حكومة دبي
GOVERNMENT OF DUBAI

مركز الإمارات العالمي للاعتماد
Emirates International Accreditation Centre

مركز الإمارات العالمي للاعتماد

Emirates International Accreditation Center

سياسة المركز بشأن الاستخدام الأخلاقي والمسؤول للذكاء الاصطناعي في أنشطة جهات تقييم المطابقة

EIAC Policy on the Responsible Use of Artificial Intelligence (AI) in Conformity Assessment Activities

EIAC-PL-007

Signatories	
Approved:	CEO, Emirates International Accreditation Centre

Revision history			
Issue no.	**Rev. No.**	**Details**	**Date**
1	0	First Issue for use	30-04-2026

Contents

1 Purpose

This Policy establishes the mandatory EIAC policy governing the use of Artificial Intelligence (AI) within accredited conformity assessment activities.

Artificial Intelligence is recognized as a form of Information and Communication Technology (ICT) that may be used to support conformity assessment processes. This policy aims to ensure that:

1. The efficiency and effectiveness of conformity assessment activities may be enhanced without compromising the validity, integrity, or objectivity of results.
2. Human accountability remains the final authority for all conformity assessment decisions.
3. Compliance is maintained with EIAC requirements and the relevant recognition organizations (e.g., Global ACI) and a risk-based approach is applied to identify, evaluate, and control risks associated with the use of AI.

2 Scope of Application

This policy is mandatory for all bodies accredited by, or seeking accreditation from, EIAC, hereafter in this policy called (CABs) including:

1. Testing and Calibration Laboratories (ISO/IEC 17025)
2. Medical Testing (ISO 15189)
3. Inspection Bodies (ISO/IEC 17020)
4. Management Systems Certification Bodies (ISO/IEC 17021-1)
5. Product, Process, and Service Certification Bodies (ISO/IEC 17065)
6. Person Certification Bodies (ISO/IEC 17024)
7. Validation and Verification Bodies (ISO/IEC 17029)
8. Halal Certification Bodies (GSO UAE.S 2055-2 & OIC/SMIIC-2)
9. Halal Person Certification Bodies (OIC/SMIIC-34)
10. Proficiency Testing Providers (PTP) (ISO/IEC 17043)
11. Reference Material Producers (ISO 17034)
12. Biobanking facilities (ISO 20387)
13. All other applicable conformity assessment activities scopes and EIAC accreditation schemes

This policy applies to the use of artificial intelligence in both on-site and remote conformity assessment activities. Any use of artificial intelligence forms part of the conformity assessment methodology and shall comply with all applicable requirements. Where other schemes, regulatory frameworks, or legal requirements impose additional or more stringent obligations, such requirements shall take priority and be implemented with this policy.

3 Definitions

3.1 Artificial Intelligence (AI):

A machine-based system that, for a given set of objectives, makes predictions, recommendations, or decisions influencing real or virtual environments using data and algorithmic models. In the context of this policy, AI includes — but is not limited to — machine learning, natural language processing, computer vision, and automated decision-support systems used to support conformity assessment activities.

3.2 Algorithmic Impact Assessment (AIA):

A structured risk assessment used to identify and evaluate potential risks arising from the use of AI, including impacts on quality, objectivity, impartiality, and reliability of conformity assessment results. CABs shall conduct an AIA prior to deploying any new AI system in conformity assessment activities and shall review it periodically or following any significant change to the AI system. See Section (6) for governance requirements.

3.3 Virtual Site:

A virtual environment where an organization performs work or delivers services through online or digital platforms. Virtual sites may be subject to remote conformity assessment activities supported by AI tools, subject to the conditions and controls established in this policy and applicable accreditation requirements.

3.4 Competent Personnel:

Individuals who possess education, training, technical knowledge, skills, and demonstrated experience are required to perform and critically evaluate the results of conformity assessment activities, including AI-supported activities, in accordance with applicable standards and accreditation requirements.

3.5 Black-Box AI:

An AI system whose internal logic, decision pathways, weighting mechanisms, or outputs cannot be readily explained, interpreted, reproduced, or independently reviewed by the user or a qualified third party. The use of black-box AI in conformity assessment activities is prohibited under this policy (see Section 5).

4 Fundamental Policy Principles

EIAC mandates the following principles:

4.1 Human-in-the-Loop

AI shall function solely as a supporting tool. All final conformity assessment judgments, conclusions, and decisions shall remain the responsibility of competent human personnel.

4.2 Mutual Agreement

The use of AI within conformity assessment activities shall be mutually agreed between the CAB and the organization being assessed where applicable.

4.3 Integrity and Objectivity

CABs shall ensure that the use of AI does not compromise the validity, objectivity, impartiality, or reliability of conformity assessment activities or outcomes.

4.4 Transparency

Where artificial intelligence is used in conformity assessment activities or management system processes, CAB reports shall clearly indicate the scope and purpose of such use and its role in supporting conformity assessment activities, excluding the use of artificial intelligence solely for linguistic editing, text adjustment, or rephrasing purposes.

5 Illustrative Examples of Permitted and Prohibited Uses

The following table provides illustrative, non-exhaustive examples of permitted and restricted uses of artificial intelligence by CABs.
Final responsibility for CABs decisions shall always remain with competent human personnel.

Activity Category	Permitted Use Cases (Supportive)	Restricted Use Cases
Data Analysis (A) CABs Operational Data	Analysis of the CAB's own operational data, performance indicators, and trend identification to support its own management and technical systems.	Use of AI-generated outputs or conclusions without adequate human oversight and validation.
Data Analysis (B) Client Assessment Data	Analysis of clients' data generated during conformity assessment activities, to support assessment findings and outcomes.	Automated conformity assessment decisions, including granting, suspending, reducing, or withdrawing certification, reports, or scope without human decision-making authority.

Activity Category	Permitted Use Cases (Supportive)	Restricted Use Cases
Planning	Supportive Risk-based planning of conformity assessment activities, including inspections, audits, testing, calibration, examinations, and sampling activities, subject to human review and approval.	AI-generated planning or scheduling decisions implemented without competent human technical review and authorization.
Evidence Gathering	Supporting access to documents, records, or remote environments (including hazardous or inaccessible locations) as an aid to assessment activities supported by competent human decision on evidence validity.	Substitution of required on-site conformity assessment activities where physical presence, observation, witnessing, inspection, examination or testing is mandated by applicable standards or schemes. The use of AI to access, process, or transmit information within classified, defense-related, government-restricted, or otherwise legally protected environments is prohibited unless explicitly authorized in writing by the relevant competent authority and agreed between the CAB and the client prior to the commencement of the assessment activity.
Risk Assessment	Use of AI tools to support the identification of potential conformity, quality, or compliance risks within CAB operations or client activities.	Use of non-transparent (black-box) AI systems whose logic, outputs, or results cannot be explained, validated, reproduced, or independently reviewed.

6 Governance and Control Requirements

6.1 Responsible Use of Artificial Intelligence:

6.1.1 CABs shall define, document, and implement the responsible use of artificial intelligence within their conformity assessment processes, ensuring that AI supports — and does not replace competent human judgment.

6.1.2 CABs shall apply a risk-based approach when implementing controls for AI use. The level of governance, oversight, and documentation required shall be proportionate to the risk level associated with the AI application. Higher-risk applications — including those used in healthcare, medical testing, safety-critical inspections, and certification decisions with significant regulatory or public health and safety implications — shall be subject to more stringent controls, enhanced human oversight, and more frequent review and validation than lower-risk administrative or planning support functions.

6.1.3 CABs using AI shall establish and maintain documented controls, including but not limited to the following:

6.1.3.1 Defined Responsible Use

Clear definition of how AI is used within CAB system and processes, aligned with EIAC accreditation requirements and applicable schemes requirements.

6.1.3.2 Algorithmic Impact Assessment (AIA)

Prior to deploying any AI system in CAB activities, it shall conduct a documented Algorithmic Impact Assessment (AIA) to identify, evaluate, and address risks to quality, impartiality, objectivity, and the validity of results. The AIA shall be reviewed and updated periodically, and following any significant change to the AI system or its operational context. AIA records shall be maintained and made available to EIAC upon request.

6.1.3.3 CAB Responsibility and Accountability

The CAB top management shall retain full responsibility for all conformity assessment activities and decisions, regardless of the level of AI support utilized.

6.1.3.4 Human Oversight

Human oversight shall remain central and core to all AI-supported activities, with final technical judgments and decisions made by competent personnel.

6.1.3.5 Confidentiality and Data Protection

Confidentiality of client and assessment data shall be protected at all times. The unauthorized use, training, storage, or processing of such data by artificial intelligence systems is prohibited, unless explicitly agreed through a contractual arrangement between the CAB and its client, and only in accordance with applicable laws and regulations governing data protection, use, and processing.

6.2 Competence, Awareness, and Validation

6.2.1 CABs shall ensure that personnel involved in AI-supported conformity assessment activities are competent and appropriately trained for their assigned roles.

6.2.2 Personnel shall be trained and aware of artificial intelligence ethics, risks, limitations, and best practices, including risks related to bias, over-reliance, and data integrity.

6.2.3 CABs shall validate that artificial intelligence tools used are appropriate for their intended purpose, capable of producing reliable and repeatable outputs, and do not introduce unacceptable risks to impartiality, objectivity, or the validity of conformity assessment results.

6.2.4 CAB personnel shall demonstrate adequate technical understanding of the AI tools applied and the ability to critically evaluate AI outputs, identify anomalies or limitations, and exercise professional judgment.

6.2.5 CABs shall determine and document whether AI-related competencies, controls, and arrangements sufficiently support compliance with the governmental applicable ICT regulations, accreditation requirements, and relevant conformity assessment standards.

6.2.6 Records and Documentation Retention

CABs shall establish, maintain, and retain documented records of all AI-related controls, AIAs, validation activities, competence records, and corrective actions. Records shall be retained for a minimum period consistent with the applicable accreditation scheme requirements, EIAC accreditation rules and procedures, legal obligations, and client contractual arrangements. Records shall be made available to EIAC upon request during surveillance, reassessment, or any investigation activities.

7 Monitoring, Corrective Actions, and Non-Compliance

7.1 Performance Monitoring and Internal Review

7.1.1 CABs shall:

- Monitor the performance of artificial intelligence systems used in conformity assessment activities; and conduct regular internal reviews or audits to verify continued suitability, reliability, fitness for purpose, and compliance with applicable accreditation requirements, standards, and internal controls.

7.2 Corrective Actions

7.2.1 CABs shall:

1. Implement appropriate corrective actions without undue delay where artificial intelligence outputs deviate from expected norms, accuracy, or reliability; and

2. address any identified risks to the integrity, impartiality, or validity of conformity assessment activities arising from the use of artificial intelligence.

7.3 Incident Reporting

7.3.1 CABs shall

1. report to EIAC without undue delay any AI-related incident that has materially affected, or has the potential to materially affect, the validity, integrity, or impartiality of issued conformity assessment results, certificates, or reports. This includes, but is not limited to: AI system failures, data breaches involving AI-processed information, significant AI output anomalies, or the discovery of systematic bias in AI-system.
2. investigate reported incidents, assess the associated risks to the validity, integrity, and impartiality of affected conformity assessment activities, implement appropriate corrective actions without undue delay, and document all findings and actions taken.

7.3.2 Where the risk assessment concludes that the integrity of issued conformity assessment results, certificates, or reports may have been compromised, the CAB shall notify affected clients and take all necessary remedial actions in accordance with the requirements of the applicable accreditation standard.

7.3.3 Where identified risks cannot be adequately controlled, the CAB shall suspend use of the AI system concerned and revert to conventional conformity assessment methods until effective controls are established, documented, and verified.

7.3.4 EIAC may request access to investigation records, risk assessments, and corrective action documentation, and may initiate a review of the CAB's accreditation status as appropriate.

7.4 Reversion to Conventional Conformity Assessment Methods

7.4.1 While EIAC encourages the adoption of modern technologies and the use of innovative approaches in conformity assessment techniques and supports comply with applicable standards and accreditation requirements. The use of artificial intelligence to support conformity assessment activities remains optional and shall not be considered a mandatory or default approach.

7.4.2 Standard conformity assessment methods and techniques shall at all times remain the primary, valid, and acceptable means for conducting conformity assessment activities according to the applicable standards and requirements.

7.4.3 Accordingly, CABs shall:

1. apply conventional, non-AI-supported conformity assessment methods and techniques where agreement on the use of artificial intelligence cannot be reached; and
2. revert without restriction or delay to conventional conformity assessment methods and techniques where

adequate controls, confidentiality and data protection measures, or effective human oversight are not implemented or maintained.

7.5 Consequences of non-compliance

7.5.1 Non-compliance with this Policy may result in one or more of the following actions, in accordance with the applicable EIAC accreditation requirements and procedures:

1. nonconformities being raised during the assessment.
2. limitation, suspension, reduction, or withdrawal of accreditation scope; and
3. other appropriate actions as determined by EIAC.

8 Effective Date and Transition

8.1 This Policy comes into effect on the date of its issuance and publication on the EIAC official website.

CABs that are currently using AI in conformity assessment activities at the time of issuance shall achieve full compliance with the general requirements of this Policy within six (6) months of the effective date. However, compliance with the restricted use provisions shall be required immediately upon the effective date, with no transition period granted.

8.2 New applications for accreditation submitted after the effective date shall demonstrate full compliance with all requirements, including restricted use provisions, from the outset.

9 Bibliography

9.1 Dubai Digital Authority: Artificial Intelligence Policy and applicable digital governance requirements.

9.2 Emirates International Accreditation Centre (EIAC): Applicable accreditation schemes, accreditation criteria, mandatory requirements, policies, and procedures governing accredited conformity assessment activities.

9.3 Global Accreditation Cooperation Incorporated (Global ACI): Mandatory documents, policies, and recognition requirements relevant to conformity assessment activities accreditation process.

9.4 ISO/IEC 17011 Conformity assessment — General requirements for accreditation bodies accrediting conformity assessment bodies.

This Policy shall be read and implemented in alignment with the Dubai Digital Authority Artificial Intelligence Policy, and other applicable artificial intelligence regulations issued by the competent authorities.