TIC COUNCIL
Independent Voice of Trust

Quality Infrastructure Framework for the Digitalised World

February 2026

TABLE OF CONTENTS

INTRODUCTION

The Testing, Inspection, and Certification (TIC) industry recognises the accelerating pace of digital innovation and the changing needs of industry and society. TIC Council members are modernising how trust is delivered through agile, digitally supported approaches that reflect current industrial practices, thereby shaping the future of efficient, scalable, and trustworthy conformity assessments.

The paper calls for the freedom to adopt emerging technologies in conformity assessments while reaffirming our non-negotiable principles of independence, impartiality, technical competence, and confidentiality. Importantly, human-in-the-loop (HITL) is a core TIC principle as the sector continues to evolve, ensuring that the skilled and qualified workforce plays a central role in the responsible adoption and use of new technologies. TIC Council defines HITL as a system configuration in which human approval, input or supervision is required at defined decision points for the system to proceed or for outputs to be acted upon.

Within this overarching concept, the paper distinguishes between two complementary dimensions of HITL: human oversight and human accountability[1]. Human oversight refers to the active monitoring, validation, and, where necessary, intervention by qualified professionals in the operation of digital or automated systems. Human accountability relates to the clear allocation of responsibility to identified natural or legal persons for decisions, outcomes, and compliance with applicable legal, technical, and ethical requirements.

The extent of permissible HITL and the degree of automation in conformity assessments should be proportionate to the risk of the activity and the demonstrated performance of the supporting systems: low-risk, repeatable tasks may be more highly automated under documented guardrails, whereas safety-critical or enforcement-relevant determinations require stronger human oversight mechanisms and clear accountability. This balance is essential: innovation must be responsibly deployed by competent professionals to preserve the trust at the heart of third-party assurance.

The paper also sets out the TIC industry's vision for how Quality Infrastructure (QI)[2] should evolve by updating existing internal processes and strategically adopting new technologies to meet the demands of a rapidly digitalising world. For QI to remain relevant in today's tech landscape, all its actors and organisations must innovate, share best practices, and cooperate effectively.

The paper aims to guide policymakers, regulators, Accreditation Bodies (ABs), Standard Development Organisations (SDOs), metrology organisations, technology solution providers, TIC clients, consumers and other stakeholders on:

1. Forms of technology-enabled innovation that the TIC industry considers appropriate to implement in its services and procedures.
2. Where essential boundaries must be upheld to preserve trust.
3. How to shape a regulatory and accreditation environment that enables innovation without diluting the core values of third-party assurance.

In this context, it identifies new approaches to delivering trust, including continuous monitoring, remote validation, simulations, automation and digital evidence assessment. This openness to new assurance

[1] Further detail is set out in the Annex.

[2] TIC Council defines QI as the system comprising the organisations (public and private) together with the policies, relevant legal and regulatory framework, and practices contributing to supporting and enhancing the quality, safety and environmental soundness of goods, services and processes. The Quality Infrastructure is required for the effective operation of markets, and its international recognition is important for building trust and free trade. It is a critical element in promoting and sustaining economic development, as well as environmental and social well-being. It relies on: metrology, standardisation, conformity assessment, accreditation, and market surveillance.

models allows the sector to adapt as technology evolves, without compromising the integrity, independence, or reliability of TIC services. The paper does not prescribe detailed technical solutions or define a technology roadmap. Instead, it outlines the principles and boundaries under which innovation is considered appropriate and aligned with the public interest, ensuring relevance without undermining trust.

Section I: How Emerging Technologies Are Transforming TIC Services

The TIC sector has over 200 years of history. Originating during the Industrial Revolution, it supported the rise of innovation by helping industries demonstrate to consumers and society that new technologies and products were safe, reliable, and trustworthy. Over time, new technologies emerged, fresh risks appeared, and a digital reality took shape. As a result, the TIC sector's long-standing role in building trust in the physical world extended into the digital domain.

Our approach to conformity assessments is changing to reflect the opportunities and challenges of the digital age. We are embracing new technologies to become faster, more precise, and more globally responsive, enhancing our ability to deliver high-quality services. This transition relies on the ability of all QI actors to digitalise, innovate, and invest in advanced conformity assessments methods and cutting-edge testing technologies. Another relevant aspect is the role of metrology: the measurement methods, calibration services, reference materials and uncertainty quantification that make test results comparable, reproducible and defensible across laboratories and jurisdictions.

Yet, integrating cutting-edge tools into long-established QI processes and conformity assessments workflows introduces a set of challenges. Algorithms parsing test data, drones gathering samples, and digital twins modelling performance must achieve the near-perfect rigour traditionally delivered by human experts. In the same way we trust that an email will unfailingly reach its recipient, we must be certain that an AI interpreting safety-critical results is doing so correctly and transparently. Building this level of confidence demands robust validation, continuous performance monitoring, and lines of human accountability, ensuring that technology-enabled processes meet or surpass the rigorous standards that define the TIC industry.

To provide clearer guidance to stakeholders, the following examples illustrate how digital technologies can support conformity assessments without compromising core TIC principles:

- **AI in laboratory testing and non-destructive testing (NDT):** Used to classify sample results or detect anomalies, provided the algorithm is validated, the model is explainable, and human review is retained for final decisions. In NDT applications, AI can analyse radiographic, ultrasonic, or visual inspection data to detect defects, recognise patterns, and support anomaly detection. These tools enhance accuracy and efficiency but must operate under human oversight to ensure trust, reliability, and accountability in safety-critical assessments.
- **Remote inspection and sampling via robotics and drones:** Acceptable when operated by qualified personnel, whether using ground-based robotics or aerial systems, if data integrity, real-time traceability, and auditability are maintained throughout the process.
- **Continuous monitoring with IoT:** Supports compliance assurance when calibration, data integrity, and audit trails are ensured, and when triggers for human follow-up are clearly defined. An example is structural health monitoring in bridges or buildings, where IoT devices continuously collect vibration, strain, or temperature data. When combined with AI-based data analytics, these systems can detect early signs of degradation, helping prevent failures while ensuring timely, informed interventions by qualified professionals.
- **Digital platforms for document review and audit preparation:** These tools improve efficiency if they are transparent in how they support auditor judgment and are not used to fully automate certification conclusions.

- **Blockchain for traceability:** Improves trust in digital records when deployed in a way that ensures impartial data input and supports retrospective audits.
- **Simulated testing and digital twins:** Complements a fast-growing part of physical tests by accurately replicating system behaviours in virtual environments, provided their models are validated, and the results are subject to expert interpretation.

Section II: The Transformation – New Possibilities for Delivering Trust

The TIC industry is embracing the possibilities brought by emerging technologies to improve, enrich and extend the delivery of trust. While the purpose of TIC remains unchanged, how evidence is collected, assessed, and reported can now include advanced tools[3] such as:

Robotics and autonomous systems, including drones and unmanned aerial vehicles (UAVs), to carry out repetitive, hazardous, high-precision, or remote inspection and testing tasks.

Artificial Intelligence (AI) to support pre-screening of data, anomaly detection and structured document review. This includes Edge AI (processing data locally on devices for faster and more secure outputs), Generative AI (supporting unstructured documentation and report drafting), and agentic systems that can orchestrate routine workflow steps in conformity assessment (e.g., scheduling inspections, assigning qualified experts, triggering follow-up actions on detected non-conformities, and adapting test plans based on real-time findings).

Internet of Things (IoT) devices and smart sensors for remote and continuous data capture.

Virtual and augmented reality, along with digital twins and simulations, are increasingly used to enhance remote inspections, support auditor training, and, in some cases, complement or replace physical inspections and testing.

Distributed ledger technologies (DLT) for traceability and integrity of certification records.

Cloud and API-based platforms for automated evidence exchange.

Computer vision for automated image and video analysis, object recognition, and defect detection during inspections.

Advanced data analytics for pattern recognition, enabling the extraction of actionable insights, identification of emerging trends, and support for informed, risk-based decision-making.

Autonomous vehicles and systems used in controlled environments (e.g., factories or warehouses) to support testing and inspection in hard-to-reach or dynamic settings.

These technologies are transforming existing TIC operations and enabling new services, such as remote inspections, real-time monitoring, digital verification and large data analysis, that extend beyond traditional field presence and sampling. Many of these digital and remote tools were tested at scale under real-life conditions during the COVID-19 pandemic, providing valuable evidence of their robustness,

[3] This list reflects the tools currently used by the TIC sector and is expected to evolve as technologies advance.

limitations, and appropriate use cases, and generating practical lessons that continue to inform their responsible deployment today.

As these tools mature, it remains important to distinguish between (i) technologies that support evidence collection and analysis and (ii) the assurance functions that deliver confidence in conformity assessment outcomes.

In this context, human oversight concerns how qualified experts supervise the use of digital tools, ensuring they are used within agreed boundaries, that outputs are checked where appropriate, and that exceptions are escalated and handled. Human accountability concerns who remain responsible for the conformity assessment decision and the integrity of the service delivered, irrespective of whether technology supported parts of the process. Put simply, technology can meaningfully assist, and in some cases automate, defined tasks, but accountability for outcomes remains clearly assigned within the accredited TIC organisation.

Automation in TIC services, therefore, depends on the criticality of the activity and the potential impact of error. A risk-based approach supports wider use of automation for well-defined, validated tasks (e.g., data capture, consistency checks, triage, or pattern detection), while ensuring that appropriate oversight and escalation arrangements apply where decisions carry higher consequences. In practice, this means automation can execute tasks within validated parameters, with clear triggers for review when results fall outside expected ranges, present anomalies, or could materially affect an assessment outcome.

The TIC sector is committed to maintaining a highly skilled workforce with the competence to deploy these technologies effectively and to interpret and act on their outputs. As roles evolve, TIC experts increasingly focus on supervision, exception handling, technical judgement and continuous improvement of processes, ensuring that technology strengthens the independence, impartiality and competence that underpin TIC services.

Section III: Opportunities and Challenges

The TIC industry supports the responsible integration of digital tools and emerging technologies to improve the way trust is delivered. Under validated conditions, these tools bring clear benefits but also create challenges that must be managed, as outlined in the table below.

BENEFITS	CHALLENGES
Improve both delivery costs and delivery times, while also creating additional value for our customers by leveraging insights from the data we receive from them and their products.	Global fragmentation of measurement practices. Without harmonised metrology (traceable methods, aligned calibration procedures and agreed uncertainty treatment) for new technologies (e.g., sensor networks, IoT, digital twins), laboratories and regulators will adopt divergent measurement approaches. This could produce non-comparable test results, creating trade and market-access barriers, increasing compliance costs, and weakening the legal and regulatory enforceability of conformity evidence worldwide.
Expedite standards creation and updates, through the anonymous data collection during the digital/simulation certification by feeding those data points to the standards' committees.	Liability and accountability gaps in hybrid digital-human workflows, particularly where TIC providers depend on third-party technology suppliers, shared datasets, or client-operated monitoring systems, can create legal uncertainty. Clear allocation of responsibilities, contractual safeguards, and documented oversight and decision rights are therefore essential to maintain confidence and manage exposure.

Improved efficiency and reproducibility of conformity assessments (provided measurement and predictive methods, calibration and traceability are embedded).	Use of unvalidated or opaque AI systems without sufficient human control, which can undermine the reliability and accountability of conformity assessment results.
Increased quality and accuracy of results when validated technologies are applied responsibly (e.g., sensors reducing gaps between periodic inspections; automation reducing human error in repetitive tasks).	Single-decision or single-output AI models must include uncertainty estimation and clearly defined thresholds for acceptable risk; otherwise, they can lead to overconfidence in flawed results.
Broader service reach, including in hard-to-access or underserved areas.	Loss of traceability when evidence is collected via systems without adequate audit trails.
New trust models, such as real-time monitoring and remote auditing, match industry needs for agility, speed, and continuous improvement.	Dependency on the integrity and availability of high-quality data, as poor, incomplete, or biased data can compromise the accuracy and fairness of assessments.
Enhanced sustainability, by reducing the need for travel and physical interventions, minimising environmental impact, and supporting more resource-efficient processes through data-driven decision-making and continuous optimisation.	Cybersecurity risks, including potential attacks on connected systems that may lead to service disruption, manipulation of evidence, or data loss.
Clear value creation from TIC expertise. The industry's technical knowledge, standards-setting experience, and impartial assurance services can actively accelerate adoption of trustworthy digital solutions, unlock new business models, and deliver measurable social and environmental benefits (e.g., improved lifecycle management, reduced emissions, and validated sustainability claims).	Data leakage risks in AI systems, particularly involving sensitive or confidential information, may be inadvertently exposed or misused.
	Ethical concerns in AI use, such as bias, lack of explainability, or automated decisions that may not align with human values or regulatory requirements.
	The need for continuous monitoring of AI performance to ensure systems remain trustworthy, accurate, and compliant as they evolve over time.
	Environmental impact, including the energy consumption and carbon footprint associated with deploying and maintaining digital infrastructure, particularly in data-heavy applications like AI and cloud services.[4]

Ultimately, while digital technologies offer transformative potential, they must be embedded within a framework that preserves trust, accountability, and public interest. The TIC industry believes these risks must be addressed through accreditation criteria, updated regulations, and best practice guidance, grounded in clear principles.

To operationalise a risk-based approach to innovative conformity assessments, TIC Council members apply HITL proportionately to the criticality of the activity and the potential impact of error. TIC

[4] This risk is balanced by the positive impacts outlined in the opportunities section, where the integration of new technologies leads to improved sustainability.

organisations assess both (i) the risk associated with the conformity assessment decision (including potential safety impacts, monetary loss, and systemic trust effects) and (ii) the risk profile and maturity of the technologies used (including validation status, uncertainty handling, cybersecurity, and auditability). Where tasks are low-risk, repeatable, and well-validated, automation operates within documented guardrails with defined triggers for human review.

Where determinations are safety-critical or enforcement-relevant, stronger human oversight and explicit accountability controls apply, ensuring that qualified experts supervise, validate, and intervene as needed, while responsibility for outcomes remains clearly assigned within the accredited TIC organisation[5].

Section IV: Core Principles That Must Endure

The TIC industry is united in its view that our core principles[6] are non-negotiable and must be preserved, regardless of how technologies evolve, or services are modernised. For example, the responsible use of AI must preserve human accountability, risk-proportionate oversight, and professional competence in conformity assessment. TIC organisations remain accountable for all conformity decisions supported by AI or automation, consistent with Adherence .

These principles provide the foundation for trust, credibility, and public confidence in conformity assessment. They include:

Core principle	What this means in practice
Human-in-the-Loop (HITL)	HITL is a central principle underpinning the responsible use of digital and automated technologies in TIC activities. TIC Council defines HITL as a system configuration in which human approval, input, or supervision is required at defined decision points for a process to proceed or for its outputs to be acted upon. Within this overarching concept, two complementary dimensions apply: **Human oversight**, meaning that qualified experts set the scope and constraints of technology-supported steps, validate outputs, and intervene where anomalies, uncertainty, or boundary conditions arise. The degree of human involvement must be proportionate to the risk associated with each application: higher-risk or safety-critical activities require closer and more frequent human oversight, while lower-risk, well-validated, and repeatable processes may allow for a higher degree of automation. **Human accountability** is the assignment of responsibility for the conformity decision and the assurance service. It remains with the accredited TIC organisation and its designated decision-makers, irrespective of the degree of automation or whether third-party tools contributed to the analysis. This clarity increases confidence in innovation: the more a workflow relies on automation, the more it requires explicit governance, decision-right allocation, and documented controls to demonstrate that accountability and liability remain properly managed.
Demonstrated system performance	Demonstrated performance of decision-support systems: Digital tools, including AI models, used to support or automate elements of conformity assessments must be demonstrably fit-for-purpose and subject to ongoing performance assurance, proportionate to the risk and criticality of their application. Their use must enable

[5] TIC Council is developing technical guidance to determine the level of risk and the appropriate degree of Human-in-the-Loop (HITL), including when and how human oversight and human accountability are required.
[6] Value of the Testing, Inspection and Certification Sector, Europe Economics, December 2020.

	traceable, explainable, and auditable outcomes, and preserve the integrity, security, and reliability of conformity decisions.
Trustworthiness and ethics	Trustworthiness and ethics are what set the TIC sector apart, reflected in our capacity to discern ethical boundaries, assess acceptable risk, and make judgment calls beyond historical data patterns. Decisions must be guided, validated, and held accountable by skilled professionals who fully understand both the tools and their outcomes.
Independence & impartiality	Independence from clients, technology providers, and any commercial influence that could compromise impartiality. Impartiality in how results are interpreted and communicated, free from bias or external influence.
Technical competence	Technical competence based on verifiable qualifications, continuous training and practical experience.
Confidentiality	Confidentiality, with protection of sensitive client information, test data, and proprietary methods through strict access controls, data minimisation, anonymisation where appropriate, and clear contractual safeguards. Strong cybersecurity measures and tools are equally essential to safeguard confidentiality, privacy, and the integrity of TIC activities.
Traceability & transparency	Traceability, accountability and interpretability in all processes, whether physical or digital. Transparency, meaning that all digital processes, algorithms, and decision-making criteria must be explainable to both clients and regulators.
Robust data governance	Robust data governance and ethics, ensuring the secure, ethical handling of all data collected, processed, or stored, in full compliance with applicable data protection and privacy frameworks.

Digital tools and innovative methods may support delivery, but they must not erode these foundational values nor replace the value of human expertise. Transparency, explainability, and ethical data practices are not optional; they are critical enablers of trust in a digital age. Further, the competence of the workforce and the central role of human judgment are the ultimate safeguards to ensure technology serves, rather than undermines, the integrity of TIC services.

Section V: Regulatory Gaps and Enablers

To enable innovation while maintaining public trust, the TIC industry recommends addressing several structural gaps that currently hinder the adoption of modern, tech-enabled conformity assessment methods. The main overarching problem we see is the lack of accreditation schemes for hybrid digital-human models, which presents challenges to the sector's competitiveness and its ability to deliver faster, more efficient, and higher-quality services to clients. We have identified three main gaps as top priorities to address, in collaboration with QI partners and regulators:

1. **Recognition of digital evidence and legacy on-site requirements:** There is insufficient recognition and guidance for digitally collected or continuously validated evidence, despite its growing role in enabling real-time assurance. This, combined with an over-reliance on traditional definitions of on-site presence, static sampling, and human-only validation, restricts the adoption of more agile, tech-enabled assessment methods.

2. **Guidance on digital technologies:** Lack of clear guidance from policymakers and regulators on the acceptable use of digital technologies in conformity assessment created legal and operational risks. This uncertainty discourages innovation, and slows the adoption of technologies that could bring real value to industry and society.
3. **Regulatory capacity and coherence:** Slow regulatory adaptation, including gaps in technical knowledge among authorities. This creates a disconnect between regulatory expectations and technological capabilities. The TIC sector is ready to help close this gap by supporting capacity building and dialogue with regulators worldwide.

While the above gaps take priority, several other regulatory issues also require attention:

- **Metrology alignment risk:** Lack of internationally harmonised measurement standards for new digital and automated technologies could lead to inconsistent results, reduced traceability, and fragmentation across regions.
- **Complex legislative interplay and fragmentation:** Regulatory fragmentation across regions, which increases compliance burdens and creates barriers for globally operating TIC providers. Complex interplay between different legislative instruments, particularly in the EU, where overlapping or inconsistent rules can hinder digital innovation. A more coherent and streamlined approach, based on clear principles and cross-sectoral synergies, is needed.
- **Public demand enabler:** The TIC industry must drive greater public and client awareness of independent conformity assessment so that trust becomes a market-led expectation, not just a regulatory requirement. By bringing our role out from behind the curtain, we encourage end users to ask for accredited verification themselves, reducing reliance on slow regulatory mandates and accelerating the uptake of trustworthy products and services.

To close these gaps, regulators should explicitly define and harmonise:

1. Sufficient human oversight in hybrid digital-human models, outlining minimum engagement, decision points, and accountability frameworks for experts.
2. Human accountability in hybrid digital-human models, clarifying the non-delegable responsibility of TIC companies for conformity decisions, and setting expectations for governance, documentation of decision rights, and contractual arrangements with technology suppliers.
3. Proficiency testing and performance evaluation of digital decision-support systems, requiring independent evaluation (e.g., reference datasets, challenge tests, and inter-comparisons), and defining minimum performance criteria aligned with the risk and intended use of each system.
4. Legal equivalence of digital audit trails, ensuring that electronically recorded logs carry the same evidentiary weight as paper records.
5. AI validation requirements and intervals, specifying performance metrics, initial approval criteria, and mandatory re-validation cycles to guarantee ongoing reliability and fairness.

Lastly, the TIC sector calls for technology-neutral, principle-based regulatory frameworks that:

- Embed these clarifications into accreditation and regulatory criteria.
- Provide transparent, consistent rules that encourage responsible innovation.
- Empower TIC providers to leverage digital tools while safeguarding core assurance values of independence, impartiality, competence, and accountability.

Section VI: Recommendations and Position of the TIC Industry

The TIC industry calls on stakeholders to support the following position:

1. Recognise and facilitate digital conformity methods that uphold established QI principles while sustainably integrating deep technical expertise and practical experience.
2. Establish red lines, for instance:
    a. While full automation of conformity decisions is not acceptable in the current state of innovation and adoption within the TIC sector, we encourage ongoing dialogue and frameworks that leave room for the potential integration of fully automated processes in the future.

    b. The threshold between permissible semi-automation and inadmissible full automation in decision-making must be clearly defined, with input from TIC Council members.
3. Modernise accreditation models to reflect the reality of AI-supported testing, remote inspections, and continuous assurance, without which the absence of clear digital accreditation schemes risks undermining public trust.
4. Mandate transparency and auditability for all digital tools used in assurance processes.
5. Reinforce the role of accredited, independent TIC providers as the foundation of trust in digital and physical systems alike.
6. Apply principle-based guardrails for emerging technologies, ensuring that:
    a. Tools are validated and used strictly within their proven scope and re-validated at defined intervals.

    b. Human accountability and oversight will continue to be integrated at critical decision points, particularly where higher risks are involved.

    c. Algorithms used in decision-making must be explainable and auditable to clients and regulators.

    d. Data integrity, traceability, and evidence quality must be guaranteed and protected.

    e. Secure, ethical handling of all collected data complies with relevant privacy regimes.

    f. Strengthen metrology alignment by ensuring that measurement methods, calibration, and traceability for new digital and sensor-based technologies are harmonised internationally and regularly updated to prevent fragmentation and maintain consistent global standards.

This position reflects the shared commitment of the TIC industry to both technological progress and the enduring values of third-party trust. To further support actionable dialogue, the TIC industry proposes the following recommendations for key stakeholders:

For ABs	For Policymakers and Regulators	For SDOs
Update accreditation scopes and assessment criteria to include digital and hybrid assurance models.	Adapt regulatory language to explicitly accept digital evidence, remote audits, and continuous monitoring.	Ensure that new standards and revisions acknowledge the role of digital technologies and offer guidance on how to integrate them without undermining QI principles (i.e., Smart Standards).
Develop criteria for the validation, auditability, and oversight of AI-supported or sensor-driven conformity methods.	Define when digital trust mechanisms (e.g., digital twins, AI analytics) are equivalent to or supportive of traditional TIC methods, considering the need to avoid any safety and/or security risks.	Promote technology-neutral, principle-based language that integrates digital methods without diluting core QI values.
Ensure auditors receive dedicated training in digital tool validation.	Conduct public consultations when drafting digital conformity standards to harmonise expectations and address liability for automated errors, including clear expectations on how responsibilities are allocated between TIC companies, TIC clients, and technology suppliers, while keeping accountability for conformity decisions with the TIC organisation.	Implement modular standard architectures and accelerated revision cycles, enabling timely updates that align assessment schemes with rapidly evolving technologies.
	Clarify the legal equivalence of digital audit trails and paper records.	
	Collaborate with metrology bodies to ensure global consistency in measurement standards for emerging technologies and integrate these into regulatory frameworks.	

By adopting these recommendations, stakeholders will harmonise innovation with public trust, ensuring that digital transformation in TIC services advances safely, securely, ethically, and transparently.

Conclusion

As the TIC industry navigates a new era of digitalisation, our core message is clear: embrace the freedom to adopt AI, IoT devices, digital twins and other emerging technologies, but only within a framework that enshrines independence, impartiality, technical competence, ethics and expert human oversight and accountability. By doing so, we unlock unprecedented speed, precision and scalability in conformity assessment while safeguarding the trust that underpins every certificate and audit report.

Preserving these non-negotiable principles is not a nostalgic throwback; it is the very reason why third-party assurance remains indispensable in a world where algorithms can outpace human analytics. Our experts will shift from manual tasks to high-value oversight, ethical judgment and risk management, ensuring that technology serves society rather than replacing the critical human element that discerns acceptable risk and upholds integrity.

Now is the moment for regulators, ABs, standard-setters and industry leaders to join us in updating accreditation models, clarifying digital equivalence and embedding principle-based guardrails. Together, we can lead a responsible digital transformation, one that champions innovation, fortifies public confidence and secures the future of trustworthy QI.

Annex – Difference between human oversight and human accountability

As the TIC sector accelerates the adoption of digital tools, automation, and AI-enabled systems, a clear and shared understanding of HITL is essential for enabling innovation while maintaining regulatory confidence and accreditation recognition. For TIC Council, HITL is a governance framework that enables the responsible deployment of new technologies at scale, while ensuring legal certainty and trust in conformity assessment outcomes.

TIC Council defines Human-in-the-Loop (HITL) as a system configuration in which human approval, input, or supervision is required at defined decision points for a process to proceed or for its outputs to be acted upon. HITL ensures that technological innovation enhances, rather than replaces, professional judgment and responsibility in conformity assessments.

Within this framework, TIC Council distinguishes between two complementary but distinct concepts that are particularly relevant for regulators and ABs: human oversight and human accountability.

Human oversight

Human oversight refers to the set of human-led governance, operational and technical controls applied to technology-enabled TIC activities to ensure that the use of digital tools remains appropriate to the task, reliable in practice, and aligned with applicable standards and procedures. It seeks to ensure that TIC experts can monitor, understand, intervene in, or override an automated and/or AI system throughout its lifecycle and operation. Oversight focuses on how the technology is used and controlled, especially where outputs inform inspection, testing, audit planning, classification, prioritisation, or other decision-support functions.

Key characteristics:	**Typical mechanisms include:**	**In practice, human oversight covers:**

Applies before, during, and after system operation;
Focuses on risk mitigation, safety and reliability;
Does not require constant human involvement, but requires meaningful ability to intervene;
Can be procedural (e.g., policies, escalation paths) and/or technical (e.g., kill-switches, alerts).
	Monitoring dashboards;
	Threshold-based alerts;
	Manual override/shutdown;
	Review and escalation processes;
	Human review of edge and/or high-risk cases.
		Design and configuration choices (e.g., defining the system's intended use, decision thresholds, escalation routes, and acceptance criteria);
		Validation and ongoing performance monitoring (e.g., checking continued fitness-for-purpose, drift monitoring, anomaly detection);
		Review and intervention capability (e.g., the ability to pause, override, correct, or escalate outputs when warranted);
		Competence and independence safeguards (e.g., ensuring qualified staff supervise use, and conflicts of interest are managed).

Human accountability

Human accountability is the clear and explicit assignment of responsibility to a competent person and/or the accredited TIC organisation for the conformity assessment outcome and the integrity of the service delivered, regardless of the degree of automation and/or whether technology supported parts of the process. Accountability focuses on who remains responsible for the outcome, including where technology supported, informed, or streamlined parts of the service.

Key characteristics:	**Typical mechanisms include:**	**In practice, human accountability covers:**
Focuses on responsibility and liability, rather than technology interaction; Ensures no accountability gap arises as a result of automation; Is central to governance, auditability, and regulatory and legal compliance; Exists independently of the technology's level of autonomy or sophistication.	Clearly named accountable roles (e.g., product owner, model owner, conformity decision-maker); Clear RACI or responsibility matrices; Audit trails linking system behaviour to human decisions; Accountability for key lifecycle decisions, including: a. Model selection; b. Data choice and management; c. Risk acceptance; d. Deployment and use decisions; e. Post-incident response and corrective measures.	The final conformity assessment decision and attestation (e.g. certification decisions, assessment conclusions, or reported results, as applicable); Compliance with applicable standards, accreditation rules, and contractual or regulatory obligations; Duty of care and liability for the service and its impacts, including demonstrating that appropriate governance, controls, and oversight mechanisms are in place for any technology used.

Acknowledgement

TIC Council would like to acknowledge the valuable contributions of the Digital Committee, and the subject matter experts who supported the development of this publication. Their time, expertise, and collaborative input were essential throughout the process, and their engagement helped ensure the relevance and quality of the outcome.

Contributors

(Listed in alphabetical order by last name)

Sarah Askaou; Apave
Shahm Barhom; BSI
Daniel Bejnarowicz; UL Solutions
Thibault Bonneton; ALS Global
Emanuele Castagno; RINA
Danilo Diomede; RINA
Thomas Doms; TÜV Austria
Thami El Idrissi; Eurofins
Dr. Nick Flohrer; TÜV SÜD
Maxime François; AHK Group
Hinda Gharbi; Bureau Veritas
Xu Keija; CCIC
Piotr Majcherkiewicz; UDT
Michael Nicholls; Bureau Veritas
David Pickup; KIWA
Dietmar Schlößer; TÜV NORD
Martin Schaffer; SGS
Wayne Stewart; Intertek
Mark Thirlwell; BSI
Xavier Valero; DEKRA
Fernando Vallejo; Applus+
Sun Xinkai; CCIC

Contact Person
Ángel Moreno Rubio, Digital Policy Manager
Rue du Commerce 20/22, B-1000 Brussels
Tel: +32 487 02 07 32
Email: amorenorubio@tic-council.org

Editor's Note About TIC Council

TIC Council is the global trade association representing the independent third-party Testing, Inspection and Certification (TIC) industry which brings together about 100-member companies and organizations from around the world to speak with one voice. Its members provide services across a wide range of sectors: consumer products, medical devices, petroleum, mining and metals, food, and agriculture among others. Through provision of these services, TIC Council members assure that not only regulatory requirements are met, but also that reliability, economic value, and sustainability are enhanced. TIC Council's members are present in more than 160 countries and the wider TIC sector currently employs more than 1 million people across the globe.