Technical Bulletin: The use of Artificial Intelligence (AI) technologies in accredited conformity assessment

20 June 2025

0. Purpose

0.1. This Technical Bulletin is applicable to all UKAS applicant and accredited conformity assessment bodies (CABs) adopting artificial intelligence (AI) technologies and tools in their business activities. It seeks to establish a set of principles for the responsible development, deployment and use of AI technologies. It is not the intention to establish new or additional requirements for accreditation, but to contextualise existing requirements. This document shall be read in parallel with the relevant standard(s) used for accreditation which remain the authoritative document(s).

1. Guiding principles for AI use in conformity assessment

1.1. Establishing a set of principles for the responsible development, deployment, and use of AI technologies is adopted in a manner that is responsible, ethical, transparent, and beneficial to stakeholders. By establishing these principles, organisations can help mitigate potential risks, such as bias, privacy violations, and unintended consequences, whilst maintaining the integrity, consistency, reliability and technical rigour of accredited conformity assessment services.

1.2. While a set of principles for this purpose has yet to be universally agreed, there are a number of common themes emerging. For the purposes of this technical bulletin, UKAS has defined the following core principles to support the use of AI by CABs and UKAS's assessment activities.

Principle	Description
Accountability and governance	Effective governance measures should be in place to ensure oversight of AI systems and establish clear lines of accountability across the AI lifecycle.
Bias and fairness	AI systems shall not undermine legal rights, discriminate unfairly, or create unjust market outcomes.
Safety, security, and robustness	AI systems should function in a robust, secure, and safe manner throughout their lifecycle, with risks continuously identified, assessed, and managed.
Transparency and explainability	AI systems should be appropriately transparent and explainable, ensuring stakeholders understand how decisions are made.
Contestability and redress	Users, impacted third parties, and stakeholders should have the ability to challenge AI-driven decisions or outcomes that may cause harm or introduce material risks.

1.3. As part of maintaining effective communication and ongoing compliance with the requirements for accreditation CABs are reminded of the expectation to inform UKAS, at the earliest opportunity, of any significant changes to equipment, resources, or their conformity assessment processes, practices, or procedures. The adoption or implementation of AI technologies is considered a noteworthy development. CABs are therefore required to notify UKAS - initially via their allocated Assessment Manager - so that any potential impacts can be reviewed and, where appropriate, additional assessment activities can be considered.

2. Accountability and governance

2.1. Roles, responsibilities and authorities

2.1.1. CABs should ensure that the responsibilities and authorities for any AI systems are clearly assigned and communicated within the organisation. This should include the assignment of a responsibility for deciding that an AI system is fit for purpose and authorises its deployment and use.

2.1.2. CABs should assign responsibility and authority for the following:

- Ensuring that the AI systems continue to meet the requirements of the relevant standard(s) used for accreditation.
- Regularly reporting the ongoing performance and use of the AI systems to the CABs top management.
- Regularly reviewing the performance and use of AI systems to ensure they remain suitable, adequate, and effective in fulfilling the principles outlined in this document.
- Providing effective oversight and control of the AI systems.
- Considering the risks that the AI systems may pose to the competence, consistency, and impartiality of the conformity assessment process and its outcomes.

2.2. Competence

2.2.1. CABs should determine and provide the resources needed for the responsible development, deployment, and use of AI systems within their conformity assessment processes.

2.2.2. CABs should ensure that personnel have the competence to use AI systems when undertaking conformity assessment activities and to recognise and evaluate the significance of any unexpected outputs from such AI systems.

2.2.3. CABs should monitor the ongoing competence and performance of all personnel involved in the development, deployment, and use of AI systems and should be able to demonstrate that its monitoring activities are effective.

2.2.4. CABs should have access to the necessary technical expertise for advice on matters relating to the ongoing operation and maintenance of the AI systems or in instances where unexpected outputs from such AI systems prompt for such expertise. Such advice may be provided from external resources.

2.3. Risk-based approach

2.3.1. CABs should undertake and document an AI system impact assessment for each AI system deployed. This assessment should determine the potential effects that the deployment, intended use, and foreseeable misuse of an AI system may have on individuals, groups, or society as a whole.

2.3.2. CABs should define a process to identify, analyse, evaluate, treat, monitor, and document the risks related to the responsible development, deployment, and use of AI systems within their conformity assessment processes. This process should be designed to ensure that repeated AI risk assessments produce consistent, valid, and comparable results. CABs should consider the results of the AI system impact assessments in its risk assessments.

2.3.3. When threats to the competence, consistency, and impartiality of the conformity assessment process or outcomes are identified, CABs should document and demonstrate how it eliminates or minimises such threats and document any residual risk.

2.3.4. CABs should retain suitable and sufficient documented information about the operation of the AI risk assessment process to readily demonstrate its effective operation.

2.3.5. When determining their system impact and risk assessment approach(es), CABs should consider published guidance from publicly available sources to inform their approach and help ensure the approach adopted is fit for purpose.

2.4. Internal audit and management review

2.4.1. CABs should ensure that deployed AI systems are subject to an appropriate level of internal audit. The frequency of these internal audits should be determined and technically justified, considering the results of the AI system impact assessment and risk assessment processes.

2.4.2. CABs' management review should include a formal review of the AI system impact assessment and risk assessment process outputs, as well as the results of the internal audits of those AI systems. This is to ensure that any threats to the competence, consistency, and impartiality of the conformity assessment process or outcomes are being managed and mitigated in a timely manner.

3. Bias and fairness

Bias in AI systems refers to the presence of systematic errors or prejudices that can lead to incorrect outcomes. These biases can arise from various sources, such as the data used to train the AI, the algorithms themselves, or even the way the AI is deployed. Bias can also manifest as over-reliance on the recommendations or outputs of AI systems.

Fairness, on the other hand, is about ensuring that AI systems treat all individuals and groups equitably. This means that the outcomes produced by the AI should not disproportionately benefit or harm any particular group.

3.1. Impartiality

3.1.1. When deploying AI systems in the conformity assessment process, CABs should demonstrate that these activities are undertaken impartially.

3.1.2. CABs should be responsible for the impartiality of its conformity assessment activities and should not allow the use of AI systems in these activities to compromise impartiality under any circumstances.

3.1.3. CABs should take action to respond to any risks to its impartiality arising from the implementation or use of any AI systems, as soon as it becomes aware of them.

3.1.4. CABs should ensure that the risk of over-reliance on the recommendations or outputs of AI systems is appropriately managed and mitigated through their risk assessment process.

NOTE: Risk mitigation strategies may include (but are not limited to) regular audits and monitoring, user education and training, and maintaining a human-in-the-loop oversight mechanism.

3.2. Non-discriminatory conditions

3.2.1. The AI systems implemented by CABs in their conformity assessment activities should be non-discriminatory. CABs should ensure that when developing and deploying their own AI systems, their use does not create discriminatory conditions or unfair conformity assessment outcomes that compromise the integrity and impartiality of the conformity assessment process.

3.2.2. CABs should ensure that when compensating for bias identified in one area, they do not inadvertently increase bias in another context.

4. Safety, security, and robustness

4.1. Confidentiality

4.1.1. CABs should develop and document policies and procedures to ensure confidentiality is maintained as it develops, deploys, and uses AI systems throughout the conformity assessment process. CABs should also have measures in place to take corrective actions when security breaches occur.

4.1.2. When a CAB is developing its own AI systems, policies and procedures it should include provisions to minimise the risk of inadvertent exposure or unauthorised access to datasets that include sensitive client information.

4.1.3. CABs should be responsible, through legally enforceable commitments, for the information it shares with third-party AI developers or providers. CABs are reminded that sharing confidential information with those third parties might inadvertently breach previously established confidentiality agreements, and they should ensure such breaches do not occur.

4.1.4. CABs should inform their clients in advance of the information they intend to use for building large datasets for the training and operation of any AI systems developed, deployed, or used.

4.2. Control of data and information management

4.2.1. CABs should have access to the data and information needed to perform their conformity assessment activities.

4.2.2. CABs AI systems used for collecting, processing, recording, reporting, sharing, storing, or retrieving data should be validated for functionality, including the proper functioning of interfaces within the AI systems, by CABs before introduction. Whenever there are any changes, including CAB software configuration or modifications to commercial off-the-shelf software, they should be authorised, the risks documented, and validated before implementation.

4.2.3. The AI systems should:

a) be protected from unauthorised access;
b) be secured against tampering and loss;
c) be operated in an environment that complies with the AI systems provider or CAB specifications;
d) be maintained in a manner that ensures the integrity of the data and information;
e) be monitored, and outputs assessed, and any perceived failures should be investigated and corrective action taken.

4.2.4. When AI systems are managed and maintained off-site or through an external provider, CABs should ensure that the provider or operator of the system complies with all applicable requirements of this document and those defined in the accreditation criteria standards used for UKAS assessments.

4.2.5. CABs should ensure that instructions, documentation, manuals, and reference data relevant to AI systems are made readily available to conformity assessment personnel.

5. Transparency and explainability

5.1. Verification and validation of AI system(s) performance

5.1.1. CABs should demonstrate the validity of the AI systems it develops, deploys, and uses conform to specified requirements before being used in the conformity assessment process.

5.1.2. AI systems should be demonstrably capable of consistently delivering the required output accuracy needed to provide technically valid conformity assessment outcomes.

5.1.3. AI systems that are found to give questionable output results, or are defective or outside specified requirements, should be taken out of service. These AI systems should not return to service until they have been corrected and demonstrably verified to perform correctly. CABs should examine the effect of the defect or deviation from specified requirements and should initiate the management of nonconforming work procedure (see 5.3).

5.1.4. When checks are necessary to maintain confidence in the performance of the AI systems, these checks should be carried out according to a documented procedure.

5.1.5. CABs should validate AI systems according to a documented procedure. The validation should be as extensive as necessary to meet the needs of the given application or field of application.

5.1.6. When changes are made to a validated AI system, the impact of such changes should be determined. If these changes affect the original validation, a new AI system validation should be performed.

5.2. Ensuring the validity of conformity assessment outcomes

5.2.1. CABs should have a procedure for monitoring the validity of AI system outputs. The resulting data should be recorded in such a way that trends are detectable, and where practicable, statistical techniques should be applied to review the validity of the outputs.

5.2.2. The monitoring of the validity of AI system outputs should be planned, and the frequency should take into consideration the importance of the AI system's role in determining conformity assessment outcomes, the results of previous performance monitoring activities, AI system impact assessment(s) and the identified risks associated with its use (see 2.3).

5.2.3. Data from monitoring activities should be analysed and used to improve the AI system's performance. If the results of the analysis of data from monitoring activities are found to be outside pre-defined criteria, appropriate action should be taken to prevent incorrect conformity assessment outcomes from being reported.

5.3. Nonconforming work

5.3.1. CABs should have a procedure to follow when any aspect of AI system outputs does not conform to its own procedures (e.g., when AI system outputs are not as expected, or results of monitoring fail to meet specified criteria). The procedure should ensure that:

- Responsibilities and authorities for managing nonconforming work are defined.
- Actions (including halting or repeating work and withholding reports, as necessary) are based on the risk levels established by CABs.
- An evaluation is made of the significance of the nonconforming work, including an impact analysis on previous conformity assessment outcomes.
- A decision is taken on the acceptability of the nonconforming work.
- Where necessary, the client is notified, and work is recalled.
- Where necessary, AI system impact assessment(s) and risk assessment(s) are reviewed and updated.
- The responsibility for authorising the resumption of work is defined.

5.3.2. CABs should retain records of nonconforming work and all actions taken.

5.3.3. If the evaluation indicates that the nonconforming work may recur, or if there is doubt about the conformity of the CAB's operations with its own management system, CABs should implement corrective action.

5.4. Openness

5.4.1. CABs should maintain and make public, in all the geographical areas in which it operates, clear and unambiguous information about:

a) how AI systems are used to provide the conformity assessment services;

b) how the AI system outputs have been verified or validated to confirm their suitability for use;

c) how CABs monitor and periodically revalidate the AI systems for continued suitability and reliability.

5.4.2. CABs should ensure that clients are provided with a clear and accessible mechanism to process complaints, and where appropriate seek redress, for any AI system outputs they believe to be incorrect.

5.5. Addressing AI system output complaints

5.5.1. CABs should have a documented process to receive, evaluate, and make decisions on complaints received regarding the technical validity of AI system outputs, including internal challenges highlighted through whistleblowing procedures.

5.5.2. Submission, investigation, and decision on AI system output complaints should not result in any discriminatory actions against the parties or persons raising the challenge with CABs.

5.5.3. The challenge-handling process should include at least the following elements and methods:

a) An outline of the process for receiving, validating, and investigating the complaint, and for deciding what actions need to be taken in response to it, taking into account the results of previous similar complaints.

b) Tracking and recording complaints, including actions undertaken to resolve them.

c) Ensuring that any appropriate correction and corrective action are documented and taken.

5.5.4. CABs receiving the complaint should be responsible for gathering and verifying all necessary information to validate the complaint.

5.5.5. CABs should acknowledge receipt of the complaint and provide the parties raising the complaint with progress reports and the result of the complaint investigation.

5.5.6. The decision to be communicated to the parties raising the complaint should be made by, or reviewed and approved by, individuals not previously involved in the subject of the complaint.

5.5.7. CABs should give formal notice to the parties raising the complaint of the end of the complaint investigation process.