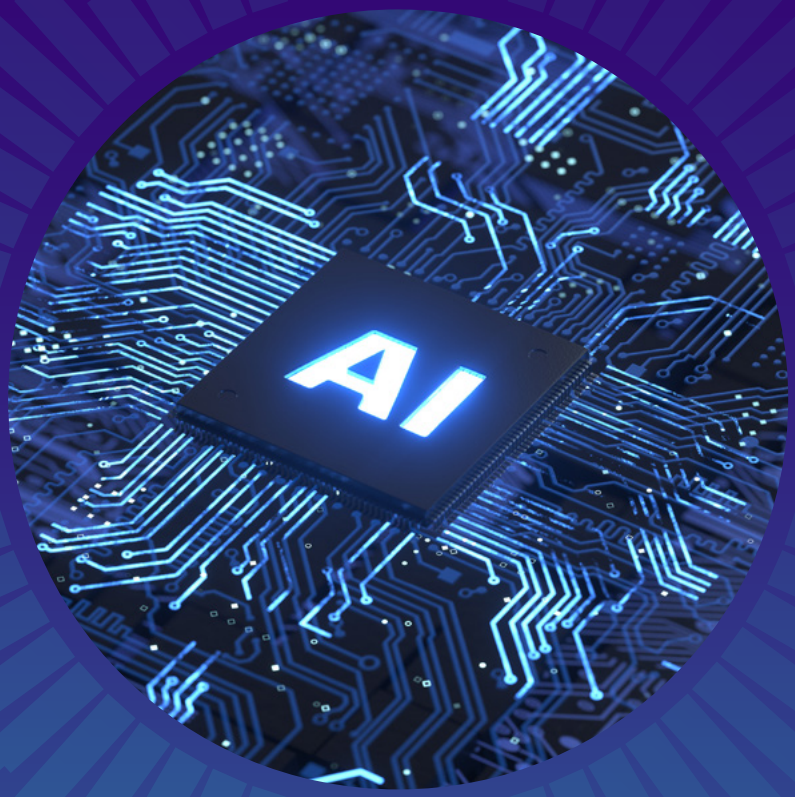


Technical Bulletin

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

This document was created in partnership between:

UKAS
A world of confidence

DAkkS
Deutsche
Akkreditierungsstelle

Introduction

This joint Technical Bulletin sets out shared considerations of UKAS and DAkkS to provide informative guidance regarding the responsible development, deployment, and use of Artificial Intelligence (AI) technologies and tools by conformity assessment bodies (CABs) in their business activities. It does not establish new or additional requirements for accreditation, but intends to support CABs in identifying and contextualising existing applicable requirements which are potentially formulated technology-agnostic. Hence, this document shall be read in parallel with the relevant standard(s) used for accreditation which remain the authoritative document(s). Existing requirements for CABs remain unaffected by this document, including in the context of the use of AI systems.

Obligation to inform national accreditation bodies (NABs) when introducing AI into conformity assessment processes

As part of maintaining effective communication and ongoing compliance with the requirements for accreditation, CABs are reminded of the need to inform their NAB, 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 their NAB so that any potential impacts can be reviewed and, where appropriate, additional assessment activities can be considered. The notification should include at least:

+ a brief description of the AI system including the specific function or purpose the AI system is designed to perform, the utilised training data/knowledge, and the implementation approach (e.g., machine learning concepts and algorithms);
+ information on where in the functional approach/conformity assessment process the AI system is used; and
+ the degree of reliance on the AI system (e.g., purely administrative support; advisory or decision-support functionality; and any attempt to delegate decisions to AI).

Because this documentation can also be utilised by the CAB to identify the requirements relevant to their application of AI, a prerequisite for ensuring conformity, it is in the CAB's own interest to assemble this information diligently.

Context sensitivity

AI is a *general-purpose technology* that can be used in various ways and contexts by CABs, therefore deriving a uniform or 'one-size-fits-all' set of requirements from the Level 3 Standards (e.g., ISO/IEC 17025, ISO/IEC 17024, ISO/IEC 17065) applicable to all uses of AI systems by CABs is neither feasible nor appropriate.

Instead, a context-sensitive evaluation, i.e., considering the specific technical specifications, use case, and context, is necessary to determine which requirements are relevant and how these must be contextualised and implemented in practice. This is because the specific application and technical features of an AI system and the context in which it is applied determines the applicability of requirements from the respective standards.

At least three aspects must be considered when evaluating AI in conformity assessment to determine context sensitivity.

1. Type of AI system

In order to identify relevant requirements and assess their applicability, the AI system must be analysed and described at a technical level. Use of Internationally standardised terminology should be used for this purpose from ISO/IEC 22989 *information technology — Artificial intelligence — Artificial intelligence concepts and terminology*.[1]

The analysis must be described at a technical level and include the tasks the system performs, the data/knowledge that was used for model training purposes and is intended to be used as input, and the implementation approach.

+ Application areas:

The application areas refers to the specific function or purpose the AI system is designed to perform within the CAB's processes. The nature of these tasks is a primary determinant of potential risks and, consequently, the applicability and priority of certain requirements derived from the Level 3 Standards. For example, different requirements will be applicable to an AI system used for automated document review from the ones used for predictive maintenance, for example for equipment or facilities being assessed.

To describe the tasks and application areas, ISO/IEC 22989 Section 9 (*Fields of AI*) and Section 10 (*Applications of AI systems*) provide examples, concepts and terminology. However, as AI is a general-purpose technology, the standard does not cover all possible use cases that might be relevant for CABs. Therefore, in some cases it is advisable to consult further sector or technology specific standards.

+ Training data/knowledge:

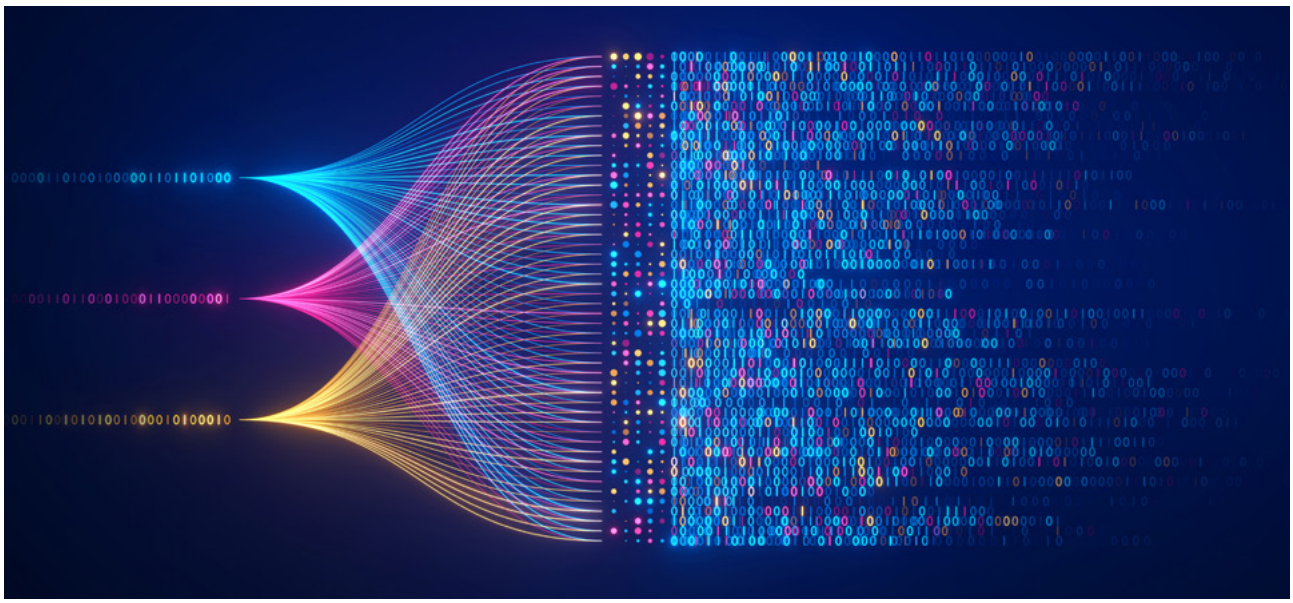
Data serves as the foundation for AI system performance and reliability, encompassing both the training data used to develop the model and the input data processed during operation. The nature of this data, e.g., whether it is structured (e.g., relational databases) or unstructured (e.g., images, audio, or natural language text), directly influences the technical complexity of data handling and affects the potential for bias or error. Furthermore, the origin and sensitivity of the data might directly influence the applicability of requirements regarding confidentiality or information obligations towards customers.

+ Implementation approach:

The implementation approach refers to the specific computational techniques and algorithms used. This includes the selection of specific machine learning concepts (e.g., *supervised or reinforcement learning*) and algorithms (e.g., neural networks, decision trees, or support vector machines). The underlying design decisions are a critical determinant of requirements, particularly regarding explainability and validation. For instance, rule-based systems are generally more explainable than deep learning models, which may require additional measures to satisfy transparency obligations. The implementation approach dictates whether the system operates as a static trained model or utilises continuous learning, with the latter potentially necessitating additional safeguards such as a more rigorous regime of continuous validation during operation.

ISO/IEC 22989 Section 5.11 (*Machine learning concepts*) and Section 5.12 (*Examples of machine learning algorithms*) provide examples, concepts and terminology. Other Sections of ISO/IEC 22989 provide further concepts and terminology on non-machine-learning-based AI systems.

1. The standard is available free of charge at https://www.iso.org/standard/74296.html.



2. The use of the AI system within the conformity assessment process

The tasks for which the AI system is deployed matters significantly. Systems used for administrative tasks (e.g., translating emails) entail different risks and requirements compared to those that directly affect decisions on conformity. The applicability of most requirements from Level 3 Standards is heavily dependent on whether the AI system is used in one of the core process steps of conformity assessment.

Administrative tasks that do not affect decisions on conformity may be suitable to allocate to AI systems. It is vital to differentiate between applying AI in administrative functions (such as translating internal non-technical correspondence) and applying it in a way that integrates into the functional approach (such as translating technical documentation used as input for determination). Correctly identifying whether a system supports a functional step of the conformity assessment process or serves a solely administrative purpose with no impact on conformity decisions is therefore a prerequisite for determining the relevant requirements and the associated risk profile.

3. Degree of reliance on the AI system

The third factor that determines the applicability of the requirements is the degree to which the CAB relies on the AI system. While the positioning of the AI system within the functional approach or conformity assessment process identifies which process steps are affected, the degree of reliance determines how stringent the requirements need to be. This factor directly influences the necessity for human oversight and the level of system validation required to address the risks associated with the use of the AI system.

The greater the reliance on the system's output for critical assessment steps, the more robust the necessary safeguards must be.

The AI system's role can be categorised into one of three main categories:

+ purely administrative support;
+ advisory or decision-support functionality; and
+ any attempt to delegate decisions to AI.

Systems that only offer administrative support (which, by definition, have no impact on conformity decisions) entail the lowest risk. Advisory AI systems require rigorous human competence and validation of the functioning of the AI system. If essential steps of the conformity assessment process are affected, processes need to be in place to account for automation bias and similar risks of overconfidence on the system by human decision-makers relying on the support systems. Importantly, final decisions on conformity (the review and decision function, as defined by ISO/IEC 17000) must not be delegated to an AI system under current accreditation frameworks.

Procedural perspective: How to identify and contextualise relevant requirements

Contextualising the relevant requirements requires a dedicated translation step when applied to AI. It is necessary to systematically map the specific features and risks of the AI system in question back to the existing Level 3 Standard. This allows the CAB to identify where the standard's existing requirements must be interpreted through the lens of the specific AI technology being deployed.

The procedure begins with the identification of the applicable Level 3 Standard and a review of the AI system's profile or documentation as defined in the previous sections, i.e., specifically its technical features, its role in the functional approach, and the degree of reliance placed upon it. The CAB should conduct a clause-by-clause analysis, cross-referencing these system characteristics against the standard's requirements to determine applicability.

This contextual analysis reveals which generic requirements are specifically triggered by the use case. For example, if the system involves sharing data with external providers or using client data for model training (including continuous learning), the standard's requirements regarding confidentiality and the management of external provision are potentially implicated. Similarly, if the AI system is used within the evaluation process, it must be validated as a technical resource to ensure it supports the integrity of the conformity decision and may also necessitate updating publicly available information regarding the assessment process to inform potential customers on the use of AI in the evaluation process. Furthermore, such a use of AI impacts personnel requirements, requiring that competence criteria and training be expanded to ensure employees can effectively manage the system and mitigate risks such as (systematic) overconfidence in an AI system's output ('automation bias').

Adherence to the identified requirements from Level 3 Standards may necessitate the implementation of distinct organisational processes or specific technical safeguards. On a procedural level, this might involve establishing effective human oversight mechanisms, mandating the cross-verification of AI-generated results against established procedures, and ensuring that personnel possess the specific competence to detect system errors or anomalies. On a technical level, compliance may dictate specific system configurations or design choices, such as processing data locally to ensure confidentiality, or implementing safeguards to prevent customer data from being used to train the model. While the Level 3 Standards mandate these general obligations, they do not prescribe the technical specifications. Therefore, CABs should refer to Level 5 Standards to determine the expected 'state-of-the-art' regarding technical attributes such as accuracy, transparency, and robustness if requirements for these technical attributes are derived from the Level 3 Standard.

In certain scenarios, few requirements are applicable. This is the case, for instance, if an AI system is used to translate purely administrative emails. In such cases, the CAB ensures (by either processes or technical means) that confidentiality is maintained and that the system is not used outside its intended scope, preventing its use for tasks like translating technical documentation that could influence decisions on conformity.

Evaluation of the setting may reveal also that a specific requirement fundamentally prohibits an intended use case. For example, where a Level 3 Standard explicitly assigns the responsibility for a certification decision to a competent person, the substitution of this individual with an autonomous AI-based decision-making system would be incompatible with the standard. In such instances, the requirement does not merely shape the implementation but acts as a strict boundary, preventing the delegation of authority to an algorithm regardless of the system's technical specifications. Consequently, CABs must identify these hard constraints early to ensure that their adoption of AI remains within the limits of the applicable accreditation framework.

UKAS
A world of confidence

DAkkS
Deutsche
Akkreditierungsstelle

United Kingdom Accreditation Service (UKAS)

Registered Office:
Building Two, Pine Trees, Chertsey Lane,
Staines-upon-Thames, Surrey, TW18 3HR
United Kingdom

Tel: +44 (0)1784 429000
Website: www.ukas.com

Registered in England as a Company Limited by Guarantee

Company Number: 3076190

Deutsche Akkreditierungsstelle GmbH (DAkkS)

Registered Office:
Spittelmarkt 10, 10117 Berlin Germany

Tel: +49 (0)30 670591-0
Email: kontakt@dakks.de
Website: www.dakks.de

Executive Board: Dr.-Ing. Stephan Finke

Chair of the Supervisory Board:
Bernd Kowalski

Court: AG Berlin-Charlottenburg

Register number: HRB 122846 B

VAT ID number: DE815123526