and controlled method documents.

The central boundary condition of the study is that it does not provide cross-laboratory validation. The results therefore support an operational claim—namely, that within one laboratory workflow, explicit decision rules, structured review, and controlled evidence records reduce ambiguity and improve determinability—rather than a universal performance claim about all laboratories or all automation-assisted assessment models.

5.2. Data Sources and Analytic Integration Logic

The case study integrates four artefact classes. First, an ETSI TS 103 701 assessment workbook aligned with ETSI EN 303 645 [34] provides a draft-versus-reviewed assessment trail at the provision level. Second, an IEC 62443 corrective-action dataset provides governance-oriented nonconformity and remediation records. Third, ISO/IEC 17025 internal audit findings provide a management-system signal regarding confidentiality, authorization, document control, and review discipline. Fourth, laboratory governance artefacts—including method-selection and validation procedures, a controlled list of methods, a work instruction, and a Used Computer Master List—provide the operational substrate through which ISO/IEC 17025 clauses were instantiated in practice.

The four source classes were integrated deliberately. The ETSI workbook provides insight into verdict ambiguity and changes in determinability during structured review. The IEC 62443 action plan records show where governance and reporting problems cluster in programme-level assurance work. The internal audit findings provide a management-system signal regarding the maintenance of confidentiality [35], authorization, document control, and review discipline [36,37]. The governance artefacts then anchor these observations in the laboratory's controlled day-to-day procedures. Table 3 summarizes the analytic integration logic.

Table 3. Analytic integration of the case study data sources.

Artefact Class	Unit of Analysis	What Was Extracted	Analytical Role	Primary Research Question Served
ETSI TS 103 701 workbook	Provision/test-group row	Applicability, verdict state, reviewer notes, evidence references	Quantitative ambiguity and traceability analysis	How do structured review and evidence rules affect determinability?
IEC 62443 action plan dataset	Corrective-action row/NCR cluster	Theme, scope issue, report issue, evidence issue	Governance-gap typology	Where do assurance workflows fail before technical verdicts are finalized?
ISO/IEC 17025 internal audit records	Clause-linked finding	Finding theme, closure logic, maintenance signal	Governance-maintenance interpretation	What management-system weaknesses threaten evidence trustworthiness?
Method/toolchain governance artefacts	Controlled procedure or register	Method-control logic, validation rule, environment-control mechanism	Operationalization anchor	How are ISO/IEC 17025 clauses instantiated in practice?

5.3. Data Analysis

5.3.1. 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 [38] (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 programme audit action plan: a nonconformity-driven improvement log (nonconformity report (NCR)-based) capturing findings and corrective actions related to methodology completeness, Test Report Form (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.

5.3.2. Quantitative Analysis

The primary quantitative unit of analysis in the ETSI dataset is the provision- or test-group-level row. Extracted variables included:

- Claim/applicability state;
- Requirement type;
- Support/evidence presence;
- Verdict state;
- Reviewer commentary presence.

Four quantitative indicators were used:

- Conformity Statement Ambiguity Index (CSAI): the proportion of claimed/applicable items that remain INCONCLUSIVE at a given assessment state.
- Verdict transition counts: the number of items moving from INCONCLUSIVE or FAIL to PASS, remaining unresolved, or shifting into explicit out-of-scope states.
- Evidence Traceability Ratio: the share of reviewer-flagged items for which the final review explicitly references identifiable evidence artefacts.
- Theme frequency counts: the grouping of IEC 62443 action plan nonconformity content into methodology completeness, scope discipline, report integrity, and evidence traceability categories.

5.3.3. Qualitative Analysis

Qualitative analysis used directed thematic coding with two complementary coding frames:

- An ISO/IEC 17025-oriented frame covering method governance, technical records, reporting integrity, decision rules, and corrective-action handling.
- A Plan-Do-Check-Act assurance-maintenance frame covering scope planning, controlled execution, review and validity checks, and corrective-action closure.

Reviewer notes, audit findings, and governance documents were coded to identify recurring sources of ambiguity and the organizational mechanisms used to resolve them.

5.4. Automation Layer and Workflow Architecture

ISO/IEC 17025 specifies what must be controlled, documented, and reviewed, but cybersecurity laboratories also need a practical way to manage rapidly changing tools, large evidence volumes, and the operational pace of assessment work [39]. In the proposed

framework, automation is treated as part of the method and technical record rather than as a separate convenience layer. It orchestrates test execution, captures raw artefacts such as packet capture (PCAP) files, tool logs, and configuration snapshots, and preserves the chain from requirement to observation to verdict under controlled access and change management (ISO/IEC 17025 [11]; International Laboratory Accreditation Cooperation (ILAC) G8 [40]). Figure 1 shows the automation boundary and the end-to-end evidence traceability chain.

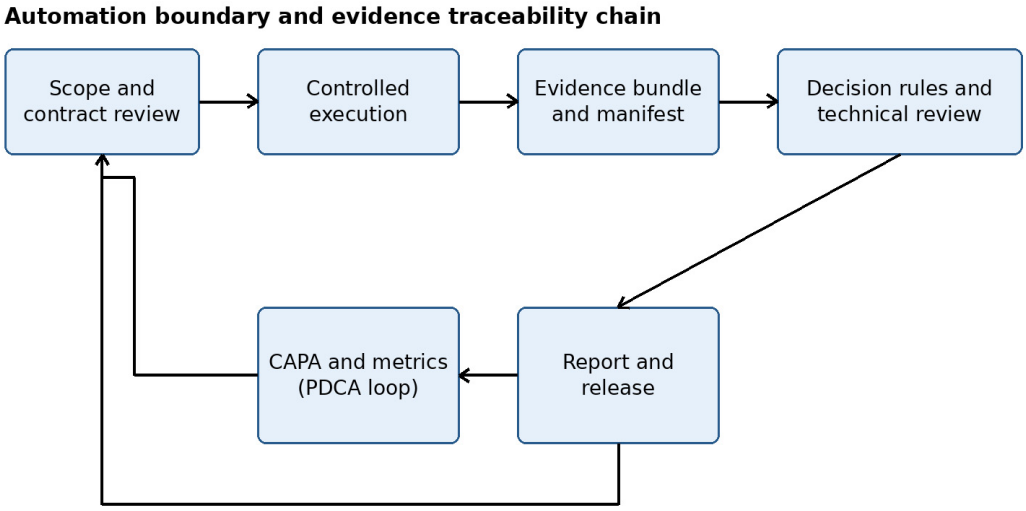


Figure 1. Automation-ready workflow architecture for ISO/IEC 17025 cybersecurity conformity assessment. The updated diagram separates the corrective and preventive action (CAPA)/metrics feedback path from content blocks and shows the scope, execution, evidence, review, reporting, and Plan-Do-Check-Act (PDCA) feedback links without overlapping arrows.

Conceptually, the workflow operates as a Plan-Do-Check-Act assurance maintenance loop. In the Plan phase, the scope is defined programmatically by combining the applicable requirement catalogue (e.g., ETSI TS 103 701, IEC 62443, EN 18031) with product-specific implementation statements (Implementation Conformance Statement (ICS) and Implementation eXtra Information for Testing (IXIT)-style artefacts) and risk context. This enables a risk-based test plan in which non-applicable requirements are filtered consistently, and any conditional applicability is documented as machine-checkable logic within the technical record.

In the Do phase, approved and version-controlled test scripts invoke validated toolchains (scanners, fuzzers, protocol analysers, static-analysis tools) within controlled environments (e.g., container images or virtual machines) whose software bills-of-materials, configuration baselines and hashes are captured automatically. Evidence is ingested into an append-only store to prevent silent modification, with cryptographic hashing and timestamping used to bind each artefact to the specific tool versions and environment images that produced it.

In the Check/Act phases, a decision engine cross-references collected evidence against pre-defined decision rules and flags nonconformities or gaps for technical review (JCGM 106 [41]). Role-Based Access Control (RBAC) and immutable audit trails enforce impartiality and confidentiality: automation generates draft verdicts, but only authorized personnel can approve exceptions, override automated outcomes, or issue final conformity statements (ISO/IEC 17025 [11]).

Table 4 summarizes how selected ISO/IEC 17025 requirements can be translated into cybersecurity workflow controls, linking clause-level expectations to controlled execution, review, and reporting practices.

Table 4. Representative mapping from ISO/IEC 17025 requirements to cybersecurity workflow controls.

ISO/IEC 17025 Requirement	Cybersecurity-Native Implementation	Why It Matters
Impartiality (Clause 4.1)	Role-based separation of duties, audit trails, controlled approval rights	Prevents silent manipulation of draft verdicts and preserves review accountability
Personnel and competence (Clause 6.2)	Controlled authorization, competence matrices, role-linked approval gates	Ensures that assessment and approval activities match competence requirements
Method selection and validation (Clause 7.2)	Version-controlled methods, change classification, re-validation triggers	Reduces toolchain drift and stabilizes method interpretation
Ensuring validity (Clause 7.7)	Review checkpoints, consistency checks, comparison planning, retrospective analytics	Supports defensible results in qualitative domains
Reporting and amendments (Clause 7.8)	Template control, explicit decision rules, amendment traceability	Protects conformity-statement clarity and longitudinal integrity

5.5. Decision Trees for Scope, Evidence, and Conformity Verdicts

To operationalise ISO/IEC 17025 decision-rule requirements in qualitative cybersecurity testing, we formalize an auditable decision tree that separates (i) applicability and scope from (ii) evidence sufficiency and (iii) acceptance evaluation. This prevents "silent" scope drift and makes the meaning of PASS/FAIL/INCONCLUSIVE reproducible across projects and reviewers.

Figure 2 sketches the decision logic used throughout the workflow. The key design choice is to treat INCONCLUSIVE as a controlled quality state: if the requirement is applicable but evidence is missing, the workflow opens a traceable gap (e.g., corrective action or evidence request) rather than forcing a PASS/FAIL judgement. This preserves auditability and reduces false acceptance risk.

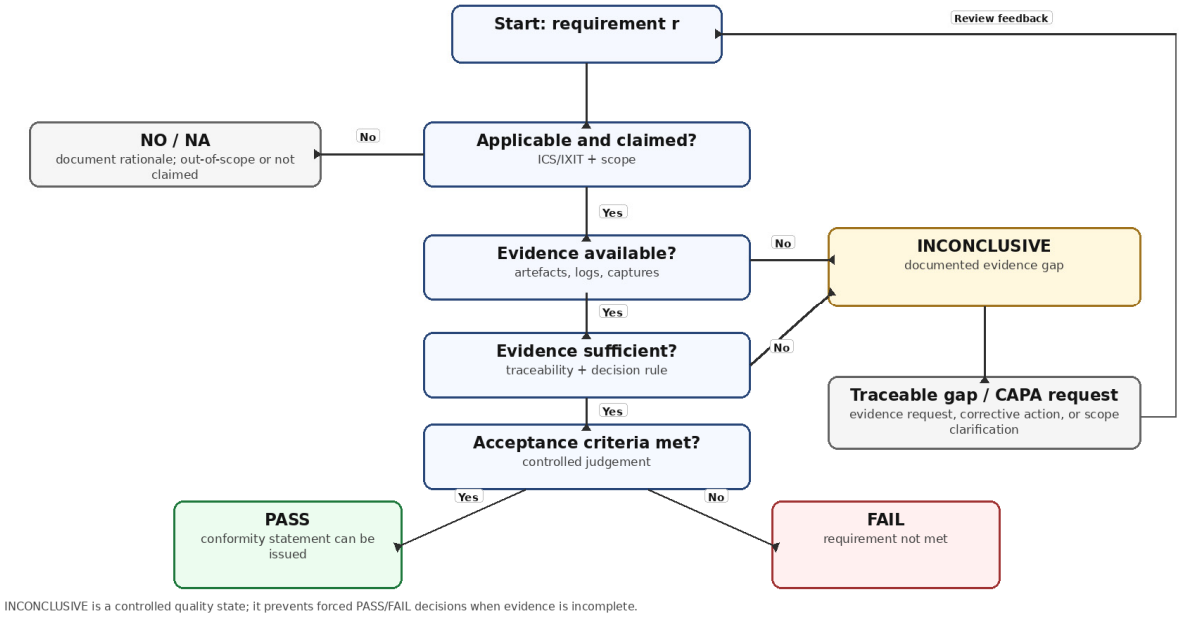


Figure 2. Decision tree for qualitative conformity outcomes in cybersecurity testing. The redrawn diagram separates applicability, evidence availability, evidence sufficiency, and acceptance evaluation while keeping feedback paths clear of the decision blocks.

5.6. Decision Tree for EN 18031 Restrictions and Conformity Route Triage

For Radio Equipment Directive cybersecurity, the EN 18031 series is published with restrictions that may remove the presumption of conformity under specific product design conditions. For laboratories, these restrictions translate into early triage questions that influence (i) which requirements must be evidenced, (ii) whether third-party assessment pathways apply, and (iii) how to structure test plans and evidence packages to withstand regulatory scrutiny.

Figure 3 provides a practical decision tree for early-stage classification. It is intended as a workflow "gate" during contract review and scope definition: the assessment team records the answers as part of the technical record, and the workflow selects the relevant EN 18031 part(s) and highlights restriction-triggering conditions that require additional assurance evidence.

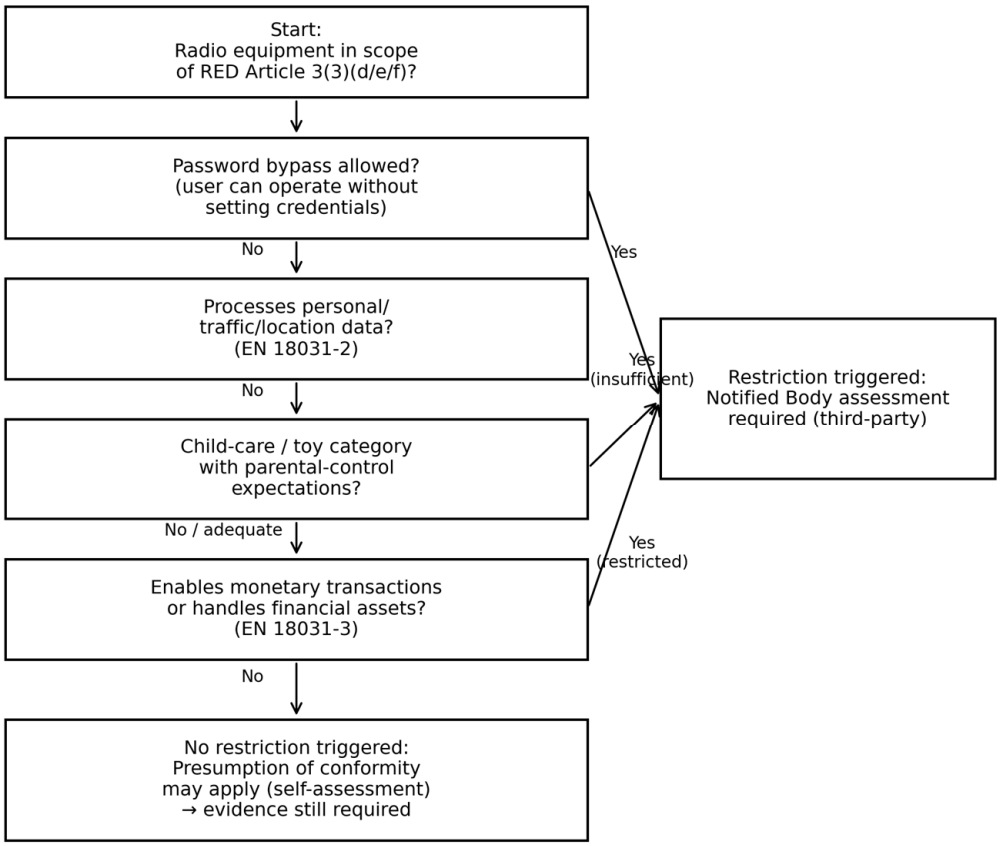


Figure 3. EN 18031 restriction triage decision tree (conceptual). Restriction-triggering conditions may remove presumption of conformity, affecting the conformity route and the depth of evidence expected in the assessment workflow.

5.7. Method Change Control and Re-Validation Triggers

Because cybersecurity toolchains evolve rapidly (scanner versions, rulesets, exploit frameworks, container images), method control must include explicit change classification and re-validation triggers. In the proposed framework, every toolchain update is logged as a change request and evaluated for impact on scope, decision rules and evidence interpretation before it can be used in accredited work.

Figure 4 sketches the decision logic used to decide whether a change requires full method validation, targeted verification (regression), or only a recorded baseline update. Treating this logic as part of the controlled method reduces drift and increases repeatability across versions and projects.

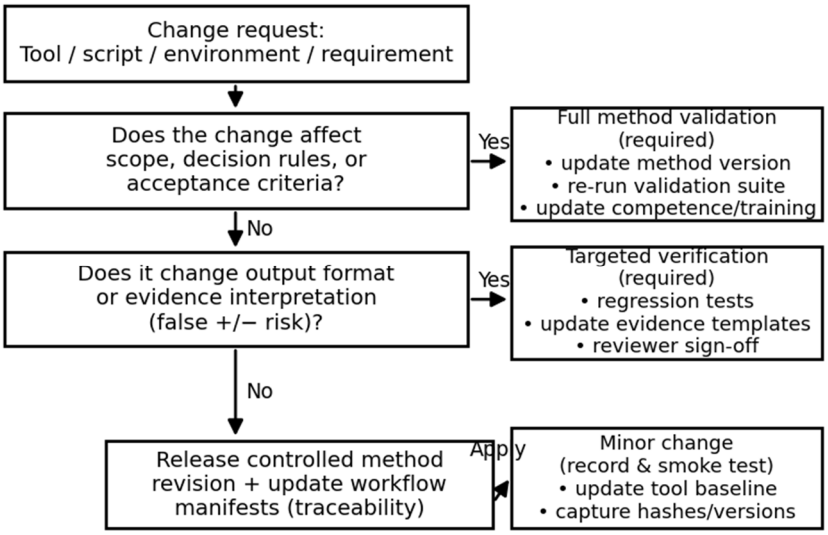


Figure 4. Method change control decision tree for cybersecurity testing laboratories (conceptual). Changes are classified by impact on scope/decision rules and on evidence interpretation to determine the required level of validation/verification before release as a controlled method revision.

The workflow figures in this section should be interpreted as design artefacts grounded in the case study evidence. They clarify the proposed control logic and operational boundaries, but they are not presented as independent numerical experiments or cross-laboratory validation results.

6. Results

This section reports the case study findings across the analyzed artefact classes. The results are presented as descriptive case study evidence and are interpreted within the stated single-laboratory boundary of inference.

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

The analyzed artefact set shows that ISO/IEC 17025 requirements can be instantiated into cybersecurity-specific records without forcing cybersecurity testing into a purely measurement-uncertainty model.

- Method identification and control: a controlled list of methods assigns internal identifiers to cybersecurity activities (e.g., ETSI/Radio Equipment Directive-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 authorized 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 [7] work instruction includes explicit steps from application evaluation to conformity assessment, report packaging, and technical 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).

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

6.2.1. 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 [42].

The draft assessment as per Table 5 state exhibited a high reliance on INCONCLUSIVE outcomes, while the reviewed state produced a substantially higher share of PASS outcomes.

Table 5. Verdict distribution before and after review in the ETSI workbook (n = 68 provisions).

Verdict Category	Draft Assessment	Reviewed Assessment	Interpretation
PASS	0	38	Most determinable claimed items become PASS only after evidence integration and review
INCONCLUSIVE	40	2	Ambiguity is concentrated in the draft state
FAIL	1	1	A small number of items remain or become negative after clarification
NO/not claimed	0	5	Review clarifies explicit out-of-scope or unclaimed items
NA/conditional not applicable	27 *	22	Draft state includes unresolved scope handling; reviewed state clarifies scope boundaries

* Draft NA count reflects the residual category after claimed/applicable items are accounted for in the 68-row dataset and should be interpreted cautiously because the draft state is less explicit about scope classes than the reviewed state.

The central quantitative finding is the reduction in the CSAI from 0.976 in the draft state (40 inconclusive outcomes among 41 claimed items) to 0.050 in the reviewed state (2 inconclusive outcomes among 40 claimed items). This is a substantial within-process reduction in ambiguity, but it should be interpreted as improved determinability within the assessed workflow rather than as external validation across laboratories or assessors.

The improvement mechanism is traceability-intensive. In the reviewed state, most claimed items became determinate only after evidence links, scope clarifications, and review notes were aligned with the laboratory decision logic.

6.2.2. Verdict Transition Analysis

The transition analysis clarifies how ambiguity was resolved during review.

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

The shares in Table 6 are descriptive case study ratios. They show which transition types dominated this particular assessment snapshot, but they are not intended as universal rates. In other laboratories, product categories, or assessment scenarios, the ratios may vary substantially depending on scope complexity, documentation maturity, toolchain stability, and the strictness of the decision rules applied.

Table 6. Verdict transition counts and descriptive shares (draft → reviewed; n = 68 provisions).

Transition	Count	Interpretation	Share of Dataset (n = 68)
INCONCLUSIVE → PASS	37	Review resolves evidence and decision-rule ambiguity	54.4%
FAIL → PASS	1	Correction and clarification change the verdict outcome	1.5%
INCONCLUSIVE → INCONCLUSIVE	2	Evidence gaps remain open at snapshot time	2.9%
INCONCLUSIVE → FAIL	1	Review shows that a mandatory expectation cannot be treated as unclaimed	1.5%
NA → NA	22	Most non-applicable items remain outside scope	32.4%
NA → NO	5	Review converts ambiguous draft scope handling into explicit not-claimed states	7.4%

6.2.3. 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.

6.2.4. 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:

- A total of ~75% referenced IXIT updates (documentation additions to support repeatable testing).
- A total of ~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.

6.3. IEC 62443 Audit Action Plan Results

The IEC 62443 action plan comprised 26 corrective-action rows grouped into four nonconformity clusters. The dominant themes were not new vulnerability discoveries

but governance and reporting weaknesses that affect the credibility and comparability of conformity work.

- 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 [43,44]).
- 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.
- Test Report Form (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.

These findings show that cybersecurity assurance quality can fail long before a laboratory reaches the point of "technical failure" in a product. Governance errors in scope definition, template handling, or evidence metadata directly undermine the comparability and credibility of conformity statements.

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).

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

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 International Laboratory Accreditation Cooperation (ILAC) G8 [40] (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).

The internal audit findings reinforce the governance-heavy character of cybersecurity conformity assessment. The case study audit data shows minor nonconformities around confidentiality governance, responsibilities and signatory authorization, external service records (including cloud-service dependencies), fit-for-purpose interlaboratory comparison planning for qualitative outcomes, report-template suitability for qualitative testing, the statement of decision rules, re-issued report traceability, and risk-and-opportunity management. None of these items is a technical exploit in itself; yet each affects the trustworthiness, confidentiality, or reproducibility of the laboratory's work.

Interpreted through a maintenance lens, these findings are leading indicators of governance degradation. They show where "assurance downtime" can emerge: not only from poor test execution, but from weak authorization records, ambiguous decision rules, or insufficient document revision control. In this sense, internal audit functions as preventive maintenance for the laboratory's quality system.

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" [29] that complement technical test KPIs and support sustained comparability and defensibility of conformity statements in fast-evolving security test domains.

6.5. Cross-Dataset Synthesis of Findings

Across the four artefact classes, five consolidated findings emerge.

- Decision rules are the principal lever for reducing ambiguity in qualitative cybersecurity conformity assessment.
- Evidence quality is often limited not by the absence of technical activity, but by the absence of explicit, traceable links between observations, artefacts, and verdicts.
- Toolchain control matters because evidence interpretability depends on environment state, version context, and controlled change.
- Governance deviations, especially in authorization, report integrity, and document control, act as early warning indicators of future conformity-statement instability.
- EN 18031 and Radio Equipment Directive restrictions make early-stage restriction triage a practical necessity because restricted clauses alter both evidence expectations and the possible conformity route.

7. Discussion

This section interprets the results in relation to ISO/IEC 17025 operationalization, prior work, automation-assisted evidence handling, Radio Equipment Directive readiness, and the limitations of the present case study design.

7.1. Why the Results Support ISO/IEC 17025 Operationalization 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 [45]/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 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.

7.2. 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 International Laboratory Accreditation Cooperation (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.

Two discussion implications follow:

- "Inconclusive" is not a failure of testing; it is a controlled quality state, where evidence expectations are recognized but not met, preserving an inconclusive outcome prevents false passes and enables later reassessment without reconstructing context.
- "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.

7.3. Relation to Existing Studies

This positioning is consistent with the related literature. Recent continuous-compliance and compliance-automation work emphasizes data-centric evidence handling, embedded validation, and reduced dependence on manual, episodic evidence collection [31–33]. Internal-audit research similarly highlights the growing role of data-driven review, control monitoring, and cross-functional coordination in cybersecurity governance [30]. The present study complements these strands by focusing on a laboratory setting where the final output is not only a dashboard or compliance score, but a laboratory-controlled conformity statement that must remain reviewable and defensible. That is the point at which ISO/IEC 17025 becomes decisive.

7.4. 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. externalized work terminology), which can introduce interpretive noise and inconsistent reporting expectations (Clause 7.8.3).
- 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 externalized (Clause 6.6.2).
- Document control sensitivity points, including periodic review and consistent revision-state identification, directly affect whether a given test was executed under the correct controlled method and template revision (Clauses 8.2/8.3—critical points).

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.

Moreover, the literature-informed baseline comparison in Table 2 clarifies why automation matters in this domain. Manual evidence workflows tend to rely on retrospective collection of screenshots, scattered logs, manually curated spreadsheets, and narrative justifications reconstructed late in the process. Automation-assisted workflows, by contrast, can bind evidence to scope decisions, toolchain versions, timestamps, and review checkpoints earlier and more consistently. The value proposition is therefore not "full automation of compliance decisions," but better provenance, faster reviewability, and lower ambiguity when technical review occurs. This framing responds directly to reviewer requests for baseline logic while remaining honest about the limits of the present empirical dataset.

7.5. 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 definition, decision rules, and cyber-specific risk models determine whether the assurance chain is stable before testing begins.
- Do: Controlled execution depends on fit-for-purpose templates, controlled external-provider interfaces, technical records, and disciplined handling of tooling and environments.
- Check: Completeness review, internal audit, and inter-laboratory validity mechanisms help detect ambiguity, comparability gaps, and qualitative PASS/FAIL validity issues.
- Act: Corrective actions update procedures, templates, decision rules, competence records, and risk registers, with closure timeliness treated as a measurable maintenance parameter.

7.6. 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:

- 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 $\rightarrow$ 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 nonconformity report (NCR) creation to verified closure (internal audit and programme action plans). Interpretation: Governance means time to repair (MTTR); it measures how quickly the laboratory restores assurance and 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.

7.7. AI-Augmented Evidence Engineering for Continuous Compliance

A practical extension of the proposed framework is to use AI not to replace conformity decisions, but to reduce the friction of producing and maintaining traceable evidence. In laboratory settings, much of the effort is spent on transforming heterogeneous technical

artefacts—captures, logs, scanner outputs, configuration snapshots, design documents—into a structured evidence package that can be reviewed and defended. Natural language processing can support this step by classifying artefacts, extracting salient claims (e.g., which interface is in scope), and proposing links between requirements, test cases, and concrete evidence items. For example, an LLM can draft an "evidence index" for each provision, pointing to the exact log section or capture that supports a PASS verdict, while an analyst validates every citation before the report is released.

Used carefully, such tooling aligns well with the assurance maintenance loop: evidence packages become living, versioned assets, and AI can help detect when an update invalidates prior assumptions. Model-assisted diffing of device documentation (e.g., IXIT changes), firmware release notes, or test scripts can flag drift that should trigger reassessment. Similarly, anomaly detection over toolchain telemetry can highlight sudden shifts in scanner behaviour or configuration that might otherwise remain invisible until an audit. The outcome is not "automated compliance," but faster, more consistent identification of what must be re-tested and which governance records must be updated.

Reviewer comments correctly called for stronger emphasis on automation while also making clear that conceptual elements should not be overstated. In that spirit, the revised paper positions AI as an evidence-engineering aid rather than a conformity decision-maker. Practical uses include requirement-to-evidence indexing, artefact classification, log triage, and drift detection between controlled baselines. However, any AI-supported output that enters the technical record should be treated as a controlled intermediate artefact: it requires versioning, review, traceable source references, and explicit human sign-off.

This control perspective is consistent with current AI governance guidance and with the management-system logic of ISO/IEC 17025. The relevant question is not whether an AI model can generate plausible text, but whether the evidence chain remains auditable, reproducible, and attributable after the model is introduced. For laboratories handling sensitive client material, confidentiality and data-protection constraints further favour local or dedicated deployments and careful retention policies.

Because compliance evidence is only valuable when it is auditable, any AI-generated intermediate artefact should be treated as a controlled record: it needs a defined purpose, versioning, and a clear reviewer sign-off. Risk management frameworks for AI, such as the NIST AI RMF [46], are useful here because they emphasize transparency, traceability, and monitoring across the AI lifecycle [47].

7.8. Trustworthy AI Controls for Compliance Evidence Quality

Introducing AI into a laboratory workflow creates a new class of "method components" that can affect verdicts and the interpretability of evidence. From an ISO/IEC 17025 perspective, this suggests three concrete controls. First, the laboratory should define the AI system's role and boundaries: what it is allowed to propose (e.g., candidate links, summaries, prioritization) and what it must never decide (e.g., final conformity statements). Second, the laboratory should validate the AI component for its intended use, in the same spirit as method validation: test sets should reflect the laboratory's artefacts and domains, and performance criteria should include error modes that matter for compliance, such as false evidence links or overconfident summaries. Third, the laboratory should monitor drift and reproducibility: model version, prompting templates, and retrieval corpora must be controlled so that the same input produces stable outputs, or deviations are explainable and recorded.

Organizational AI governance standards and guidance can be mapped onto these needs. ISO/IEC 42001, for instance, frames an Artificial Intelligence Management System (AIMS) with continuous improvement and risk-based controls that fit naturally with the

PDCA logic used in this paper [48]. Where AI is used for high-impact decisions, the EU Artificial Intelligence Act's risk-based obligations are also relevant to consider, especially regarding documentation, transparency, and human oversight [49].

In practice, laboratories can operationalise "AI evidence quality" with measurable indicators similar to CSAI: (i) citation coverage (share of AI-produced statements that are backed by an explicit artefact reference), (ii) reviewer override rate (how often a reviewer rejects an AI suggestion), and (iii) reproducibility rate (how often repeated runs under controlled settings yield materially different outputs). These metrics do not require perfect AI; they require visibility into error and control over correction.

7.9. Data Privacy and Confidentiality in AI-Assisted Assurance Workflows

Cybersecurity testing laboratories routinely process highly sensitive information: product architectures, vulnerability details, credentials, customer logs, and sometimes personal data. Artificial intelligence (AI) adoption therefore intersects directly with confidentiality commitments, client contracts, and data protection law. A simple design choice, such as sending artefacts to a hosted model application programming interface (API) for summarisation, may trigger cross-border data transfers, new processors or sub-processors, and retention risks that are incompatible with the laboratory's obligations. In European contexts, personal data processing must meet General Data Protection Regulation (GDPR) requirements such as purpose limitation, data minimisation, and appropriate technical and organizational measures [50].

Several privacy-preserving patterns are compatible with the framework proposed in this paper. When feasible, laboratories can prefer local or dedicated deployments of models so that raw evidence never leaves the controlled environment. Where data must be shared for benchmarking or inter-laboratory learning, techniques such as differential privacy can help limit disclosure risk while still enabling statistical insights [51]. Federated learning can support cross-laboratory model training without centralizing raw datasets, although it introduces its own operational and security challenges that must be addressed explicitly [52].

Finally, privacy and evidence quality are linked: aggressive redaction can make a verdict non-reproducible, while over-retention can create unnecessary exposure. The management system should therefore document a defensible balance: what is retained, for how long, under which access controls, and how privacy-preserving transformations are applied without breaking traceability. Treating privacy controls as first-class governance records—rather than as an afterthought—helps ensure that AI-enabled automation strengthens compliance evidence instead of undermining it.

7.10. Evidence Analytics and Deep Data Analysis Roadmap

The case study results show that governance artefacts (decision rules, evidence traceability and technical review) can be treated as measurable quality signals rather than as purely procedural requirements. Beyond descriptive counts of PASS/FAIL/INCONCLUSIVE outcomes, laboratories can extend the assurance maintenance loop with an analytics layer that monitors drift, detects anomalous patterns in evidence quality, and supports risk-based prioritization of retesting. This aligns with metric programmes such as ISO/IEC 27004 and operational resilience monitoring in OT environments (ISO/IEC 27004 [29]; NIST SP 800-82 [53]).

In practice, this means treating test and audit artefacts as time-series and graph data: toolchain versions, requirement applicability decisions, defect types, remediation lead times, and evidence completeness can be analyzed to identify weak control points. Statistical process control and probabilistic modelling support early warning indicators, while machine-learning methods support scalable triage in large assurance datasets. Table 7

summarizes a non-exhaustive set of analytical methods that are directly applicable to cybersecurity assurance and conformity evidence data.

Table 7. Advanced analytical methods applicable to cybersecurity assurance and conformity evidence data.

Analytical Methodology	Primary Application in Cybersecurity	Core Mathematical/Statistical Mechanism
Statistical Anomaly Detection	Identifying deviations in user behaviour or network traffic	Z-scores, Exponentially Weighted Moving Averages (EWMA), and Chi-square hypothesis testing
Bayesian Networks	Dynamic risk assessment and causal inference in OT environments	Updating the probability of a hypothesis (e.g., an attack is occurring) as more evidence or information becomes available
Monte Carlo Simulations	Forecasting potential financial loss and risk exposure	Repeated random sampling of uncertain variables (attack frequency, breach cost) to generate loss exceedance probability curves
Principal Component Analysis (PCA)	Dimensionality reduction for massive network datasets (e.g., IoT-23)	Orthogonal transformation converting observations of correlated variables into a set of linearly uncorrelated principal components
Density-Based Clustering (DBSCAN)	Identifying distinct operational states and isolating network outliers	Grouping points that are closely packed together while marking points that lie alone in low-density regions as anomalies

7.11. EN 18031 Restrictions and Evidence Implications for Radio Equipment Directive Readiness

The EN 18031 series provides a mechanism-oriented structure summarized in Table 8 for Radio Equipment Directive cybersecurity essential requirements and therefore offers an opportunity to standardize evidence expectations across laboratories. At the same time, the harmonized EN 18031 standards were published with restrictions that can affect the presumption of conformity and can require additional depth of assessment depending on product design choices (Commission Implementing Decision (EU) 2025/138 [9]; DEKRA guidance [27]). For laboratories operating under ISO/IEC 17025, these restrictions should be treated as explicit decision-rule inputs: they must be detectable during scoping, traceable in the technical record, and reflected in the issued conformity statement.

Practically, this implies three evidence-planning tasks:

- Package evidence in a way that supports internal technical review and, when applicable, Notified Body assessment.
- Map product information to restricted clauses and select compensating or additional tests where required.
- Collect structured product information, such as onboarding flows, authentication choices, parental or guardian controls, and secure-update categories for monetary-value equipment.

For laboratories supporting products under the Radio Equipment Directive, EN 18031 restrictions make decision-rule engineering and scope triage especially important. Restriction-triggering product characteristics can change the presumption-of-conformity logic and the expected depth of evidence. Laboratories therefore need a contract review and scoping mechanism that records these triggers early and ensures that the technical

record explicitly captures them. The framework developed here provides a practical way to do that by connecting scoping logic, evidence manifests, and report-generation rules.

Table 8. EN 18031 mechanisms relevant to Radio Equipment Directive cybersecurity conformity assessment and corresponding evidence considerations.

Mechanism Code	Mechanism Name	Technical Implementation and Assessment Requirements	Relevant EN Standard
ACM	Access Control Mechanism	Ensures that only authorized entities can access security, network, privacy, or financial assets. Requires defined privilege boundaries and the prevention of unauthorized privilege escalation	EN 18031-1, -2, -3
AUM	Authentication Mechanism	Verifies the identity of users or external entities before granting system access. Strictly prohibits the use of hard-coded default passwords and mandates robust password strength evaluation or cryptographic pairing	EN 18031-1, -2, -3
SUM	Secure Update Mechanism	Facilitates the secure, verifiable installation of new firmware. Requires cryptographic verification of software integrity (e.g., digital signatures) and architectural protection against rollback or downgrade attacks	EN 18031-1, -2, -3
SSM	Secure Storage Mechanism	Protects sensitive assets stored on the physical device from unauthorized read/write access. Necessitates robust encryption for data at rest and potentially isolated execution environments	EN 18031-1, -2, -3
SCM	Secure Communication	Safeguards data transmitted over external network interfaces. Requires the implementation of modern cryptographic protocols (e.g., TLS 1.2/1.3) to guarantee confidentiality, integrity, authenticity, and anti-replay protection	EN 18031-1, -2, -3
LGM	Logging Mechanism	Generates and securely stores records of security-relevant events to aid in incident response and anomaly detection	EN 18031-1, -2, -3
DLM	Deletion Mechanism	Provides the user with a simple, irreversible method to delete all personal data and configuration settings prior to device disposal or transfer	EN 18031-2
RSM	Resilience Mechanism	Ensures the device can withstand and recover from network-based attacks, such as Denial of Service (DoS), without exhausting broader network resources	EN 18031-1

The Cyber Resilience Act reinforces the same direction of travel. Because the Act increasingly emphasizes lifecycle obligations, manufacturers and testing partners need evidence that can survive updates, re-assessment, and vulnerability-handling cycles. A laboratory quality system that treats evidence as a versioned, auditable asset is better aligned with this trajectory than one that relies on static report assembly at the end of a project.

7.12. Limitations and Future Work

The main limitation is the single-laboratory design. A single case can show how the framework is instantiated and how it affects one assessment workflow, but it cannot establish how far the results generalize. Broader validation would require multi-laboratory comparison, repeated-case designs, and formal evaluation of inter-assessor consistency. A second limitation is that the manual-versus-automation comparison is a structured discussion framework rather than an experiment conducted within this study. A third limitation is that some workflow elements remain design artefacts grounded by the case rather than independently benchmarked software components.

Future work should therefore proceed in four directions. First, multi-laboratory intercomparison designs are needed for qualitative PASS/FAIL/INCONCLUSIVE domains. Second, controlled baseline studies should compare manual and automation-assisted evidence workflows on ambiguity, review time, rework, and report integrity. Third, longitudinal studies should examine how toolchain drift affects evidence interpretability over time. Fourth, AI-assisted evidence handling should be evaluated against reproducibility, citation coverage, reviewer override rates, and confidentiality constraints rather than general language model performance metrics.

8. Conclusions

This paper set out to make a bounded contribution: to show, in operational detail, how one cybersecurity testing laboratory translated ISO/IEC 17025 clauses into workflow controls for qualitative conformity assessment, and to examine what changed when those controls were applied. The study does not claim field-wide validation. Its value lies in the close analysis of one laboratory, one assessment workflow, and the evidence available within that boundary.

The central empirical result is the reduction in the CSAI from 0.976 to 0.050 between the draft and reviewed ETSI TS 103 701 workbook, indicating a substantial decrease in unresolved ambiguity within the assessed process. Read alongside the IEC 62443 corrective-action records, the internal audit findings, and the governance artefacts, this result supports a consistent conclusion: technical expertise is necessary for cybersecurity conformity assessment, but it is not sufficient. A laboratory must also explain its scope decisions, bind evidence to verdicts, and preserve auditability through change.

From a regulatory perspective, the framework gives laboratories a practical way to handle EN 18031 and Radio Equipment Directive readiness by treating restriction logic and evidence expectations as scoping issues rather than as late reporting tasks. More broadly, the paper argues that assurance in cybersecurity testing is not a one-time achievement. It is a property that must be actively maintained through measurable indicators and a corrective-action loop that verifies closure.

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 work received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets and laboratory artefacts analyzed 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: Author Aymen Gatri was employed by Teligencia Labs SARL. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

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-Centred 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. 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; p. L_202402847.
2. 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).
3. 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).
4. *EN 18031-1:2024*; Common Security Requirements for Radio Equipment—Part 1: Internet Connected Radio Equipment. European Committee for Standardization and European Committee for Electrotechnical Standardization: Brussels, Belgium, 2024.
5. *EN 18031-2:2024*; Common Security Requirements for Radio Equipment—Part 2: Radio Equipment Processing Data, Namely Internet Connected Radio Equipment, Childcare Radio Equipment, Toys Radio Equipment and Wearable Radio Equipment. European Committee for Standardization and European Committee for Electrotechnical Standardization: Brussels, Belgium, 2024.
6. *EN 18031-3:2024*; Common Security Requirements for Radio Equipment—Part 3: Internet Connected Radio Equipment Processing Virtual Money or Monetary Value. European Committee for Standardization and European Committee for Electrotechnical Standardization: Brussels, Belgium, 2024.

7. 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: Luxembourg, 2014. Available online: https://eur-lex.europa.eu/eli/dir/2014/53/oj/eng (accessed on 15 February 2026).
8. 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: Luxembourg, 2022. Available online: https://eur-lex.europa.eu/eli/reg_del/2022/30/oj/eng (accessed on 15 February 2026).
9. 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: Luxembourg, 2025. Available online: https://eur-lex.europa.eu/eli/dec_impl/2025/138/oj/eng (accessed on 15 February 2026).
10. 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: Luxembourg, 2024. Available online: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (accessed on 15 February 2026).
11. *ISO/IEC 17025:2017*; General Requirements for the Competence of Testing and Calibration Laboratories. International Organization for Standardization (ISO): Geneva, Switzerland, 2017. Available online: https://www.iso.org/standard/66912.html (accessed on 15 February 2026).
12. *ISO/IEC 17025*; A Complete Guide to Lab Accreditation. IntuitionLabs: San Jose, CA, USA, 2025. Available online: https://intuitionlabs.ai/pdfs/iso-iec-17025-a-complete-guide-to-lab-accreditation.pdf (accessed on 15 February 2026).
13. *ISO 9000:2015*; Quality Management Systems—Fundamentals and Vocabulary. International Organization for Standardization (ISO): Geneva, Switzerland, 2015.
14. Kuckartz, U.; Rädiker, S. *Qualitative Content Analysis: Methods, Practice and Software*; SAGE Publications: London, UK, 2023.
15. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2022.
16. *IEC 62443-4-1:2018*; Security for Industrial Automation and Control Systems—Part 4-1: Secure Product Development Lifecycle Requirements. International Electrotechnical Commission (IEC): Geneva, Switzerland, 2018.
17. *IEC TR 62443-2-3:2015*; Security for Industrial Automation and Control Systems—Part 2-3: Patch Management in the IACS Environment. International Electrotechnical Commission (IEC): Geneva, Switzerland, 2015.
18. *IEC 62443-3-3:2013*; Industrial Communication Networks—Network and System Security—Part 3-3: System Security Requirements and Security Levels, Edition 1.0. International Electrotechnical Commission (IEC): Geneva, Switzerland, 2013.
19. *IEC 62443-2-1:2010*; Industrial Communication Networks—Network and System Security—Part 2-1: Establishing an Industrial Automation and Control System Security Program. International Electrotechnical Commission (IEC): Geneva, Switzerland, 2010.
20. 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).
21. *IECEE 02:2020*; Scheme of the IECEE for Mutual Recognition of Test Certificates for Electrotechnical Equipment and Components (CB Scheme)—Rules of Procedure. International Electrotechnical Commission: Geneva, Switzerland, 2020. Available online: https://www.document-center.com/standards/show/IECEE-02 (accessed on 7 May 2026).
22. *IEC 60300-3-11:2009*; Dependability Management—Part 3-11: Application Guide—Reliability Centred Maintenance. International Electrotechnical Commission (IEC): Geneva, Switzerland, 2009. Available online: https://webstore.iec.ch/en/publication/1296 (accessed on 19 April 2026).
23. Bukowski, L.; Werbinska-Wojciechowska, S. Towards Maintenance 5.0: Resilience-Based Maintenance in AI-Driven Sustainable and Human-Centric Industrial Systems. *Sensors* **2025**, *25*, 5100. [CrossRef] [PubMed]
24. 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. [CrossRef] [PubMed]
25. 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. [CrossRef]
26. 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).
27. DEKRA. *Guidance for RED-DA Restrictions in EN 18031 Harmonized Standards*; DEKRA: Stuttgart, Germany, 2025. Available online: https://dekraprod-media.e-spirit.cloud/416969f7-5dae-4948-b0f6-809804143c1e/media/dekra-red-da-guidance-standards-harmonization.pdf (accessed on 5 March 2026).
28. Otkhozoria, N.; Petriashvili, L.; Zhvania, T.; Lortkipanidze, N. Information Risk Analysis in Laboratories Complying with ISO/IEC 17025 Standard. *Int. Sci. J. Eng. Agric.* **2025**, *4*, 50–61. [CrossRef]

29. *ISO/IEC 27004:2016*; Information Technology—Security Techniques—Information Security Management—Monitoring, Measurement, Analysis and Evaluation. International Organization for Standardization: Geneva, Switzerland, 2016.
30. Ferreira, L.V.A.; Alves, C.A.d.M.; Peotta de Melo, L.; Nunes, R.R. Internal Audit Strategies for Assessing Cybersecurity Controls in the Brazilian Financial Institutions. *Appl. Sci.* **2025**, *15*, 5715. [CrossRef]
31. Zakharchenko, A. Integrating Continuous Compliance into DevSecOps Pipelines: A Data Engineering Perspective. *Software* **2026**, *5*, 6. [CrossRef]
32. Morić, Z.; Balković, M.; Isić, D. Evaluating the Operational Impact of Automated Endpoint Compliance and Security Monitoring in Linux Environments. *J. Cybersecur. Priv.* **2026**, *6*, 61. [CrossRef]
33. Grigaliūnas, Š.; Schmidt, M.; Brūzgienė, R.; Smyrli, P.; Andreou, S.; Lopata, A. Holistic Information Security Management and Compliance Framework. *Electronics* **2024**, *13*, 3955. [CrossRef]
34. *ETSI EN 303 645 V2.1.1 (2020-06)*; Cyber Security for Consumer Internet of Things: Baseline Requirements. ETSI: Sophia Antipolis, France, 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).
35. LLumin. *Cybersecurity Best Practices for Maintenance Systems*; LLumin: Springfield, MA, USA, 2025. Available online: https://llumin.com/blog/cybersecurity-best-practices-for-maintenance-systems/ (accessed on 15 February 2026).
36. Basson, M.; Aladon. *Reliability Centered Maintenance (RCM3): Risk-Based Reliability Centered Maintenance*; Industrial Press: New York, NY, USA, 2019.
37. Molęda, M.; Małysiak-Mrozek, B.; Ding, W.; Sunderam, V.; Mrozek, D. From Corrective to Predictive Maintenance—A Review of Maintenance Approaches for the Power Industry. *Sensors* **2023**, *23*, 5970. [CrossRef] [PubMed]
38. *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.
39. SentinelOne. *Cybersecurity Metrics & KPIs: What to Track in 2026*; SentinelOne: Mountain View, CA, USA, 2026. Available online: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-metrics/ (accessed on 15 February 2026).
40. *ILAC-G8:09/2019*; Guidelines on Decision Rules and Statements of Conformity. International Laboratory Accreditation Cooperation (ILAC): Newton, Australia, 2019. Available online: https://www.iasonline.org/wp-content/uploads/2021/03/ILAC_G8_09_2019.pdf (accessed on 15 February 2026).
41. *JCGM 106:2012*; Evaluation of Measurement Data—The Role of Measurement Uncertainty in Conformity Assessment. Joint Committee for Guides in Metrology (JCGM): Sèvres, France, 2012.
42. Industrial Cyber. *Cybersecurity Best Practices in the Manufacturing Sector*; Industrial Cyber: Elsternwick, Australia, 2024. Available online: https://industrialcyber.co/manufacturing/cybersecurity-best-practices-in-the-manufacturing-sector/ (accessed on 15 February 2026).
43. 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; p. L_202400482.
44. *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.
45. *ISO/IEC 13528:2022*; Statistical Methods for Use in Proficiency Testing by Interlaboratory Comparison. International Organization for Standardization: Geneva, Switzerland, 2022.
46. Scarfone, K.; Souppaya, M.; Cody, A.; Orebaugh, A. *Technical Guide to Information Security Testing and Assessment*; NIST Special Publication 800-115 2008; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2008. [CrossRef]
47. National Institute of Standards and Technology (NIST). *Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1)*; NIST: Gaithersburg, MD, USA, 2023. [CrossRef]
48. *ISO/IEC 42001:2023*; Information Technology—Artificial Intelligence—Management System. International Organization for Standardization: Geneva, Switzerland, 2023.
49. European Union. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*; Official Journal of the European Union: Luxembourg, 2024.
50. European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*; Official Journal of the European Union: Luxembourg, 2016.
51. Dwork, C.; Roth, A. *The Algorithmic Foundations of Differential Privacy*; Foundations and Trends in Theoretical Computer Science; Now Publishers: Hanover, MA, USA, 2014.

52. McMahan, H.B.; Moore, E.; Ramage, D.; Hampson, S.; Agüera y Arcas, B. Communication-Efficient Learning of Deep Networks from Decentralized Data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS 2017), Fort Lauderdale, FL, USA, 20–22 April 2017; PMLR 54.
53. National Institute of Standards and Technology (NIST). *Guide to Operational Technology (OT) Security (SP 800-82 Rev. 3)*; NIST: Gaithersburg, MD, USA, 2023. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.