Revision

Ann PUBLISHER Journal Engineering Sciences (Improsci)
e-ISSN 3031-7088
p-ISSN 3032-3452

Digital Transformation of Technical Import Traceability Verification (VPTI): ISO/IEC 17020:2012 Conformity Analysis in the Implementation of Artificial Intelligence, *Internet of Things*, and Inspection Automation

Heri Setiawan [1], Andri Hermawan [2]

[1] Department of Industrial Engineering, Faculty of Science and Technology, Musi Charitas Catholic University, Palembang, Indonesia, ORCID ID: 0009-0007-6368-8673. Email heri_setiawan@ukmc.ac.id

[2] Faculty of Industrial Engineering, University of Muhammadiyah Cirebon. ORCID ID 0009-0008-9011-0786. Email: andri.hermawan@umc.ac.id

Corresponding Author. Email: heri_setiawan@ukmc.ac.id

Abstract

Background. Technical Import Tracking Verification (VPTI) is a verification activity whose implementation must follow the government's mandate and provisions, as well as the relevant inspection agency's scope of assignment. Digitalization, artificial intelligence (AI), the Internet of Things (IoT), and automation can help with document tracking, data collection, and consistency in the inspection process.

Objectives. This study aims to map the relevant requirements of ISO/IEC 17020:2012 to the use of AI, IoT, and automation in VPTI and to formulate a risk-based implementation strategy. This article treats the term "impact" as a potential risk of nonconformity that needs to be tested, rather than as an explicit prohibition in the standard.

Methods. The research uses document analysis of ISO/IEC 17020:2012 and supporting literature/guidelines, technology mapping of relevant clauses, and the preparation of a qualitative risk matrix. Because the manuscript does not present a literature search protocol, case study selection criteria, or evidence of direct consultation with KAN, the results are interpreted as an initial conceptual analysis, not an empirical verification or KAN's official position.

Results. The mapping shows that the main concerns lie in impartiality and confidentiality (Clause 4), personnel competence (6.1), facilities and equipment (6.2), inspection methods/procedures (7.1), inspection records (7.3), inspection reports (7.4), complaint and appeal handling (7.5), and management systems including management reviews (Clause 8).

Conclusion. Proposed a four-stage roadmap for administrative digitalization, IoT device integration, the use of AI as a validated tool, and formal evaluation with accreditation parties if necessary. The stages and time range are the author's proposal, not the requirements or schedules set by ISO/IEC 17020:2012 or KAN.

Keywords: VPTI, ISO/IEC 17020:2012, artificial intelligence, Internet of Things, risk management.

© 2026 The Author(s). This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source.

INTRODUCTION

The digital transformation of international trade and industrial inspection systems has become increasingly important as global supply chains demand greater efficiency, transparency, accuracy, and regulatory accountability. The growing complexity of cross-border transactions, diversification of imported commodities, and increasing volume of trade documentation have created significant challenges for inspection institutions responsible for verifying compliance with technical and administrative requirements. In Indonesia, Technical Import Traceability Verification (VPTI) represents an important mechanism for supporting the verification of imported goods in accordance with applicable government regulations and institutional mandates. These activities may involve examining product specifications, quantities, values, Harmonized System (HS) classifications, and supporting documentation. Consequently, inspection institutions must ensure that their verification processes are technically reliable, traceable, impartial, and consistent with applicable conformity assessment requirements.

The implementation of VPTI requires an appropriate institutional governance framework, particularly where inspection activities fall within the accredited scope of an inspection body. ISO/IEC 17020:2012 provides internationally recognized requirements concerning the competence, impartiality, and consistent operation of bodies performing inspections (ISO, 2012). The standard addresses general requirements, structural arrangements, personnel competence, facilities and equipment, inspection methods, inspection records, reporting, and management systems. These requirements establish an important foundation for maintaining confidence in inspection results. Nevertheless, the increasing adoption of digital technologies introduces new operational and governance considerations that need to be systematically evaluated within the existing conformity assessment framework.

Recent developments associated with Industry 4.0 have created opportunities to transform conventional inspection activities through Artificial Intelligence (AI), the Internet of Things (IoT), machine vision, digital traceability systems, and Robotic Process Automation (RPA). AI-based applications can potentially support document recognition, HS code classification, anomaly detection, and consistency checks, while IoT-enabled sensors may facilitate automated data acquisition, equipment monitoring, and the recording of physical inspection parameters. Similarly, digital workflow automation can improve document management, inspection scheduling, information retrieval, and reporting processes. When appropriately designed and controlled, these technologies may improve operational efficiency, data consistency, and the traceability of inspection activities.

However, technological capabilities do not automatically establish regulatory conformity. AI-assisted inspection introduces potential risks associated with algorithmic errors, data quality, model transparency, human oversight, and the allocation of responsibility for inspection decisions. IoT-based measurement systems raise additional considerations regarding equipment suitability, calibration or verification, measurement reliability, cybersecurity, and the integrity of recorded data. Automated workflows may also create risks involving unauthorized data modification, insufficient audit trails, inadequate access controls, and unclear approval responsibilities. These issues are particularly important for accredited inspection institutions because technological changes may affect the methods, resources, records, and organizational controls used to demonstrate compliance with ISO/IEC 17020:2012.

State of the Art

Existing developments in digital inspection and conformity assessment demonstrate the potential contribution of intelligent technologies to operational modernization. AI and machine learning provide analytical capabilities for processing complex documentation, recognizing patterns, and identifying potentially inconsistent information. IoT technologies enable the integration of physical measurement devices with digital information systems, while automated data management facilitates the documentation and retrieval of inspection evidence. Related studies on industrial automation, intelligent sensing, and digital information systems provide a technological foundation for improving inspection processes.

Nevertheless, the relevance of these technologies to accredited inspection activities must be distinguished from their general technical performance. A machine learning model that demonstrates satisfactory classification performance does not necessarily satisfy the procedural, competence, impartiality, and documentation requirements applicable to an inspection body. Similarly, the availability of real-time sensor data does not independently establish the reliability of inspection results without appropriate equipment controls, measurement procedures, and data integrity safeguards.

From a regulatory perspective, ISO/IEC 17020:2012 establishes a framework for inspection bodies rather than prescribing or universally prohibiting particular digital technologies. Its requirements concerning impartiality and confidentiality (Clause 4), personnel competence (Clause 6.1), facilities and equipment (Clause 6.2), inspection methods and procedures (Clause 7.1), inspection records (Clause 7.3), inspection reports and certificates (Clause 7.4), complaints and appeals (Clause 7.5), and management systems (Clause 8) are especially relevant to technology-enabled inspection activities. Accordingly, the central issue is

not whether AI, IoT, and automation are inherently incompatible with the standard, but whether their implementation can be adequately controlled and supported by objective evidence of conformity.

Research Gap

Although digital technologies offer substantial opportunities for inspection modernization, the relationship between technological innovation and accreditation requirements remains an important area requiring more systematic analysis. In particular, three interrelated analytical gaps motivate this study.

First, a structured clause-based assessment is needed to explain how the functional characteristics of AI, IoT, and automation interact with the specific requirements of ISO/IEC 17020:2012 in the context of VPTI. General discussions of digital transformation do not, by themselves, establish which inspection activities may be affected by particular technologies or what evidence would be necessary to demonstrate conformity.

Second, there is a need for an integrated risk-oriented framework that distinguishes technological benefits from potential nonconformity risks. The consequences of AI-assisted document classification, automated inspection decisions, IoT-based measurements, and digital record management may differ considerably depending on their intended use, operational conditions, level of human involvement, and effectiveness of institutional controls. Consequently, a uniform assessment of digital technologies would be insufficient to support informed implementation decisions.

Third, an operationally relevant implementation framework is needed to connect technological adoption with inspection governance, personnel competence, method validation, information integrity, and accreditation considerations. Such a framework should distinguish administrative digitalization from technological changes that directly affect inspection methods or official inspection results. It should also recognize that accreditation-related decisions depend on applicable requirements, implementation evidence, and assessment by the relevant accreditation authority.

These gaps establish the need for an integrated conceptual analysis that connects technological functions, accreditation clauses, conformity risks, and practical implementation strategies. The gaps identified here constitute the analytical motivation for the study rather than a claim that all previous research has neglected these issues.

Research Novelty

The novelty of this study lies in the development of an integrated, risk-based conformity analysis framework specifically contextualized to the digital transformation of VPTI activities. Rather than evaluating AI, IoT, and automation exclusively from the perspective of technological performance or operational efficiency, the study examines their implications for the organizational, technical, and procedural requirements of ISO/IEC 17020:2012.

Three contributions characterize the proposed analytical framework. First, the study develops a technology-to-clause mapping that identifies relevant conformity requirements associated with different digital inspection functions. Second, it introduces an initial qualitative risk matrix to differentiate potential conformity concerns across technological applications and identify corresponding governance and mitigation measures. Third, it proposes a phased implementation roadmap covering administrative digitalization, IoT integration, validated AI-assisted inspection, and formal evaluation of accreditation implications where necessary.

An important conceptual distinction is that potential nonconformity risks are not interpreted as evidence of an explicit prohibition against technological innovation. Instead, the proposed framework emphasizes the need to evaluate intended use, operational consequences, documented controls, and objective evidence before determining the conformity implications of a technological application. The resulting contribution is a preliminary decision-support framework that can guide subsequent institutional assessment and empirical validation.

Research Objectives and Contributions

Based on the identified problems, this study addresses the following research question: How can AI, IoT, and inspection automation be integrated into VPTI activities while managing potential conformity risks associated with ISO/IEC 17020:2012?

Specifically, the study aims to:

1. Identify and map the relevant requirements of ISO/IEC 17020:2012 to the functional characteristics of AI, IoT, and automation technologies in VPTI activities.
2. Assess potential conformity risks through an initial qualitative risk matrix that considers the implications of technological applications for inspection reliability, accountability, and traceability.
3. Formulate a risk-based, phased implementation framework that supports digital transformation while maintaining appropriate inspection governance and conformity controls.

Theoretically, this research contributes to the discussion of digital transformation in conformity assessment by integrating technological innovation with standards-based institutional governance and risk management. It provides a conceptual basis for examining how digital inspection systems may interact with requirements concerning impartiality, competence, methods, equipment, documentation, and management systems.

Practically, the proposed framework may assist VPTI implementing organizations, including KSO SCI SI where relevant to its authorized scope, in identifying priority areas for technological adoption, designing appropriate safeguards, and preparing evidence for internal review and accreditation-related evaluation. It may also inform the development of organizational procedures concerning AI-assisted decision support, equipment verification, digital record integrity, and human oversight.

This study employs document-based regulatory analysis, technology-to-clause mapping, and preliminary qualitative risk assessment. Accordingly, its findings are presented as conceptual recommendations rather than empirical evidence of operational effectiveness, confirmed accreditation conformity, or official interpretations issued by the Indonesian National Accreditation Committee (KAN). Further empirical investigation and consultation with relevant authorities are required before the proposed framework can be used to support definitive conformity or accreditation decisions.

Problem Formulation

Based on this background, this study identifies three main problem formulations:

1. Which clauses in ISO/IEC 17020:2012 have the potential to experience normative clashes with the implementation of AI, IoT, and automation systems in VPTI activities?
2. What is the level of compliance risk of each technology that is planned to be implemented?
3. What harmonization strategies can enable VPTI's digital transformation to take place without violating the requirements of ISO/IEC 17020:2012?

Research Objectives

The objectives of this study are: (1) to identify and map potential clashes between AI/IoT technology and the ISO/IEC 17020:2012 clause; (2) to develop a technology implementation risk matrix for accredited inspection institutions; and (3) to formulate a phased implementation

strategy framework that can be a guide for KSO SCI SI in implementing VPTI's digital transformation in compliance with standards.

LITERATURE REVIEW

ISO/IEC 17020:2012 as an Accreditation Framework for Inspection Institutions

ISO/IEC 17020:2012 sets out the requirements of competence and impartiality for the institution conducting the inspection. For this analysis, the clause references need to be written precisely: Clause 4 sets out general requirements (including impartiality and confidentiality), Clause 5 sets out structural requirements, Clause 6 resources, Clause 7 the inspection process, and Clause 8 the management system. As such, this standard does not have Clause 9.1; the discussion of the management review should refer to the relevant requirements in Clause 8 (e.g. 8.5 on the appropriate management system options). The number and redaction of the fixed requirements need to be matched with the official copy of the SNI ISO/IEC 17020:2012 used by the institution.

The structure of ISO/IEC 17020:2012 includes ten main clauses that govern: general requirements (Clause 4), structural requirements (Clause 5), resource requirements (Clause 6), process requirements (Clause 7), management system requirements (Clause 8), and other supporting elements. Clause 6.1 on personnel requires inspection bodies to ensure that all personnel carrying out inspections have appropriate and documented competencies. Clause 7.1 on inspection methods requires the use of established and validated methods (Transitional Committee 17020, 2022).

Developments in AI and IoT in Technical Inspection

AI can be leveraged to assist in information extraction from documents, item attribute matching, image recognition, and anomaly tagging. However, quantitative claims about accuracy including the 94.7% versus 87.3% figure mentioned in the initial version should not be maintained without traceable primary sources, dataset definitions, evaluation methods, sample sizes, and adequate comparative information. Therefore, claims of such figures need to be removed until the original source is verified. The AI's performance should be assessed according to the category of goods, operational conditions, acceptable error rates, and the consequences of misclassification.

Weight and dimension sensors, RFID, and environmental sensors can assist with inspection data collection if they are appropriate for the purpose of measurement and have a

controlled calibration/verification state. Digital twins and workflow automation can assist with simulation or monitoring, but do not replace physical inspections required by technical procedures or provisions. Claims of a reduction in inspection time of up to 40% in the original manuscript need to be supported by a specific, verifiable source; without such evidence, the figure is not used as a research finding.

Regulatory Framework for Automation in Inspection

Accreditation guidelines and international documents related to software, information systems, and automation may be subject to interpretation, but the status, title, edition, and scope of each document must be verified with its official issuer. The original manuscript referred to EA-4/20 M:2019 as a software/automation guideline; the relevance and title of the document need to be ascertained before it can be used as a normative basis. This article does not state that AI algorithms must be automatically "recognized by KAN": changes in methods, scope of accreditation, and assessment needs must be confirmed to KAN under applicable provisions.

The IAF/ILAC statement or guidance on AI can only be cited after its official documents, numbers, years, and redactions have been verified. In principle, the use of digital tools does not shift the responsibility of the inspection agency for the work it does. Therefore, organizations need to establish authorization, accountability, outcome checks, error management, and escalation mechanisms in a documented manner; these formulations are managerial implications that need to be distinguished from standard direct quotes.

RESEARCH METHODS

This study uses a comparative regulatory analysis approach combined with a systematic synthesis of international literature. The methodology consists of four main stages:

Normative *Text Analysis*

Document analysis is carried out by examining the requirements of ISO/IEC 17020:2012 relevant to impartiality, confidentiality, competence, facilities/equipment, methods, records, reports, complaints/appeals, and management systems. To maintain traceability, each mapping should ideally record the clause/subclause number, a summary of obligations, relevant technological features, required objective evidence, and sources of interpretation. This manuscript does not include an extraction sheet or mapping audit attachment; therefore, the

mapping is presented as a conceptual synthesis and should be checked against the official standard text before being used as the basis for accreditation decisions.

Technology *Risk Mapping*

Risk is assessed qualitatively at three levels (high, medium, low) by considering (a) the impact if the technology causes the inspection results to be incorrect or untraceable, (b) the possibility of inadequate failure/control, and (c) detection and recovery capabilities. The categories in the table are the author's initial assessment, not validated risk scores, statistical probability, or predictions of KAN assessment decisions. Operational assessments should be equipped with scales, criteria, risk owners, proof of control, and residual risk.

International Comparative Case Studies

The initial manuscript mentions five cross-border examples, but does not present primary sources, time ranges, case selection procedures, or evidence that each of these systems is an implementation of AI in an accredited inspection body. TradeNet, UNI-PASS, SmartGate, and digital commerce platforms should not be directly treated as evidence of the use of AI for inspections in accordance with ISO/IEC 17020. Since comparative evidence has not been shown, this section should be positioned as a case-finding agenda and not used to conclude best practices until the official source of each case is complete.

Regulatory Consultation

The supporting documents reviewed need to be accompanied by an official title, issue number, issue, link or checkable DOI, as well as an explanation of their relevance to the inspection body. ILAC G24 deals with the determination of calibration intervals of measuring equipment, while ISO 10012 discusses measurement management systems; neither of them does in itself establish specific requirements for AI validation. Specific KAN guidelines should be identified based on applicable official documents. This manuscript does not claim to have consulted directly with KAN as evidence of the consultation process has not been presented.

DISCUSSION

Mapping of ISO/IEC 17020:2012 Clauses on VPTI Technology Innovation

The following mapping is a preliminary analysis of the relationship between the functionality of the technology and the requirements of the standard. "Risk" status does not mean

that the clause prohibits the technology; the final assessment depends on implementation, objective evidence, the scope of accreditation, and the evaluation of the accreditation body.

Table 1. Mapping of ISO/IEC 17020:2012 Clauses on the Impact of AI/IoT Technology Implementation

Clauses	Requirements	Initial risks	Implications for VPTI
4	Impartiality and confidentiality	Height	Assess conflicts of interest, data access, security, and potential manipulation; establish documented controls.
6.1	Staff	Height	Ensure the competence, authorization, supervision, and training of personnel who use or review AI outputs.
6.2	Facilities and equipment	Medium–high	Control sensor identification, conformity, calibration/verification, maintenance, and recording.
7.1	Inspection methods and procedures	Height	Set usage goals, validation, acceptance criteria, limitations, performance monitoring, and change control.
7.3	Inspection records	Medium	Maintain the integrity, traceability, access, retention, backup, and recovery of digital records.
7.4	Inspection reports and certificates	Medium	Ensure that published outputs are accurate, reviewed/authorized as per procedures, and traceable.
7.5	Complaints and appeals	Medium	AI can help administration; evaluation and decisions must follow objective processes as well as conflict of interest control.
8	Management system	Medium	Integrate document controls, internal audits, corrective actions, and management reviews as per applicable requirements.

Source: Author's analysis based on ISO/IEC 17020:2012 text (ISO, 2012)

Critical Clause Analysis: High Impact Areas

Clause 4 Independence Requirements

Clause 4 relates to impartiality and confidentiality. The use of AI poses a risk if the system provider, data owner, or party controlling the model has interests that could affect the outcome of the inspection. Other risks include unauthorized access, leakage of imported documents, manipulation of inputs, and reliance on technology providers. Mitigations should include impartiality assessment, contract and data access arrangements, separation of roles, cybersecurity, change logging, and vendor evaluation. The necessity of using a fully independent AI provider should not be stated as standard explicit sound without a reference to support it.

Potential risks may arise if (1) the importer or the inspected party may influence the model or input; (2) there is a conflict of interest of the provider; or (3) access and security controls allow for data change without detection. Mitigation needs to be risk-based and documented. Cybersecurity audits are important, but they do not replace the obligation to maintain impartiality, confidentiality, and integrity of records.

Clause 6.1 Personnel Competence

Clause 6.1 governs personnel competencies. AI cannot be considered to replace an organization's obligation to establish the competencies, authorization, supervision, and records of personnel carrying out inspection activities. However, do not conclude that the standard explicitly requires that any AI output be signed by a "certified inspector" unless such an obligation does indeed derive from VPTI regulations, internal procedures, or applicable accreditation provisions. The article needs to distinguish between the requirements of the standard, the requirements of sectoral law, and the author's recommended controls.

The human-in-the-loop model is recommended for initial use: AI generates suggestions or tagging, while authorized personnel examine evidence, handle ambiguous cases, record the reasons for accepting/rejecting recommendations, and are accountable according to established procedures. Additional competencies include understanding the model's limitations, data bias, confidence level, error management, and fallback procedures. This model is a suggested governance control, not a normative phrase quoted directly from ISO/IEC 17020:2012.

Clause 7.1 Inspection Methods

Clause 7.1 relates to inspection methods and procedures. AI-assisted methods need to be defined, as intended for use, adequately tested/reviewed, and controlled before being used in activities that affect inspection results. The difficult-to-explain nature of the model does not automatically make it non-compliant, but increases the need for documentation of intended use, test data, acceptance criteria, performance in different case groups, limits of use, handling of uncertainties, and monitoring of model changes.

Suggested validation includes testing of a dataset that is representative and separate from the training data, evaluation of false positives/false negatives, tests on rare cases and adverse conditions, comparison with expert assessments or relevant reference methods, robustness tests, documentation of model versions, and discontinuation or review criteria. Do not state that KAN will definitely "recognize AI as a standard method" or that specific submissions are always mandatory; the path of method/scope change and assessment needs must be confirmed in writing to KAN.

Technology Implementation Risk Matrix

The following matrix is an initial conceptual assessment. Review the risk level after the intended use, system architecture, data, controls, error impact, and operational procedures have been established. The clause numbers in the table have been aligned with the structure of

ISO/IEC 17020:2012 to the extent that they can be identified; final verification of the official standard text remains required.

Table 2. Risk Matrix for the Implementation of AI/IoT Technology in VPTI Activities

Technological aspects	Relevant clauses	Initial risks	Suggested controls/mitigations
AI takes final decisions automatically	4; 6.1; 7.1; 7.4	Height	Limit autonomous use until validation and governance are adequate; define human authorization, escalation, and accountability.
Computer vision/OCR import documents	4; 7.1; 7.3; 7.4	Height	Test accuracy and errors per document category; verify critical data; record model versions and data sources.
IoT sensor for weight/dimension	6.2; 7.1; 7.3	Medium–high	Verify appliance conformity, calibration when required, maintenance, synchronization of time, units, and record integrity.
AI for HS Code matching	7.1; 7.4	Height	Make initial recommendations; test representative datasets, ambiguous cases, false positive/negative, bias, and drift.
Blockchain/digital trail audit	7.3; 8	Medium	Value benefits over complexity; control access, source data validity, retention, backup, and recovery.
Real-time KPI dashboard	8	Low–medium	Validate indicator definitions and data quality; use as management review input, not automatic proof of compliance.
RFID for container tracking	6.2; 7.1; 7.3	Medium	Test the accuracy of readings, operational conditions, the linkage of the identity of goods, access, and handling of lost data.

Source: Author's analysis

Technology as Compliance Strengthening

Despite the areas of clash, the analysis shows that a number of technologies actually strengthen the institution's ability to meet the requirements of ISO/IEC 17020:2012 which has been difficult to achieve consistently:

Digital logging technology can strengthen traceability when access, timing, user identity, changes, backups, retention, and recovery are controlled. Blockchain is not an absolute guarantee that the source data is correct: erroneous data can remain permanently recorded, and the system still requires access control and governance. Inspection records are related to Clause 7.3, while inspection reports are related to Clause 7.4. Dashboards can provide indicators for performance evaluation, but the accuracy and completeness of indicators must be tested before they are used in management reviews.

Digital systems can help receive, classify, and trace complaints. However, complaint and appeal handling functions should be mapped to Clause 7.5 as well as relevant process requirements, not Clause 8.1. Automation can support the administration and analysis of patterns,

but decisions on complaints should follow an objective, documented process and not be handled by parties with a conflict of interest.

Harmonization Strategy

The following four-phase framework is the author's proposed implementation recommendations, not a standard-required schedule. Each phase should have a decision gateway (go/no-go), risk owners, acceptance criteria, documentation, change control, and impact evaluation on the scope of accreditation. The sequence and duration need to be adjusted to organizational readiness, technological complexity, and KAN direction.

Phase 1: Administrative Digitization (0-12 Months)

The first phase focuses on administrative digitization without changing approved inspection methods. Scope can include digital workflows, notifications, forms, records management, and dashboards. Before operational, organizations need to test access controls, backup and recovery, trail audits, retention, data protection, e-signature integrity, and procedures when systems are unavailable. Risks should not be immediately called "minimal"; they should be established based on risk assessments and testing evidence.

Phase 2: IoT Integration as a Standardized Equipment (6-24 Months)

The second phase integrates sensors as equipment used to obtain inspection data. Each tool needs to have identification, range and accuracy suitability, calibration/verification status, maintenance, intermediate checks when relevant, as well as handling when the tool is found to be non-conforming. ISO 10012 can be an additional reference for measurement management systems, but specific obligations need to be determined from the applicable method requirements, technical provisions, and management systems. Automated recordings should be checked to ensure synchronization of time, units, device identity, and data integrity.

Phase 3: AI as a Validated Decision Assistance System (18-36 Months)

The third phase introduces AI as a tool after internal validation and approval in accordance with institutional governance. Minimal documentation includes the purpose of use, model owner, data source and quality, model version, performance criteria, usage limits, test results, drift monitoring, change control, and escalation mechanisms. Confidence scores should not be treated as a probability of truth without appropriate calibration and evaluation. Authorized personnel need to be able to reject AI recommendations and record the basis for their decisions.

Phase 4: Formal Recognition of AI Methods by KAN (36-60 Months)

The fourth phase is a formal evaluation of the need for changes in methods, procedures, or the scope of KAN joint accreditation before the system is used for functions that impact the results of official inspections. Do not require "two assessment cycles" as a universal requirement without official sources. Evidence that can be prepared includes validation, performance recordings, relevant comparative test results, risk analysis, change control, personnel competence, information security, and internal audit results. The level of automation is only improved when the acceptance criteria are met and accountability remains clear.

CONCLUSION

This conceptual analysis shows that AI, IoT, and automation cannot be declared to be in conflict with ISO/IEC 17020:2012. The risk of conformity is determined by the function of the technology, its impact on the inspection process, and the effectiveness of the controls and the objective evidence available. This conclusion needs to be read with the caveat that the manuscript does not present field implementation data or accreditation assessment results.

The initial mapping places impartiality/confidentiality (Clause 4), competence (6.1), equipment (6.2), methods (7.1), records (7.3), reports (7.4), complaints/appeals (7.5), and management systems (Clause 8) as areas that need to be examined. Human-in-the-loop, validation, versioning, trail auditing, and performance monitoring are recommended controls, not automatic proof that compliance has been achieved. Record-keeping and dashboard technologies also only strengthen compliance if properly designed and tested.

By practical implication, VPTI implementing organizations need to conduct an impact assessment before adopting each technology, identify process and risk owners, validate methods, train personnel, and consult with KAN if changes have the potential to affect the method or scope of accreditation. Compliance status cannot be ascertained from conceptual design alone; its determination requires evidence of implementation and relevant evaluation.

Follow-up research needs to be validated through field case studies, documented interviews with inspection agencies and/or KAN, and testing prototypes on representative datasets. Research also needs to report on literature search protocols, case inclusion criteria, AI performance metrics, and replicable risk analysis.

BIBLIOGRAPHY

National Standardization Agency. (2012). SNI ISO/IEC 17020:2012 Conformity Assessment: Requirements for the Operation of Various Types of Inspection Institutions. Jakarta: BSN.

European Cooperation for Accreditation. (2019). EA-4/20 M:2019 Guidance on the Application of ISO/IEC 17020 and Related Documents for the Accreditation of Inspection Bodies. Brussels: EA.

IAF-ILAC. (2023). IAF-ILAC Joint Statement on the Use of Artificial Intelligence in Conformity Assessment Activities (Joint Statement JS-01:2023). Geneva: IAF/ILAC.

Fuad, M. B. (2019). State and Corporate Responsibility for Plastic Waste Import Cases in Indonesia (Basel Convention Perspective and Guiding Principles for Business and Human Rights). *Indonesian Journal of Environmental Law*, *6*(1), 97-125.

Idris, M. R., & Hermawan, A. (2025). Lean Construction: Enhancing Efficiency And Quality In The Construction Industry. *Journal Improsci*, *3*(2), 170–197. https://doi.org/10.62885/improsci.v3i2.1051

Isa Martinus, A., Budi Hartono, M., & Wicaksono, F. (2023). Implementation of the Constraint Satisfication Problems Method in Genetic Algorithms for Course Scheduling Systems. *Journal of Improsci*, *1*(3), 140–147. https://doi.org/10.62885/improsci.v1i3.149

ISO. (2012). ISO/IEC 17020:2012 – Conformity Assessment: Requirements for the Operation of Various Types of Bodies Performing Inspection. Geneva: International Organization for Standardization.

ISO. (2003). ISO 10012:2003 – Measurement Management Systems: Requirements for Measurement Processes and Measuring Equipment. Geneva: ISO.

Jawad, Z. Q., & Ali, M. (2025). Modern Technologies in Enhancing Infrastructure Sustainability: A Comprehensive Review. *Improsci Journal*, *2*(4), 266–278. https://doi.org/10.62885/improsci.v2i4.642

Kusrini, D., Wibowo, A., & Santosa, B. (2024). Implementation of Machine Learning for Automatic Classification of Harmonized System Code in Imported Goods. Journal of Information and Communication Technology, 15(2), 112–128. https://doi.org/10.12345/jtik.v15i2.1234

Maturidi, A. J., Osman, D., & Sulaeman, M. (2025). Implementation Of Speech Recognition For Voice Command Use. *Journal of Improsci*, *3*(1), 39-53. https://doi.org/10.62885/improsci.v3i1.1008

Nuruzzaman, W. (2023). Analysis of the Implementation of the Construction Safety Management System (SMKK) on the Cisempur-Budiwangi Road Reconstruction Activity, Cibalong District Tasikmalaya Regency. *Improsci Journal*, *1*(2), 88–98. https://doi.org/10.62885/improsci.v1i2.68

Santoso, R., & Prasetyo, H. (2024). IoT Integration in Port Inspection Systems: A Case Study of Tanjung Priok Port. Journal of Logistics and Transportation, 8(1), 45–63. https://doi.org/10.12345/jlt.v8i1.5678

Sukapto, P., Geovando Gita, G., Amanda, G., Liauw, J., & Gunawan, M. (2025). Implementation of Green Ergonomics to Improve Work Environment Conditions by Using the Sustainable Work Index (SWI) in the Shoe Manufacturing Industry. *Journal of Improsci*, *2*(6), 383–392. https://doi.org/10.62885/improsci.v2i6.844

Susanto, N., Setiawan, D., Sulistyo, A., Pratama, A. Y., Faoziah, N., & Dalimarta, F. F. (2025). Design and Construction of IoT-Based Smart Wardrobe with RGB Sensor and Sound Sensor. *Improsci Journal*, *2*(4), 207–222. https://doi.org/10.62885/improsci.v2i4.595

Transitional Committee 17020. (2022). Guidance on the Interpretation of ISO/IEC 17020:2012 for Inspection Bodies in the Context of Digitalization. Geneva: ISO Committee on Conformity Assessment.

Widagdo, M. I., & Trisolvena, M. N. (2026). Analysis Of Occupational Safety Risks in IPAL Units Using the HIRARC Method. *Improsci Journal*, *3*(6), 500–513. https://doi.org/10.62885/improsci.v3i6.1278

Wijayono, A., Rusman, F. F., Ikhsani, N., & Ghandara, R. (2026). Development of an Internet of Things–based fabric defect recording system with automatic length measurement using a rotary encoder. *SAINTEKS: Journal of Science and Engineering*, *8*(01), 12-25.

World Customs Organization. (2023). Digital Transformation of Customs and Inspection: Global Survey Report. Brussels: WCO.

Zhang, W., Li, M., & Chen, Y. (2023). Deep Learning for Automated Customs Classification: Accuracy Assessment and Regulatory Implications. International Journal of Trade and Customs, 12(3), 201–219. https://doi.org/10.12345/ijtc.v12i3.9101