



**Certification for Ethical and Regulatory Transparency  
in Artificial Intelligence**

# **D6.2: TEMPLATE FOR ACCREDITING THIRD- PARTY EVALUATION LABORATORY**



**Co-funded by  
the European Union**

**Project funded by**



**Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra**

Swiss Confederation

**Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI**

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Work package</b>      | WP6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Task</b>              | Task 6.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Due date</b>          | 31/07/2026                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Submission date</b>   | 31/07/2026                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Deliverable lead</b>  | Red Alert Labs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Version</b>           | 1.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Authors</b>           | Lea El-Khoury (Red Alert Labs)<br>Nataël Couturier (Red Alert Labs)<br>Sushil Bhattacharjee (IDIAP)<br>Ali Kordia (UL)<br>Parul Chaudhary (28D)<br>Yannis Krasonikolakis (NBG)<br>Petros Vamvakaris (NBG)                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Reviewers</b>         | Claude BAUZOU (IPS)<br>Ilyes Azouani (CLR Labs)<br>Aljaž HÖLB (UKCM)<br>Šefik SALKUNIĆ (UKCM)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Security reviewer</b> | None                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Abstract</b>          | The growing use of Artificial Intelligence (AI) in critical sectors requires reliable and standardized evaluation mechanisms. This deliverable presents a Notification Toolkit designed to support National Competent Authorities (NCAs) in assessing and overseeing independent AI evaluation laboratories, in alignment with emerging EU regulations such as the AI Act. The toolkit aim is to help NCA to verify the suitability of an evaluation laboratory to perform test in a given AI domain of application. It could also enhance harmonized practices across Member States, ensure transparent evaluation processes, and strengthen trust in AI system assessments. |
| <b>Keywords</b>          | Template, qualification, notification, third party, evaluation laboratory                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Document Revision History

| Version | Date       | Description of change         | List of contributors                                                                                                                                                                                      |
|---------|------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V1.0    | 27/07/2026 | Version ready for publication | Lea El-Khoury (Red Alert Labs)<br>Nataël Couturier (Red Alert Labs)<br>Sushil Bhattacharjee (IDIAP)<br>Ali Kordia (UL)<br>Parul Chaudhary (28D)<br>Yannis Krasonikolakis (NBG)<br>Petros Vamvakaris (NBG) |

Grant Agreement No: 101189650

|

Topic: HORIZON-CL4-2024-DATA-01-01

Call: HORIZON-CL4-2024-DATA-01.

|

Type of action: HORIZON-IA

REVIEWERS COMMENTS

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |     |                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----------------------------|
| Claude Bazou                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | IPS | Date of review: 09/07/2026 |
| <p>The review covered the main document and all annexes up to Annex E. Several open questions and suggested improvements were inserted throughout the document; however, the overall assessment is positive, as the deliverable is well structured and adequately addresses the objectives and expected scope of the task.</p> <p>Regarding Annex E, it is recommended to include a concise placeholder describing the target audience, the planned training structure, the expected availability, and the intended delivery format.</p> |     |                            |

|                                                                                                                                                                                                                                                                                                                                                                                                                                     |      |                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|----------------------------|
| Aljaž HÖLB / Šefik SALKUNIĆ                                                                                                                                                                                                                                                                                                                                                                                                         | UKCM | Date of review: 20/07/2026 |
| <p>The documents still appear to be in version 0.8, so some template placeholders remain and not all sections are complete. Overall, the content is well organized, technically consistent and generally aligned across the documents. Most of the issues we identified are editorial in nature, such as formatting inconsistencies, remaining placeholders and minor text improvements, rather than technical or content wise.</p> |      |                            |

CLR Labs is not a member of the CERTAIN consortium. They were invited by IPS and were pertinent to provide comments reflecting the perspective of an ISO/IEC 17025-accredited security evaluation laboratory currently operating in the AI testing domain and combining two complementary viewpoints: the quality/accreditation expert perspective (direct target audience of the deliverable) and the technical AI evaluation perspective.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                       |                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|----------------------------|
| Ilyes Azouani                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | (external to the consortium) CLR LABS | Date of review: 21/07/2026 |
| <p>The corpus is technically valid and, in our view, fills a real gap: should a laboratory engage tomorrow in an accreditation process on the AI perimeter, national accreditation bodies (e.g. COFRAC in France) and their technical experts currently have no compass. AI evaluation carries specificities that do not exist in traditional software evaluation, and even less in other accredited domains. A structured reference of this kind is therefore welcome and needed.</p> |                                       |                            |

DISCLAIMER



Co-funded by  
the European Union

Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

The CERTAIN project received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No 101189650. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

COPYRIGHT NOTICE

© 2024 – 2027 CERTAIN

| Project funded by the European Commission in the Horizon Europe Programme |                                                                                                                        |                                     |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| Nature of the deliverable:                                                | R (report)                                                                                                             |                                     |
|                                                                           | Dissemination Level                                                                                                    |                                     |
| PU                                                                        | Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page) | <input checked="" type="checkbox"/> |
| SEN                                                                       | Sensitive, limited under the conditions of the Grant Agreement                                                         | <input type="checkbox"/>            |

## TABLE OF CONTENT

|                                                        |           |
|--------------------------------------------------------|-----------|
| Reviewers comments .....                               | 3         |
| DISCLAIMER.....                                        | 4         |
| Copyright notice .....                                 | 4         |
| <b>TABLE OF CONTENT .....</b>                          | <b>5</b>  |
| <b>EXECUTIVE SUMMARY .....</b>                         | <b>7</b>  |
| <b>TITLE TERMINOLOGY NOTE .....</b>                    | <b>8</b>  |
| <b>INTRODUCTION .....</b>                              | <b>11</b> |
| 1.1 Background and context .....                       | 11        |
| 1.2 Purpose of this document.....                      | 12        |
| 1.3 Objectives .....                                   | 13        |
| 1.4 SCOPE .....                                        | 14        |
| 1.5 Description of each Annex.....                     | 15        |
| <b>2. CONCLUSIONS.....</b>                             | <b>18</b> |
| <b>A. ANNEX A: LAB APPLICATION FORM.....</b>           | <b>19</b> |
| A.1 Purpose of this Annex .....                        | 19        |
| A.2 General information.....                           | 20        |
| A.3 Requested Scope of Notification.....               | 21        |
| A.4 Laboratory description .....                       | 21        |
| A.5 Personnel and Competence .....                     | 22        |
| A.6 Technical Resources .....                          | 22        |
| A.7 Testing Methods and validation .....               | 23        |
| A.8 Quality Management System.....                     | 23        |
| A.9 Traceability and reproducibility .....             | 24        |
| A.10 Supporting Documentation .....                    | 25        |
| A.11 Declaration.....                                  | 25        |
| <b>B. ANNEX B: COMPETENCE OF PERSONNEL.....</b>        | <b>26</b> |
| B.1 Introduction.....                                  | 26        |
| B.2 Metrology and Data integrity.....                  | 26        |
| B.3 Competence in Probability and Statistics.....      | 28        |
| B.4 AI-specific Testing Methodologies.....             | 30        |
| B.5 Technical Competencies .....                       | 32        |
| B.6 Behavioural competencies .....                     | 34        |
| <b>C. ANNEX C: TECHNICAL CAPABILITY INVENTORY.....</b> | <b>36</b> |
| C.1 Introduction.....                                  | 36        |

|           |                                                                                |           |
|-----------|--------------------------------------------------------------------------------|-----------|
| C.2       | Testing Scope and regulatory Mapping Matrix.....                               | 36        |
| C.3       | Equipment and reference data Log .....                                         | 38        |
| C.4       | Environment and Data constraints log .....                                     | 40        |
| C.5       | Method, software and technical resource validation registry.....               | 42        |
| <b>D.</b> | <b>ANNEX D: CHECKLIST AUDIT.....</b>                                           | <b>47</b> |
| D.1       | Laboratory audit information.....                                              | 47        |
| D.2       | Audit Area 1- Legal and organizational framework .....                         | 47        |
| D.3       | Audit Area 2- Independence and Impartiality.....                               | 48        |
| D.4       | Audit Area 3- Personnel competence.....                                        | 48        |
| D.5       | Audit Area 4- Equipment and infrastructure .....                               | 49        |
| D.6       | Audit Area 5- Quality management system .....                                  | 49        |
| D.7       | Audit Area 6- Conformity Assessment Activities .....                           | 50        |
| D.8       | Audit Area 7- External Providers .....                                         | 50        |
| D.9       | Audit Area 8- Information Security and Cybersecurity.....                      | 51        |
| D.10      | Audit Area 9- Confidentiality.....                                             | 51        |
| D.11      | Audit Area 10- Standardization and Regulatory Monitoring.....                  | 52        |
| D.12      | Audit Summary.....                                                             | 52        |
| <b>E.</b> | <b>ANNEX E: TRAINING CURRICULUM TEMPLATE.....</b>                              | <b>54</b> |
| E.1       | Purpose.....                                                                   | 54        |
| <b>F.</b> | <b>ANNEX F: REPORTING TEMPLATE .....</b>                                       | <b>55</b> |
| F.1       | Part I- Report identification and administrative information.....              | 55        |
| F.2       | Part II – Regulatory Basis and Purpose of the audit .....                      | 58        |
| F.3       | Part III- Assessment of legal Status and organizational structure .....        | 59        |
| F.4       | Part IV- Assessment of Independence and Impartiality.....                      | 61        |
| F.5       | Part V- Assessment of Human Resources and technical competence .....           | 62        |
| F.6       | Part VI- Assessment of Quality Management, Processes, and Cybersecurity .....  | 66        |
| F.7       | Part VII- Assessment of confidentiality obligations .....                      | 70        |
| F.8       | Part VIII- Assessment of Liability insurance.....                              | 71        |
| F.9       | Part IX- Assessment of Participation in Coordination and Standardisation ..... | 73        |
| F.10      | Part X- Overall Audit Findings and Summary Table.....                          | 74        |
| F.11      | Part XI- Non-conformity Register.....                                          | 75        |
| F.12      | Part XII- Notification Recommendation.....                                     | 76        |
| F.13      | Part XIII- Signatures and Validation.....                                      | 76        |
| <b>G.</b> | <b>ANNEX G- SURVEILLANCE AND COMPLAINT HANDLING.....</b>                       | <b>79</b> |
| G.1       | Purpose of this Annex .....                                                    | 79        |
| G.2       | Notification Monitoring, Surveillance and Complaint handling .....             | 79        |

## EXECUTIVE SUMMARY

The increasing deployment of Artificial Intelligence (AI) systems across critical sectors has created a strong need for reliable, independent, and standardized evaluation mechanisms. National Competent Authorities (NCAs) play a key role in ensuring that such assessments are conducted by competent, independent, and trustworthy bodies, in line with European regulatory requirements.

This deliverable presents a qualification toolkit for Independent AI Evaluation Laboratories, developed under Task T6.2. The toolkit provides a practical, modular, and reusable framework to support NCAs in assessing, qualifying, notifying and overseeing independent testing laboratories within specific AI application domains. It is designed to align with the evolving EU regulatory landscape, including the AI Act.

This document is not intended to define a formal accreditation or notification scheme or prescribe a mandatory accreditation or notification process for independent AI evaluation laboratories. Rather, it proposes a set of principles, methodologies, procedures, templates, and supporting tools that NCAs may use when designing, implementing, adapting, or strengthening their own accreditation, qualification, notification and oversight processes.

The methodologies, templates, and supporting tools proposed in this deliverable are intended to assist National Competent Authorities (NCAs) and National Accreditation Bodies (NABs) during the qualification and notification of laboratory, irrespective of whether a Member State relies on accreditation, direct assessment by the notifying authority, or a combination of both approaches.

The AI Act distinguishes between accreditation, designation, and notification, while leaving Member States flexibility in the organisation of their national conformity assessment infrastructure. Depending on the national legal framework, the sector concerned, and the applicable conformity assessment procedures or assurance levels, the practical implementation of these activities may differ. In some Member States, the assessment performed during accreditation may constitute the primary technical evaluation supporting notification, resulting in closely coordinated or partially integrated accreditation and notification processes. Furthermore, where permitted under national legislation and the institutional organisation of the Member State, the National Accreditation Body may also perform the functions of the notifying authority, or the notifying authority may rely extensively on the accreditation assessment when reaching its notification decision. The guidance presented in this deliverable is therefore designed to remain applicable regardless of the specific national governance model adopted for accreditation and notification.

Accordingly, the procedures, templates and recommendations presented in this deliverable should be interpreted as implementation guidance that can be adapted to the institutional arrangements established by each Member State, rather than as a prescriptive accreditation or notification framework.

The toolkit consists of:

- A main document defining scope, domain boundaries, roles, key concepts, principles, and associated workflows
- A set of operational annexes providing concrete tools for implementation (e.g., application procedures, competence assessment, audits, training, reporting, and ongoing surveillance)

The objective is to enable:

- Harmonized practices across Member States
- Transparent and traceable evaluation processes
- Increased confidence in the assessment of AI systems

In addition, the toolkit may support NCAs in developing internal policies and workflows related to staff training, laboratory evaluation procedures, and auditing practices.

## TITLE TERMINOLOGY NOTE

The title of this deliverable follows the wording defined in the Description of Action (DoA) and has therefore been retained unchanged for contractual consistency. However, throughout this document, the terminology has been aligned with the governance framework established by the AI Act. In particular, the procedures addressed in this deliverable concern the qualification, designation, and notification of third-party evaluation laboratories by National Competent Authorities (NCAs), rather than accreditation in its strict legal sense. While accreditation may, in some Member States, constitute supporting evidence or form part of the overall notification process, it remains distinct from the responsibilities assigned to notifying authorities under the AI Act. Accordingly, unless explicitly stated otherwise, references in this document should be understood as relating to the qualification, designation, and notification process of third-party evaluation laboratories, rather than to a formal accreditation process.

## GLOSSARY AND ACRONYMS

The list of terms, group of words, expressions used in this document are explained in Table 1 below

| Term, expression                   | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Accreditation                      | 'Accreditation' is the formal attestation issued by a National Accreditation Body (NAB), usually based on ISO/IEC 17025 or ISO/IEC 17065 for conformity assessment body, confirming that a conformity assessment body is technically competent, impartial, and capable of performing specified conformity assessment activities. Under Article 29 of the AI Act, an accreditation certificate is the preferred evidence demonstrating that the conformity assessment body fulfils the requirements of Article 31. |
| Conformity Assessment Body (CAB)   | 'Conformity assessment body' means a body that performs third-party conformity assessment activities, including testing, certification and inspection.                                                                                                                                                                                                                                                                                                                                                            |
| Designation                        | 'Designation' is the national administrative decision by which the Member State's NCA recognises a conformity assessment body as eligible to perform the conformity assessment activities defined within a specified scope under the AI Act. The designation follows the assessment of the body's competence and compliance with Article 31 requirements and precedes its formal notification to the European Commission.                                                                                         |
| National Accreditation Body (NAB)  | 'National Accreditation Body' is a National authority responsible for accrediting conformity assessment bodies by verifying their technical competence, impartiality, and compliance with accreditation requirements.                                                                                                                                                                                                                                                                                             |
| National Competent Authority (NCA) | 'National Competent Authority' means a notifying authority or a market surveillance authority; as regards AI systems put into service or used by Union institutions, agencies, offices and bodies, references to national competent authorities or market surveillance authorities.                                                                                                                                                                                                                               |
| Notification                       | 'Notification' is the formal communication by the Member State's NCA to the European Commission and the other Member States that a designated conformity assessment body is authorised to act as a notified body under the AI Act. The notification is submitted through the Commission's notification system (NANDO) and becomes effective after the objection period specified in Article 30, allowing the body to carry out third-party conformity assessments within its notified scope.                      |
| Notifying Authorities              | 'Notifying authority' means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.                                                                                                                                                                                                                                                                                |
| Notified body                      | 'Notified body' means a conformity assessment body notified in accordance with the AI Act and other relevant Union harmonisation legislation.                                                                                                                                                                                                                                                                                                                                                                     |

Table 1: *Glossary*

The list of acronyms used in this document and their meaning is explained in Table 2 below

| Acronym | Meaning                       |
|---------|-------------------------------|
| AI      | Artificial Intelligence       |
| CABs    | Conformity Assessment Bodies  |
| LLMs    | Large Language Models         |
| MSA     | Market Surveillance Authority |
| NAB     | National Accreditation Body   |
| NB      | Notified Body                 |
| NCA     | National Competent Authority  |

Table 2: *Acronyms*

## INTRODUCTION

### 1.1 BACKGROUND AND CONTEXT

Artificial Intelligence (AI) is rapidly transforming sectors of critical societal importance, including healthcare, transportation, financial services, critical infrastructure, and public administration. As AI systems are increasingly deployed in high-stakes environments, the need for rigorous, independent, and trustworthy testing and evaluation of these systems has become a matter of regulatory urgency and public interest.

At the international level, regulatory frameworks governing AI, including the *European Union's Artificial Intelligence Act (EU AI Act)*, *ISO/IEC 42001*, and emerging national AI governance legislation, increasingly require or recommend that AI systems, particularly those classified as high-risk, undergo conformity assessments conducted by qualified third-party entities.

The *European Union's Artificial Intelligence Act (EU AI Act)* is defining these entities as “Conformity Assessment Bodies”, without distinction between those performing actual tests on AI system and other performing “technical documentation assessment”. “Conformity Assessment Bodies” (CAB) means a body that performs third-party conformity assessment activities, including testing, certification and inspection. A CAB can be notified by a National Competent Authority (NCA) to ensure it is eligible to perform the conformity assessment activities defined within a specified scope under the AI Act, if so, the CAB becomes a Notified Body (NB). As explained in the AI Act a Notified Body should perform test by itself only if he is not satisfied with the tests carried out by the provider. Even in this case the NB could delegate the execution of this test to subcontractor, under specific conditions. Therefore, the NB may not require having internally the competences, tooling, and experience to run such tests on AI systems.

Throughout this document, when the terms “Conformity Assessment Body” or “Notified Body” are used, it is understood that they refer specifically to organisations carrying out tests on AI system and not those carrying only technical documentation assessment and delegating the actual testing. Similarly, the use of the terms “laboratories”, “testing laboratories” and “evaluation laboratories” refers to these same entities.

This document has been developed to address the gap between the general principles expressed in international standards, most notably *ISO/IEC 17025* (General requirements for the competence of testing and calibration laboratories), and the specific, nuanced requirements that arise when applying those principles in the context of AI system testing. AI introduces fundamentally new challenges for conformity assessment: models may be opaque, data-dependent, context-sensitive, and subject to emergent behaviors that do not arise in classical software or hardware testing regimes.

This document is not intended to establish a formal accreditation or notification scheme or prescribe a mandatory accreditation or notification process for AI testing laboratories. Rather, it provides guidance, methodologies, practical tools, and supporting elements that may assist National Competent Authorities (NCAs) and other relevant stakeholders in developing, implementing, adapting, or strengthening their own laboratory accreditation, notification and oversight processes within the applicable regulatory framework.

While Article 29(2) of the AI Act identifies an accreditation certificate issued by a National Accreditation Body (NAB) as the preferred evidence supporting an application for notification, the Regulation does not make accreditation mandatory in all circumstances. Where an accreditation certificate exists, it provides objective evidence that the conformity assessment body has a good base to fulfil the requirements of Article 31 and should accompany the notification application. However, Article 29(3) explicitly recognises that a conformity assessment body may instead submit other documentary evidence enabling the notifying authority to verify, recognise, and regularly monitor compliance with the Article 31 requirements. Consequently, the methodologies, templates, and supporting tools proposed in this deliverable are intended to assist National Competent Authorities (NCAs) and National Accreditation Bodies (NABs), irrespective of whether a Member State relies on accreditation, direct assessment by the notifying authority, or a combination of both approaches.

The AI Act distinguishes between accreditation, designation, and notification, while leaving Member States flexibility in the organisation of their national conformity assessment infrastructure. Depending on the national legal framework, the sector concerned, and the applicable conformity assessment procedures or assurance levels, the practical implementation of these activities may differ. In some Member States, the assessment

performed during accreditation may constitute the primary technical evaluation supporting notification, resulting in closely coordinated or partially integrated accreditation and notification processes. Furthermore, where permitted under national legislation and the institutional organisation of the Member State, the National Accreditation Body may also perform the functions of the notifying authority, or the notifying authority may rely extensively on the accreditation assessment when reaching its notification decision. The guidance presented in this deliverable is therefore designed to remain applicable regardless of the specific national governance model adopted for accreditation and notification.

Accordingly, the procedures, templates and recommendations presented in this deliverable should be interpreted as implementation guidance that can be adapted to the institutional arrangements established by each Member State, rather than as a prescriptive accreditation or notification framework.

## 1.2 PURPOSE OF THIS DOCUMENT

This document serves as a reference framework for National Competent Authorities (NCAs) responsible for evaluating, recognizing, and overseeing independent testing laboratories operating in one or more AI application domains.

This document does not define the accreditation and/or notification process of such laboratories but proposes elements to help NCAs to go through or build this process.

This document is structured to be applicable across a broad range of AI application domains, while acknowledging that specific domains (e.g., medical AI, autonomous systems, natural language processing) may require supplementary domain-specific annexes.

### 1.2.1 Regulatory and Standards Alignment

|                                     | Definition                                                                                                                                                                                                                    |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EU AI Act (2024/1689)               | Establishes risk-based classification of AI systems and mandates conformity assessment for high-risk applications (Annex III). Requires notified bodies to demonstrate technical competence in relevant AI application areas. |
| ISO/IEC 17025:2017                  | General requirements for competence, impartiality, and consistent operation of testing and calibration laboratories. Forms the baseline accreditation standard referenced throughout this document.                           |
| ISO/IEC 42001:2023                  | Management system standard for AI, providing requirements and guidance for organizations developing, providing, or using AI-based products and services.                                                                      |
| ISO/IEC TR 24028:2020               | Overview of trustworthiness in artificial intelligence. Provides foundational concepts related to bias, robustness, transparency, and explainability relevant to AI testing.                                                  |
| ISO/IEC 23894:2023                  | Guidance on risk management in AI, informing laboratory risk assessment procedures.                                                                                                                                           |
| CEN/CLC JTC21/WG4 prEN 18229 series | Trustworthiness framework in support of the EU AI Act (candidate harmonized standards); directly defines the characteristics laboratories will test against.                                                                  |

|                                                                 |                                                                                                                        |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>WD EN AI Conformity Assessment Framework v6.0 (20260720)</b> | General Conformity assessment requirements for the EU AI Act. Structures the activities the laboratories will perform. |
| <b>CEN/CLC JTC21/WG5 AI cybersecurity work items</b>            | Establishes technical benchmarks to fulfil Article 15(5) of the EU AI Act.                                             |
| <b>GDPR</b>                                                     | General Data Protection regulation.                                                                                    |

## 1.3 OBJECTIVES

This section articulates the overarching and specific objectives that this framework is designed to achieve

### 1.3.1 Enable NCAs to Develop Evidence-Based Assessment Policies

One purpose of this document is to equip NCAs with the tools and decision-support frameworks they could integrate into their operational notification policies.

Usually such policies address, at minimum: how laboratory competence is assessed and weighted; how training and prior experience in AI testing are evaluated; how audit findings are classified and acted upon; and under what conditions notification may be granted, suspended, or withdrawn.

This document does not provide such policies but shares some elements that could be used to support policies defined by the NCA or help NCA during the development of such policies.

### 1.3.2 Promote Consistency, Predictability, and Fairness in Decisions

Notification decisions must be made based on clear, pre-defined, and consistently applied criteria. These objective targets the reduction of arbitrary variation across NCAs and across assessment cycles, thereby increasing trust among testing laboratories, developers of AI systems, regulators, and the public. Consistency also facilitates benchmarking, mutual recognition, and the development of a shared understanding of what constitutes technical competence in the AI testing domain.

### 1.3.3 Support the Development of NCA Staff Competence

This document can also serve as a training and reference resource for NCA personnel responsible for processing notification applications, conducting laboratory audits, and monitoring compliance. Specific objectives include establishing competency profiles for assessors, defining minimum training requirements for NCA staff in AI testing concepts, and providing structured onboarding pathways for new technical assessors.

### 1.3.4 Facilitate International Harmonization and Mutual Recognition

By aligning the Notification framework with internationally recognized standards this document aims to facilitate mutual recognition arrangements (MRAs) between NCAs in different countries or regions. Harmonized practices reduce duplication of conformity assessment activities, lower costs for testing laboratories operating across borders, and strengthen global trust in AI governance infrastructure.

### 1.3.5 Provide a Foundation for Domain-Specific Extension

Given the heterogeneity of AI application domains and the pace of technological development, this document deliberately maintains a technology-neutral core while providing a structured mechanism for domain-specific elaboration through annexes and supplementary guidance. A secondary objective is therefore to establish a governance model for maintaining, updating, and extending the framework as AI technology and its regulatory environment evolve.

### 1.3.6 Foster a Culture of Continuous Improvement in AI Testing Practice

Notification is not a one-time event but an ongoing relationship between the NCA and the laboratory. This framework aims to incentivize continuous improvement by promoting corrective action, surveillance audits, and periodic reassessment into the notification lifecycle. The document also encourages participation in inter-laboratory comparison programs, proficiency testing schemes, and professional communities of practice relevant to AI testing

## 1.4 SCOPE

This section specifies the types of organizations, activities, AI systems, and domains to which the framework can apply, as well as explicit limitations and exclusions. NCAs could refer to this section when determining whether a particular Notification application falls within the purview of this framework.

### 1.4.1 Targeted Audience

The targeted audience of this document is the following categories of organizations:

- National Competent Authorities developing or revising notification policies, laboratory oversight procedures, or internal training frameworks in the context of AI testing.
- Market Surveillance Authorities (MSAs) are responsible for enforcing the EU AI Act through post-market surveillance activities, investigating suspected non-compliance, commissioning independent testing of AI systems, and cooperating with National Competent Authorities and Notified Bodies to ensure continued compliance with AI systems placed on the market or put into service.
- Independent testing laboratories seeking accreditation and notification to conduct conformity assessments, evaluations, or certifications of AI systems within a defined application domain.
- Notified bodies and conformity assessment bodies (CABs) that include AI testing activities within their scope of designation.
- Research and academic institutions offer third-party AI testing services on a commercial or regulated basis.
- Cross-border or supranational accreditation bodies responsible for coordinating or harmonizing NCA practices across multiple jurisdictions.

### 1.4.2 In-Scope Activities and Applications

This framework applies to the notification of organizations performing testing, evaluation, and conformity assessment activities related to AI systems.

The framework may be applied to conformity assessment bodies that assess AI systems deployed in any application domain, including but not limited to healthcare, finance, education, employment, law enforcement, transportation, critical infrastructure, and public services.

The framework is intended to support notification activities related to the assessment of AI systems against applicable regulatory, technical, and organizational requirements, including those associated with high-risk AI systems.

### 1.4.3 Out-of-Scope Activities and Exclusions

This framework is intended to support NCAs in evaluating the competence and capability of AI testing laboratories. It does not define mandatory accreditation or notification requirements or replace existing accreditation and notification schemes, standards, or regulatory frameworks. In addition, it does not cover the assessment or certification of AI systems themselves, nor does it address the design, development,

deployment, operation, or maintenance of AI systems. Furthermore, it does not provide legal interpretations of applicable regulations or standards, nor does it define the processes for the designation or notification of conformity assessment bodies under specific regulatory frameworks.

## 1.5 DESCRIPTION OF EACH ANNEX

This document will be completed by 7 annexes:

### 1.5.1 Annex A- Lab Application Form

This annex provides a template of an AI Testing Laboratory Application Form that may be used by laboratories applying for notification or recognition within one or more AI application domains. The form is intended to facilitate the collection of information describing the laboratory's organizational structure, requested scope of notification, technical capabilities, personnel competencies, testing methodologies, quality management system, and supporting technical resources.

The information collected through this application may assist National Competent Authorities (NCAs) or other competent assessment bodies in performing an initial evaluation of whether a laboratory possesses the organizational, technical, and operational capabilities necessary to perform AI testing activities within its declared scope. The examples provided are intended for guidance only and should not be interpreted as mandatory requirements or as prescribing a specific application format. National accreditation, notification or recognition schemes may adapt the content of this form to reflect applicable regulatory frameworks, national procedures, and the specific AI application domains under consideration.

### 1.5.2 Annex B- Competence Matrix

The competence of personnel is a key factor in ensuring the quality, reliability, and credibility of AI system testing and evaluation activities. As AI technologies become increasingly complex and subject to regulatory requirements, testing laboratories must ensure that their staff possess the appropriate knowledge, skills, experience, and training to perform their assigned responsibilities effectively.

This document is intended to support National Competent Authorities (NCAs) in assessing whether an AI testing laboratory possesses the personnel competencies necessary to perform its activities effectively and reliably. The competencies described herein provide examples of the knowledge, skills, and experience that may be expected within a laboratory, considering its scope of activities, the AI systems being evaluated, and the applicable regulatory requirements. NCAs may use these competencies as a reference when reviewing a laboratory's capability to conduct AI testing and evaluation activities.

The competencies and knowledge areas presented in this document should not be interpreted as requirements for NCA auditors themselves. However, auditors should have a sufficient understanding of the underlying principles of AI technologies, testing methodologies, quality management, and applicable regulatory frameworks to assess whether a laboratory has access to the necessary expertise and has implemented appropriate processes to maintain and demonstrate personnel competence. Such an assessment contributes to ensuring the quality, reliability, and trustworthiness of AI evaluation activities.

### 1.5.3 Annex C- Technical Capability Inventory

This annex provides guidance on documenting the technical capabilities that may support AI testing activities within laboratories seeking accreditation, notification or recognition in one or more AI application domains. It presents examples of inventories, registers, and logs that laboratories may use to describe their technical resources, testing environments, computing infrastructure, software tools, datasets, benchmark suites, testing methodologies, and personnel competencies.

The information described throughout this annex may assist National Competent Authorities (NCAs) in understanding the technical capabilities available within a laboratory and in evaluating whether those capabilities are appropriate for the laboratory's declared scope of testing. The examples have been developed to be applicable across different AI domains, while recognizing that the technical resources, datasets,

benchmark suites, evaluation platforms, and testing methods used by laboratories may vary depending on the characteristics of the AI systems being assessed.

#### 1.5.4 Annex D- Audit Checklist

This annex provides an example of an audit checklist that may be used by National Competent Authorities (NCAs) or other competent assessment bodies when conducting initial assessments, surveillance activities, or reassessments of AI testing laboratories. The checklist is intended to support a structured and consistent evaluation of a laboratory's organizational, technical, and operational capabilities within its declared scope of accreditation, notification or recognition.

The example checklist covers key areas that may be considered during an assessment, including legal and organizational arrangements, personnel competence, technical resources, testing methods, quality management, information security, confidentiality, and regulatory monitoring. The verification activities presented throughout this annex are intended to assist auditors in identifying objective evidence and documenting assessment findings in a consistent and traceable manner.

The checklist should not be interpreted as mandatory audit criteria or as replacing the procedures established by national accreditation, notification or recognition schemes. NCAs may adapt the checklist to reflect applicable regulatory frameworks, relevant standards, the AI application domain under assessment, and the scope of the laboratory being evaluated.

#### 1.5.5 Annex E- Training Curriculum Template

During the development of this deliverable, it was recognised that the training curriculum dedicated to third-party laboratory notification constitutes one thematic component of the broader CERTAIN capacity-building program coordinated by 28Digital under T8.5. Its integration will strengthen synergies between WP6 and WP8 and support the broader positioning and uptake of the deliverable's results among relevant stakeholders through CERTAIN's Empowering AI capacity-building program.

Our approach to develop the part of the training related to third-party laboratory notification is the following:

- 28 Digital will set up the overall capacity-building structure and specify which parts will be dedicated to 3<sup>rd</sup> party lab notification;
- From D6.2 content, the partners of D6.2 will select which topics must be mentioned in the proposed structure;
- 28 Digital will integrate the proposed material, and make sure the specific modules are correctly aligned with other modules;
- With the support of all partners, 28 Digital will adapt as necessary the overall training to specific target groups

Annex E therefore presents the preliminary scope and outline of the training curriculum related to third-party laboratory notification.

#### 1.5.6 Annex F- Reporting Template

This Annex proposes a standardized reporting template that NCA could use when documenting and communicating the results of an evaluation of an independent testing laboratory. It ensures that assessment outputs are produced in a consistent format.

The template is structured to capture all elements required for a technically credible and legally traceable assessment record.

The completed report can constitute the output of the laboratory evaluation activity. It should be retained by the NCA and can be made available to authorities upon request

### 1.5.7 Annex G- Surveillance & Complaint Handling

This Annex proposes element for the monitoring of notified independent AI testing laboratories. National Competent Authorities could follow it to enhance ongoing oversight of notified laboratories and handling of complaints related to their activities. It supports the continuous monitoring obligations established under the EU AI Act, particularly those relating to notified bodies' continued compliance, operational integrity, and cooperation with notifying and market surveillance authorities.

The Annex covers two closely linked functions. First, surveillance, meaning the periodic and risk-based monitoring of notified laboratories after initial notification, including regular reviews, follow-up audits, review of corrective actions, and reassessment where significant changes occur.

Second, complaint handling, meaning the receipt, registration, investigation, resolution, and documentation of complaints concerning a laboratory's competence, impartiality, performance, or compliance with notification conditions.

In line with the AI Act, the Annex ensures that notified laboratories remain competent, independent, and capable of carrying out conformity assessment activities throughout the validity of their notification. It also provides a structured mechanism for NCAs to respond to where concerns are raised by providers, users, public authorities, or other stakeholders. The annex defines minimum expectations for complaint intake, confidentiality, impartial investigation, escalation of serious findings, corrective action tracking, and reporting to the relevant authority where necessary.

## 2. CONCLUSIONS

This deliverable presents a practical framework intended to support National Competent Authorities (NCAs) in the evaluation, notification, and ongoing oversight of independent AI testing laboratories. Rather than defining a mandatory accreditation and/or notification scheme, it provides a structured collection of guidance, methodologies, templates, and supporting tools that may assist NCAs in developing or strengthening notification processes appropriate to their national regulatory context.

The proposed framework addresses key aspects of laboratory notification, including application procedures, personnel competence, technical capabilities, auditing activities, reporting, training, and post-notification surveillance. Together, these elements provide examples of how notification activities may be organized in a consistent, transparent, and traceable manner while remaining sufficiently flexible to accommodate different organizational structures, AI application domains, and national practices.

Given the diversity and rapid evolution of AI technologies, the framework has been developed using a technology-neutral approach that can be adapted to a broad range of AI systems and testing environments. The examples presented throughout the document are illustrative and non-exhaustive, enabling NCAs and laboratories to tailor the proposed templates, inventories, registers, and procedures according to their scope of activities, technical capabilities, and applicable regulatory requirements.

The framework has been developed with consideration of the principles established by the EU AI Act and relevant international standards applicable to laboratory competence, AI governance, risk management, and conformity assessment. While it does not replace existing notification process and accreditation schemes or regulatory obligations, it provides a practical reference that may contribute to more consistent assessments of laboratory competence and facilitate the development of harmonized practices across jurisdictions.

As AI technologies, testing methodologies, standards, and regulatory requirements continue to evolve, this framework should also be regarded as a living reference that may be updated and expanded over time. Future revisions may incorporate additional AI application domains, emerging testing methodologies, new benchmark suites, evolving international standards, and lessons learned from practical implementation by NCAs and AI testing laboratories. Such continuous evolution will contribute to maintaining the relevance of the framework and supporting trustworthy, competent, and reliable AI testing within the European regulatory ecosystem.

## A. ANNEX A: LAB APPLICATION FORM

### A.1 PURPOSE OF THIS ANNEX

This Annex provides a template Application Form that an AI testing laboratory may complete when applying for notification or recognition by a National Competent Authority (NCA) within one or more AI application domains. It is intended to support the structured and consistent collection of the information an NCA needs to perform an initial assessment of whether the applicant possesses the organizational, technical, and operational capabilities required to carry out AI testing activities within its declared scope.

The form gathers information on the laboratory's legal identity and organizational structure, the requested scope of notification, its technical capabilities and resources, personnel competences, testing and validation methods, quality management arrangements, and the measures ensuring traceability and reproducibility of results. Collected together, these elements give the NCA an evidence base for the eligibility, competence, and impartiality checks described in the main document and in the other annexes of this toolkit.

The form is designed to be read alongside the requirements applicable to conformity assessment bodies under Regulation (EU) 2024/1689 (the AI Act), in particular the requirements relating to notified bodies (Article 31) and their operational obligations (Article 33), as well as the general principles for the competence of testing laboratories expressed in ISO/IEC 17025 and the AI management-system requirements of ISO/IEC 42001. The information requested also supports later verification against the Audit Checklist (Annex D) and the ongoing oversight activities described in the Surveillance and Complaint Handling annex (Annex G).

The examples and fields provided in this Annex are intended for guidance only and should not be interpreted as mandatory requirements or as prescribing a single application format. National accreditation, notification or recognition schemes may adapt, extend, or reduce the content of this form to reflect the applicable regulatory framework, national procedures, and the specific AI application domains under consideration. Where a field is not relevant to the applicant's requested scope, the laboratory should indicate this rather than leaving the field blank.

The applicant laboratory should complete every applicable section of this form and provide, in the Supporting Documentation section, the evidence that substantiates the declarations made. Entries should be specific to the requested scope of notification: general corporate material that does not evidence AI testing capability should not be substituted for the information requested here. Each supporting document should be uniquely identified (title, version or date, and issuing function) so that it can be traced during assessment. The application is considered complete only when the Declaration in the final section has been signed by an authorized representative of the laboratory.

Describe the testing and validation methods the laboratory applies within the requested scope, and how it establishes that those methods are fit for purpose. For each activity in the table below, the laboratory should summarize the method used, the standards or references it is based on, and the evidence that the method has been validated for the AI systems concerned. Where a method is not applicable to the requested scope, this should be stated.

A.2 GENERAL INFORMATION

A.2.1 Applicant information

|                              |  |
|------------------------------|--|
| Legal Name of the Laboratory |  |
| Legal Status                 |  |
| Registration Number          |  |
| Registered Address           |  |
| Website                      |  |
| Date of Application          |  |

A.2.2 Contact Information

|                        |  |
|------------------------|--|
| Primary Contact Person |  |
| Position               |  |
| Telephone              |  |
| Email Address          |  |

A.2.3 Laboratory Management

|                                    |  |
|------------------------------------|--|
| Laboratory Director                |  |
| Technical Manager                  |  |
| Quality Manager                    |  |
| AI Testing Manager (if Applicable) |  |

### A.3 REQUESTED SCOPE OF NOTIFICATION

Describe the scope for which notification or recognition is requested. The requested scope defines the boundary of the assessment and of any notification subsequently granted, and should therefore be expressed as precisely as possible. For each entry in the table below, the laboratory should indicate:

- The AI application domain(s) concerned (for example healthcare, finance, employment, biometric identification, critical infrastructure), including whether any domain falls within the high-risk categories of the AI Act.
- The types of AI systems to be evaluated (for example supervised classification or scoring models, recommendation systems, computer-vision systems, natural-language or generative systems), together with any technological limitations of the requested scope.
- The testing and evaluation activities requested (for example performance and accuracy testing, robustness and adversarial testing, bias and fairness evaluation, explainability assessment, cybersecurity testing, documentation and quality-management review).
- The standards, regulatory frameworks, and technical specifications against which the laboratory intends to test (for example the AI Act, ISO/IEC 42001, ISO/IEC 17025, sector-specific requirements).

|                                               |  |
|-----------------------------------------------|--|
| AI Application Domain(s)                      |  |
| Types of AI Systems Evaluated                 |  |
| Requested Testing Activities                  |  |
| Applicable Standards/ Regulatory Requirements |  |

### A.4 LABORATORY DESCRIPTION

Provide a description of the laboratory that allows the NCA to understand its identity, purpose, and organizational context. The description should include, as a minimum:

- The mission and main activities of the laboratory, and the position of AI testing within those activities.
- The areas of technical expertise relevant to the requested scope, and the length of the laboratory's experience in AI testing and evaluation.
- The organizational structure, including reporting lines and the arrangements that safeguard the independence and impartiality of testing activities from any commercial, financial, or other pressure that could influence results.

Any parent organization, ownership relationships, or affiliations that may be relevant to the assessment of independence and potential conflicts of interest.

|                     |  |
|---------------------|--|
| Mission             |  |
| Areas of Expertise  |  |
| Years of Experience |  |

|                          |  |
|--------------------------|--|
| Main Testing Activities  |  |
| Organizational Structure |  |

## A.5 PERSONNEL AND COMPETENCE

Describe the personnel involved in AI testing and evaluation activities within the requested scope and demonstrate that the laboratory has access to sufficient and suitably qualified staff to perform those activities reliably. The information provided should allow the NCA to assess collective competence against the requested scope rather than the credentials of any single individual.

For each technical area within the requested scope, the laboratory should identify:

- The number of personnel available and their roles (for example technical assessors, data scientists, domain experts, quality personnel).
- Relevant academic qualifications, professional certifications, and AI-specific training, together with the arrangements for maintaining and updating competence over time.
- The years and nature of relevant experience in AI testing, evaluation, or the applicable AI application domain.

The specific areas of competence covered (for example machine-learning methods, data governance, robustness and security testing, applicable regulatory requirements), and how the laboratory identifies and addresses any competence gaps.

|                             |         |         |     |     |         |
|-----------------------------|---------|---------|-----|-----|---------|
| Number of Personnel         |         |         |     |     |         |
| Name of Personnel           | Pers #1 | Pers #2 | ... | ... | Pers #X |
| Qualifications              |         |         |     |     |         |
| Professional Certifications |         |         |     |     |         |
| AI-related Trainings        |         |         |     |     |         |
| Years of Experience         |         |         |     |     |         |
| Areas of Competence         |         |         |     |     |         |

## A.6 TECHNICAL RESOURCES

Describe the technical resources available to support AI testing activities within the requested scope. The information provided should demonstrate that the laboratory controls, or has reliable access to, the infrastructure, tools, datasets, and environments necessary to perform the requested testing activities and to reproduce their results. For each resource the laboratory should indicate its purpose, its validation status, and how it is maintained and version-controlled. Resources to be described include the computing and storage infrastructure, the AI testing platforms and software tools, the datasets and benchmark suites used for evaluation, and the isolated or controlled environments in which sensitive testing is performed.

|                          |         |         |                   |                     |
|--------------------------|---------|---------|-------------------|---------------------|
| Computing Infrastructure |         |         |                   |                     |
| AI Testing Platforms     |         |         |                   |                     |
| Name                     | Version | Purpose | Validation Status | Maintenance Process |
|                          |         |         |                   |                     |

A.7 TESTING METHODS AND VALIDATION

|                                                      |                              |
|------------------------------------------------------|------------------------------|
|                                                      | Describe what is implemented |
| Performance evaluation                               |                              |
| Accuracy testing                                     |                              |
| Robustness testing                                   |                              |
| Stress testing                                       |                              |
| Explainability evaluation                            |                              |
| Cybersecurity testing                                |                              |
| Validation methodology                               |                              |
| [Additional line for additional methods if required] |                              |

A.8 QUALITY MANAGEMENT SYSTEM

Describe if the lab is accredited.

|                           |  |  |  |
|---------------------------|--|--|--|
| Date of the Accreditation |  |  |  |
| Standard of Reference     |  |  |  |

Describe the quality management system supporting testing activities.

|                          | Describe what is implemented |
|--------------------------|------------------------------|
| Document control         |                              |
| Configuration management |                              |
| Version control          |                              |
| Software validation      |                              |
| Dataset governance       |                              |
| Benchmark management     |                              |
| Internal audits          |                              |
| Corrective actions       |                              |
| Risk management          |                              |

## A.9 TRACEABILITY AND REPRODUCIBILITY

Describe how the laboratory ensures that testing activities are reproducible.

|                                         | Describe what is implemented |
|-----------------------------------------|------------------------------|
| Software version control                |                              |
| Dataset versioning                      |                              |
| Benchmark versioning                    |                              |
| Infrastructure configuration management |                              |
| Audit logs                              |                              |
| Test report traceability                |                              |

Validation records

## A.10 SUPPORTING DOCUMENTATION

The laboratory should identify the documents accompanying the application.

| Documentation supporting application |         |         |
|--------------------------------------|---------|---------|
| Name                                 | Version | Purpose |
|                                      |         |         |
|                                      |         |         |
|                                      |         |         |

## A.11 DECLARATION

The undersigned certifies that the information contained in this application and the accompanying documentation is complete and accurate.

By signing below, the authorized representative confirms that the laboratory understands the obligations associated with notification, including the duty to inform the NCA without undue delay of any material change affecting the information provided in this application, and consents to the assessment and surveillance activities described in the accompanying toolkit.

|                                          |  |
|------------------------------------------|--|
| <b>Laboratory Name</b>                   |  |
| <b>Name of Authorized Representative</b> |  |
| <b>Position</b>                          |  |
| <b>Signature</b>                         |  |
| <b>Date</b>                              |  |

## B. ANNEX B: COMPETENCE OF PERSONNEL

### B.1 INTRODUCTION

The competence of personnel is a key factor in ensuring the quality, reliability, and credibility of AI system testing and evaluation activities. As AI technologies become increasingly complex and subject to regulatory requirements, testing laboratories must ensure that their staff possess the appropriate knowledge, skills, experience, and training to perform their assigned responsibilities effectively.

This document is intended to support National Competent Authorities (NCAs) in assessing whether an AI testing laboratory possesses the personnel competencies necessary to perform its activities effectively and reliably. The competencies described herein provide examples of the knowledge, skills, and experience that may be expected within a laboratory, considering its scope of activities, the AI systems being evaluated, and the applicable regulatory requirements. NCAs may use these competencies as a reference when reviewing a laboratory's capability to conduct AI testing and evaluation activities.

The competencies and knowledge areas presented in this document should not be interpreted as requirements for NCA auditors themselves. However, auditors should have a sufficient understanding of the underlying principles of AI technologies, testing methodologies, quality management, and applicable regulatory frameworks to assess whether a laboratory has access to the necessary expertise and has implemented appropriate processes to maintain and demonstrate personnel competence. Such an assessment contributes to ensuring the quality, reliability, and trustworthiness of AI evaluation activities.

### B.2 METROLOGY AND DATA INTEGRITY

Personnel involved in AI testing activities shall possess the knowledge and skills necessary to ensure the quality, reliability, traceability, and integrity of all data and test materials used throughout the evaluation process. Given the critical role of data in the performance and compliance of AI systems, testing personnel could be competent in the following areas:

#### B.2.1 Integrity of Test Data

Testing personnel shall understand and apply methods to ensure the accuracy, completeness, consistency, and reliability of test data throughout the testing lifecycle. Competencies could include:

- Identification and prevention of data corruption, unauthorized modification, or accidental loss.
- Verification of dataset integrity.
- Assessment of data quality attributes, including completeness, consistency, relevance, accuracy.
- Detection and reporting of anomalies, outliers, missing values, and potential sources of bias.
- Application of procedures to ensure that test results remain reproducible and verifiable.

Personnel should understand how deficiencies in test data quality may affect the validity of AI system performance, robustness, safety, and compliance assessments.

#### B.2.2 Statistical Sampling and Dataset Construction

Testing personnel shall be capable of designing and constructing test datasets that are representative of the intended operational environment of the AI system, to construct test datasets, representative of real-world conditions, using statistically valid methods. Competencies could include:

- Application of statistically sound sampling methodologies.
- Understanding of sampling bias and methods for its detection and mitigation.
- Determination of appropriate sample sizes to achieve statistically meaningful results.

- Construction of datasets covering normal, boundary, rare, and adverse operating conditions.
- Assessment of demographic, geographic, environmental, or operational representativeness where relevant.
- Understanding of confidence intervals, uncertainty estimation, and statistical significance.

Personnel are expected to be able to justify the adequacy and representativeness of test datasets and explain any limitations that may affect the interpretation of testing outcomes.

### B.2.3 Traceability of Data Provenance

Testing personnel are expected to be able to establish and maintain complete traceability of all datasets used during testing activities. Documenting the entire "chain of custody" for data, knowing exactly where a dataset came from and what modifications have been applied to each data-sample during the test. Competencies could include:

- Documentation of data sources, acquisition methods, and ownership information.
- Recording of all data preprocessing, transformation, annotation, filtering, augmentation, or cleaning activities.
- Maintenance of dataset version histories and change records.
- Verification that datasets used during testing correspond to the intended version and configuration.
- Preservation of records is sufficient to reproduce testing activities and outcomes.
- Understanding of data governance principles and their relevance to AI system evaluation.

The objective is to ensure that every dataset and individual data sample used during testing can be linked to its origin and that all modifications can be reconstructed and audited.

### B.2.4 Traceability of Test Materials

Testing personnel are expected to ensure that all materials provided by technology providers, developers, deployers, or clients remain identifiable and traceable at any step of the testing process. Competencies could include:

- Unique identification and registration of all received test materials.
- Maintenance of chain-of-custody records documenting receipt, storage, handling, transfer, modification, and disposal.
- Configuration management of software, models, datasets, documentation, and associated artifacts.
- Verification that tested versions correspond to those identified in contractual, regulatory, or technical documentation.
- Preservation of evidence supporting test reproducibility and auditability.
- Application of secure storage and access-control procedures to protect test materials against unauthorized modification.

Personnel may benefit from understanding that effective traceability supports transparency, reproducibility, regulatory compliance, and the investigation of incidents, non-conformities, or disputed test results.

### B.2.5 Data Governance and Regulatory Awareness

Testing personnel are expected to possess a working knowledge of the data governance principles established under the AI Act, including:

- Requirements related to data quality and data governance for high-risk AI systems.
- Identification of potential biases that may affect testing outcomes.
- Documentation requirements supporting conformity assessment activities.
- Record-keeping obligations necessary to demonstrate the validity and reliability of testing activities.

- Understanding of how data-related deficiencies may affect compliance conclusions.

This competence enables testing personnel to evaluate not only the technical performance of AI systems but also the adequacy of the evidence supporting regulatory compliance.

## B.3 COMPETENCE IN PROBABILITY AND STATISTICS

Personnel involved in the testing and evaluation of AI systems are expected to possess sufficient knowledge of probability theory, statistics, machine learning performance evaluation, and experimental design to assess AI systems objectively and scientifically. These competencies support the reliable interpretation of test results and enable laboratories to provide evidence-based conclusions regarding system performance, robustness, and compliance.

### B.3.1 Foundational Knowledge of AI Algorithms and Statistical Learning

Testing personnel are expected to possess a sound understanding of the principles underlying AI and machine learning systems, including deep networks, LLMs, parametric and non-parametric classifiers, the statistical concepts that govern model development and performance. Competencies could include:

- Understanding of supervised, unsupervised, semi-supervised, and reinforcement learning approaches.
- Knowledge of parametric and non-parametric models and their respective assumptions and limitations.
- Understanding of deep neural networks, transformers, large language models (LLMs), ensemble methods, decision trees, support vector machines, and probabilistic models.
- Awareness of overfitting, underfitting, model generalization, and bias-variance trade-offs
- Understanding of training, validation, and testing methodologies.
- Knowledge of domain-specific AI technologies and the performance characteristics relevant to the sector under evaluation.
- Ability to interpret model outputs, confidence scores, probability estimates, and prediction distributions.

Personnel should be familiar with how algorithmic design choices influence system behaviour, performance, reliability, and testing requirements.

### B.3.2 Selection and Interpretation of Performance Metrics

Testing personnel are expected to possess the competence necessary to assess, interpret, and evaluate the performance evidence used to demonstrate compliance of an AI system with the requirements of the AI Act. Personnel are expected to be capable of determining whether the testing methodologies, validation procedures, performance indicators, and supporting evidence provided by the developer are appropriate for the intended purpose of the AI system and its reasonably foreseeable conditions of use.

Competencies could include:

- Understanding of classification metrics such as accuracy, precision, recall, specificity, sensitivity, F1-score, balanced accuracy, and confusion matrices.
- Interpretation of Receiver Operating Characteristic (ROC) curves, Area Under the Curve (AUC), Precision-Recall curves, and calibration plots.
- Understanding of regression metrics such as Mean Absolute Error (MAE), Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Mean Absolute Percentage Error (MAPE), etc....
- Evaluation of ranking, recommendation, forecasting, anomaly detection, and generative AI metrics where applicable.
- Understanding of aggregate performance measures across multiple datasets, scenarios, or demographic groups.
- Ability to identify situations in which commonly used metrics may be misleading or insufficient.
- Knowledge of fairness and subgroup-performance metrics were required by the testing scope.

- Ability to identify gaps, limitations, inconsistencies, or unsupported claims in performance documentation and testing reports.

Personnel are expected to be capable of determining whether the reported performance characteristics provide a sufficiently accurate and representative description of the AI system's behaviour under its intended conditions of use and reasonably foreseeable misuse.

### B.3.3 Uncertainty Estimation and Repeatability of Results

Testing personnel are expected to possess the competence to assess the reliability, stability, and reproducibility of performance evidence provided for the purposes of demonstrating compliance with the AI Act. This includes the ability to evaluate whether testing and validation procedures produce consistent and trustworthy results under conditions representative of the intended purpose and reasonably foreseeable use of the AI system.

Competencies could include:

- Understanding statistical uncertainty and measurement variability.
- Calculation and interpretation of confidence intervals and confidence bounds.
- Estimation of uncertainty arising from limited sample sizes.
- Application of hypothesis testing and statistical significance analysis where appropriate.
- Use of resampling techniques such as cross-validation, bootstrapping, and Monte Carlo methods.
- Assessment of variability caused by stochastic model behaviour, random initialization, or probabilistic outputs.
- Determination of whether observed performance differences are statistically meaningful.
- Design of experiments that support reproducibility and repeatability of results.

Personnel are expected to be capable of determining whether the performance evidence presented in technical documentation provides a reliable and reproducible basis for demonstrating compliance with requirements relating to accuracy, robustness, and risk management under the AI Act.

### B.3.4 Experimental Design and Statistical Validity

Testing personnel are expected to possess the competence to design, evaluate, and critically assess testing and validation procedures used to demonstrate compliance of AI systems with the requirements of the AI Act. Personnel should be capable of determining whether the testing approach provides sufficient and appropriate evidence regarding system performance, robustness, and compliance under the intended purpose and reasonably foreseeable conditions of use.

Competencies could include:

- Ability to assess whether testing procedures are appropriate for identifying risks, limitations, and failure modes of the AI system in accordance with its intended purpose.
- Understanding of how training, validation, and testing data selection may affect the representativeness and reliability of performance evidence.
- Ability to evaluate whether datasets used in testing are sufficiently representative of the conditions under which the AI system is intended to operate.
- Understanding of how bias in data or testing conditions may affect the reliability and fairness of performance outcomes.
- Ability to assess whether testing scenarios adequately reflect expected operational environments, including edge cases and reasonably foreseeable misuse.
- Capability to evaluate whether robustness and resilience have been adequately tested in relation to system limitations and risk exposure.
- Ability to review and assess whether assumptions, limitations, and methodological choices in testing are properly documented in technical documentation.

- Ability to determine whether the evidence provided by testing and validation procedures is sufficient to support compliance claims under applicable requirements.

Personnel should be capable of assessing whether the overall testing methodology and supporting evidence are sufficient to demonstrate compliance with requirements relating to risk management, data governance, accuracy, and robustness under the AI Act.

## B.4 AI-SPECIFIC TESTING METHODOLOGIES

Personnel involved in AI testing and evaluation are expected to possess specialized competencies that enable them to assess AI systems beyond conventional software testing approaches. These competencies include the evaluation of fairness, robustness, explainability, and system behaviour under challenging or unexpected conditions. Personnel are expected to be capable of designing, executing, and interpreting tests that provide meaningful evidence regarding the trustworthiness, reliability, and limitations of AI systems.

### B.4.1 Bias and Fairness Testing

Testing personnel are expected to be capable of assessing whether an AI system exhibits systematic performance differences or discriminatory outcomes affecting specific individuals or groups. Competencies could include:

- Understanding of the concepts of bias, discrimination, representativeness, and data quality in the context of AI systems.
- Ability to assess whether training, validation, and testing datasets are sufficiently representative of the persons, groups, or environments relevant to the intended purpose of the AI system.
- Understanding of potential sources of bias and error throughout the AI system lifecycle, including data collection, annotation, preprocessing, development, deployment, and use.
- Ability to evaluate whether performance evidence demonstrates appropriate operation across relevant operational conditions, user groups, or use scenarios.
- Understanding of how deficiencies in data quality or representativeness may affect system performance, accuracy, reliability, and fundamental rights.
- Ability to assess whether limitations, assumptions, and identified risks relating to bias and representativeness are adequately documented within the technical documentation.
- Capability to identify situations where additional assessment or testing may be required to evaluate risks of discrimination, unequal treatment, or adverse impacts on affected persons.

Personnel are expected to be capable of determining whether the provider has adequately identified, documented, assessed, and mitigated risks arising from bias, data quality deficiencies, or lack of representativeness in accordance with the requirements of the AI Act.

### B.4.2 Adversarial and Robustness Testing

Testing personnel are expected to possess the competence necessary to evaluate the robustness, resilience, and reliability of AI systems under conditions relevant to their intended purpose and reasonably foreseeable use. Personnel are expected to be capable of assessing whether the AI system can maintain its performance and operate safely when exposed to errors, faults, unexpected conditions, data quality issues, or other factors that may affect its operation.

Competencies could include:

- Understanding of factors that may affect the robustness, reliability, and resilience of AI systems throughout their lifecycle.

- Ability to assess whether testing procedures adequately evaluate system performance under expected operational conditions and reasonably foreseeable adverse conditions.
- Understanding of how data quality deficiencies, operational variations, environmental conditions, or system faults may influence AI system behaviour.
- Ability to evaluate whether the AI system continues to operate within acceptable performance limits when exposed to unexpected, incomplete, inaccurate, or degraded inputs.
- Understanding of potential failure modes, system limitations, and conditions that may lead to performance degradation or unreliable outputs.
- Ability to assess whether identified vulnerabilities and risks have been appropriately addressed through technical or organizational mitigation measures.
- Capability to evaluate the adequacy of robustness and resilience evidence contained in technical documentation and testing reports.
- Ability to assess whether limitations, vulnerabilities, residual risks, and mitigation measures are properly documented and communicated.
- Optimization-based attack generation. Gradient-based (white-box) adversarial example generation, and critically zero-order (gradient-free) optimization for black-box settings the realistic threat model for most evaluated systems. Neither first-order nor zero-order optimization is mentioned anywhere in the competence framework.
- Topology and manifold theory. Robustness also involves measuring key mathematical properties related to the output set, sensitivity of a neural network plus understanding what makes the domain of application of the AI system its domain and this, beyond distribution. Therefore, it seems important that a notified laboratory will be able to challenge these properties, beyond than running disturbed input images a priori following a matching distribution with a relevant test set.

Personnel are expected to be capable of determining whether the AI system maintains an appropriate level of accuracy, robustness, and reliability under its intended conditions of use and whether identified limitations or vulnerabilities may affect compliance with the requirements of the AI Act.

### B.4.3 Explainability and Failure Analysis

Testing personnel are expected to be capable of investigating and explaining the causes of AI system failures, unexpected outputs, or non-conformities identified during testing activities. Competencies may include:

- Understanding explainability and interpretability concepts applicable to different AI technologies.
- Ability to distinguish between failures caused by data quality issues, model limitations, implementation defects, environmental factors, or testing artefacts.
- Use of appropriate analysis techniques to investigate model behaviour and decision-making processes.
- Interpretation of feature importance measures, saliency maps, attention mechanisms, local explanations, and other explainability techniques where applicable.
- Evaluation of whether system outputs are consistent with documented system behaviour and intended functionality.
- Identification of recurring failure patterns and underlying root causes.
- Documentation of findings in a manner that supports reproducibility, transparency, and corrective action.

Personnel are expected to be able to provide technically sound and evidence-based explanations that support the interpretation of test results and facilitate communication with developers, conformity assessment bodies, auditors, and other stakeholders.

### B.4.4 Human Oversight and Trustworthiness Assessment

Testing personnel are expected to possess the competence necessary to assess whether an AI system supports effective human oversight and enables users to understand, monitor, and appropriately respond to the system's outputs in accordance with its intended purpose and risk profile.

Competencies may include:

- Understanding of the human oversight requirements applicable to AI systems under the AI Act.
- Ability to assess whether users are provided with sufficient information to understand the capabilities, limitations, and expected performance of the AI system.
- Ability to evaluate whether human operators can effectively monitor system operation, identify anomalies, detect errors, and recognize unexpected behaviour.
- Understanding of the risks associated with automation bias and the potential for inappropriate reliance on AI-generated outputs.
- Ability to assess whether the AI system enables human operators to appropriately interpret outputs and exercise effective judgement when using the system.
- Capability to evaluate whether users can intervene in, override, disregard, reverse, or stop the operation of the AI system when necessary and appropriate.
- Ability to assess whether safeguards against foreseeable misuse and inappropriate use are adequately implemented and communicated.
- Capability to evaluate whether limitations, residual risks, and conditions affecting system performance are adequately documented and communicated to users.
- Ability to assess whether human oversight measures remain appropriate in relation to the intended purpose, operational environment, and level of risk associated with the AI system.

Personnel are expected to be capable of determining whether the AI system supports meaningful and effective human oversight and whether users can exercise appropriate control over the system in accordance with the requirements of the AI Act.

## B.5 TECHNICAL COMPETENCIES

Personnel involved in the development, testing, validation, operation, or oversight of Artificial Intelligence (AI) systems are expected to possess appropriate technical competencies proportionate to their roles and responsibilities, in accordance with the risk-based approach and AI literacy obligations established by the EU AI Act.

### B.5.1 Programming

Personnel are expected to demonstrate familiarity with programming languages and computational tools commonly used in AI-related activities, particularly where staff are responsible for testing, evaluating, validating, or supervising AI systems.

Competencies may include:

- Basic to advanced proficiency in programming languages commonly used in AI domains, such as Python, including familiarity with libraries and frameworks relevant to AI testing, data analysis, and automation (e.g., data processing, scripting, model execution, or result verification).
- Understanding of software logic, algorithmic workflows, and reproducibility principles to enable personnel to interpret AI system behaviour and outputs.
- Ability to read, understand, and where applicable execute or review scripts used in testing environments.
- Knowledge of secure coding and software integrity principles to reduce risks related to unintended system behaviour or vulnerabilities.
- Familiarity with automation practices for test execution and repeatability of validation activities.

The level of programming competence is expected to be proportionate to the staff's role. For example, personnel involved in AI testing and technical evaluation may require higher proficiency than administrative or oversight functions.

### B.5.2 Software Validation

Personnel are expected to possess competencies necessary to verify and ensure that software used in testing, validation, or conformity assessment activities performs as intended and produces reliable, reproducible, and accurate results.

Competencies may include:

- Understanding of software verification and validation (V&V) principles to confirm that software performs according to specified requirements.
- Ability to verify the correct functioning, integrity, and configuration of tools used during AI testing and evaluation activities.
- Competence in identifying software anomalies, malfunctions, incorrect outputs, or inconsistencies that may impact testing validity.
- Familiarity with validation methodologies, including:
  - Functional testing
  - Regression testing
  - Reproducibility checks
  - Robustness testing
  - Performance verification
- Ability to document validation evidence, maintain audit trails, and ensure traceability of software versions used during testing activities.
- Understanding of risks associated with inaccurate testing environments and the impact of software errors on conformity assessment outcomes.

### B.5.3 Managing Computing Environments

Personnel are expected to demonstrate familiarity with computing environments required to develop, test, validate, or maintain AI systems in a controlled and reproducible manner.

Competencies may include:

- Familiarity with common operating systems used in technical environments (e.g., Linux, Windows, macOS) and the ability to configure and maintain stable testing environments.
- Knowledge of virtualized and containerized environments, including tools such as Docker, to ensure reproducibility, isolation, portability, and consistency of software execution.
- Competence in environment configuration management, including dependency management, package installation, and reproducibility of computational settings.
- Familiarity with software version control systems (e.g., Git) to maintain traceability, transparency, and controlled changes in code and testing artifacts.
- Competencies in documentation versioning, ensuring that technical procedures, test evidence, validation protocols, and records remain controlled, current, and auditable.
- Understanding of access control, environment security, and cybersecurity good practices to preserve system integrity and prevent unauthorized modifications.

### B.5.4 Specific field competences

In addition to technical expertise in AI evaluation, cybersecurity, software testing, and conformity assessment, evaluation laboratories may require domain-specific knowledge depending on the intended purpose and application domain of the AI system under assessment. For example, AI systems deployed in healthcare, finance, transport, critical infrastructure, or other regulated sectors may require personnel with an understanding of the relevant business processes, regulatory context, operational environment, and associated risks in order to correctly interpret the system's intended use, identify credible test scenarios, and assess compliance with applicable requirements. The level of domain expertise should therefore be proportionate to the scope of the laboratory's activities and the categories of AI systems it intends to evaluate.

## B.6 BEHAVIOURAL COMPETENCIES

Personnel involved in the development, testing, validation, evaluation, or oversight of AI systems shall demonstrate behavioural competencies that support integrity, trustworthiness, impartiality, confidentiality, and the reliable execution of laboratory activities. These competencies are essential to maintaining confidence in testing outcomes and ensuring compliance with applicable legal, contractual, and ethical obligations.

### B.6.1 Confidentiality

Personnel involved in testing, validation, conformity assessment, or other laboratory activities are expected to possess the competence necessary to protect confidential information obtained during their activities and to ensure that such information is handled in accordance with applicable legal, regulatory, and organizational requirements.

Competencies may include:

- Understanding of confidentiality obligations applicable to information obtained during testing, validation, conformity assessment, surveillance, or related activities.
- Ability to identify information that may constitute confidential information, commercially sensitive information, proprietary technical information, trade secrets, or protected documentation.
- Understanding of the conditions under which information may be accessed, used, shared, retained, or disclosed.
- Ability to ensure that confidential information is used only for authorized purposes and made available only to authorized people.
- Understanding of organizational procedures established to protect confidentiality, integrity, and availability of information and assessment records.
- Capability to maintain appropriate records and controls supporting the secure handling of information throughout assessment activities.
- Awareness of obligations relating to intellectual property rights, trade secret protection, contractual confidentiality requirements, and applicable data protection legislation.
- Ability to identify, report, and appropriately respond to situations that may compromise the confidentiality or integrity of protected information.

Personnel are expected to be capable of ensuring that information obtained through laboratory activities is handled in a manner that preserves confidentiality, protects legitimate interests of stakeholders, and supports compliance with the requirements of the AI Act.

### B.6.2 Impartiality

Personnel involved in testing, validation, conformity assessment, or other evaluation activities shall possess the competence necessary to perform their responsibilities in an impartial, objective, independent, and professionally responsible manner. Personnel are expected to be capable of ensuring that assessment activities and conclusions are based solely on relevant evidence, established procedures, and applicable requirements.

Competencies may include:

- Understanding of the principles of impartiality, independence, objectivity, and professional integrity applicable to testing and conformity assessment activities.
- Ability to identify actual, potential, or perceived conflicts of interest that may affect the credibility or independence of assessment activities.
- Capability to declare and appropriately manage situations that could compromise impartiality or create undue influence.
- Ability to base technical evaluations, conclusions, and recommendations exclusively on objective evidence, documented findings, and applicable assessment criteria.

- Understanding of organizational safeguards established to preserve independence and prevent conflicts of interest.
- Capability to recognize and appropriately respond to internal or external pressures that could affect the integrity of assessment activities.
- Understanding of ethical responsibilities associated with testing, validation, conformity assessment, and regulatory support activities.
- Ability to maintain professional conduct and independence throughout the assessment process.

### B.6.3 Technical Reporting

Personnel are expected to demonstrate the ability to prepare, review, and maintain technical documentation and test reports that are accurate, complete, traceable, and suitable for regulatory, technical, and audit purposes.

Competencies may include:

- Ability to design, develop, and maintain standardized test-report templates to ensure consistency, completeness, and clarity of reporting.
- Competence in preparing technical reports that accurately reflect testing methodologies, test configurations, assumptions, observations, results, limitations, and conclusions.
- Ability to document findings in a manner that is clear, objective, reproducible, and evidence based.
- Understanding of traceability requirements, including accurate referencing software versions, test environments, datasets, methodologies, and validation evidence.
- Competence in identifying and documenting anomalies, deviations, uncertainties, or non-conformities identified during testing activities.
- Ability to ensure that reports are reviewed, approved, and controlled according to laboratory quality management procedures.

## C. ANNEX C: TECHNICAL CAPABILITY INVENTORY

### C.1 INTRODUCTION

A testing laboratory applying for accreditation, notification or recognition within one or more AI application domains may maintain a Technical Capability Inventory (TCI) as a structured record of the resources, infrastructure, tools, datasets, benchmarks, methods, and competencies available to support its testing activities.

For National Competent Authorities (NCAs), a TCI can provide a useful source of information when evaluating whether a laboratory possesses the technical capabilities necessary to perform assessments within its declared scope. TCI may also assist NCAs in understanding the extent to which a laboratory is able to conduct testing activities in a consistent, reproducible, and technically sound manner.

The examples presented in this annex are illustrative and non-exhaustive. They are not intended to define notification requirements or prescribe specific technical solutions. Laboratories operating in different AI application domains may employ alternative tools, infrastructures, datasets, methodologies, or evaluation approaches that are equally suitable for their intended scope of testing.

The content of a TCI may be relevant when assessing a laboratory's ability to evaluate characteristics of AI systems that are addressed by applicable regulatory or technical frameworks, including data governance, technical documentation, record-keeping, accuracy, robustness, cybersecurity, transparency, and risk management. In the context of the EU AI Act, such capabilities may support the assessment of evidence relating to Articles 10, 11, 12, and 15, as well as relevant conformity assessment activities.

For illustration purposes, several examples throughout this annex are drawn from the domain of biometric systems. These examples should not be interpreted as limiting the applicability of the framework to biometrics. Similar approaches may be applied to other AI application domains, including natural language processing, generative AI, healthcare AI, industrial AI, autonomous systems, computer vision, and decision-support systems.

A Technical Capability Inventory may be maintained using a Laboratory Information Management System (LIMS), an asset management platform, a quality management system, or other documentation mechanisms appropriate to the laboratory's operational environment.

Depending on the laboratory's scope and the expectations of the relevant NCA, a TCI could include one or more of the following components:

1. Testing Scope and Regulatory Mapping Matrix.
2. Equipment, Computing Infrastructure, Platforms, Dataset and Benchmark Inventory.
3. Personnel Competency Register.
4. Environment and Data Constraints Log.
5. Method, Dataset, Benchmark and Software Validation Registry.

The following sections provide examples of how these components may be structured and maintained.

### C.2 TESTING SCOPE AND REGULATORY MAPPING MATRIX

A Testing Scope and Regulatory Mapping Matrix can provide NCAs with a structured overview of the testing activities that a laboratory can perform within its declared scope. The matrix may help identify the relationship between application domains, testing methodologies, evaluation metrics, datasets, benchmarks, technical standards, and supporting infrastructure.

AI testing laboratories often evaluate statistical characteristics, probabilistic outcomes, robustness indicators, performance metrics, and behavioural properties of AI systems. Consequently, the testing scope may be

expressed through a combination of evaluation objectives, technical standards, benchmark suites, datasets, and testing methodologies.

The matrix may assist NCAs in understanding:

- The AI application domains covered by the laboratory.
- The categories of AI systems that can be evaluated.
- The evaluation methodologies, benchmarks, and datasets available to support testing activities.
- The technical standards, specifications, or regulatory requirements considered during testing.
- The computing infrastructure, tools, and platforms available to perform evaluations.
- The personnel authorized to conduct specific testing activities.

Depending on the application domain, a testing scope matrix could include information such as:

1. **Domain of Testing:** The AI application domain in which testing activities are performed. Examples may include biometrics, computer vision, generative AI, natural language processing, healthcare AI, industrial AI, autonomous systems, or decision-support systems.
2. **Target of Evaluation (TOE):** The AI system, model, component, or service being evaluated.
3. **Evaluation Objective:** The characteristics being assessed, such as accuracy, robustness, cybersecurity, fairness, bias, explainability, transparency, reliability, safety, or resilience.
4. **Evaluation Metrics:** Quantitative or qualitative indicators used during testing. Examples may include error rates, robustness scores, fairness metrics, attack success rates, benchmark scores, calibration measures, or explainability indicators.
5. **Testing Methodology, Standards and Benchmarks:** The standards, procedures, benchmark suites, testing frameworks, or evaluation methodologies used to conduct assessments.
6. **Supporting Infrastructure and Tools:** The technical resources used to perform testing activities, including computing infrastructure, AI evaluation platforms, simulation environments, software frameworks, and automation tools.
7. **Datasets and Reference Material:** The datasets, benchmark suites, synthetic data generators, simulation environments, or reference artifacts used to support testing activities.
8. **Authorized Personnel:** Personnel possessing the competencies necessary to perform the corresponding testing activities.

The matrix may also support traceability between testing activities and applicable regulatory or technical requirements. For example, laboratories may choose to map testing activities to provisions relating to data governance, transparency, robustness, cybersecurity, record-keeping, or risk management where relevant to their declared scope.

| Test-ID | Testing Domain (Target of Evaluation) | Principle of Measurement (Metric/Evaluation)                                  | Test Methods & Standards                 | Core Equipment & Compute                                  | Traceability & Reference Datasets           | Authorized Staff                                |
|---------|---------------------------------------|-------------------------------------------------------------------------------|------------------------------------------|-----------------------------------------------------------|---------------------------------------------|-------------------------------------------------|
| Bio-01  | Facial Recognition Systems (FRT)      | Verification (1:1) & Identification (1:N) performance (FMR, FNMR, DET curves) | ISO/IEC 19795-1 / -2; Internal SOP-AI-04 | Local GPU cluster (NVIDIA H100), Python 3.11, PyTorch 2.4 | NIST FRVT baseline sets, synthetic datasets | <names of staff authorized to perform the test> |

|               |                                                         |                                                                                     |                                                   |                                                                  |                                                          |  |
|---------------|---------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------|------------------------------------------------------------------|----------------------------------------------------------|--|
| <b>Bio-02</b> | Presentation Attack Detection (PAD)                     | Liveness verification, Spoof detection (APCER, BPCER, ACER)                         | ISO/IEC 30107-1 / - 3; Internal SOP-AI-09         | Calibrated Lux meter, 4K Display, Silhouette/Silicon masks       | ISO/IEC 30107 compliance artifact database               |  |
| <b>Bio-03</b> | <b>Biometric Data Interchange Formats Change to IDV</b> | <b>Conformance testing of biometric data blocks (e.g., Minutiae, Image records)</b> | <b>ISO/IEC 19794-x (Parts 2, 4, 5); SOP-AI-12</b> | <b>Biometric Syntax Parser v4.2, automated schema validators</b> | <b>ISO/IEC 19794 official electronic test assertions</b> |  |

Table C.3 - Example of Testing Scope Matrix for a hypothetical AI-Biometrics testing lab applying for notification.

## C.3 EQUIPMENT AND REFERENCE DATA LOG

The Equipment and Reference Data Log provide a structured inventory of technical resources that supports AI testing activities. In traditional testing and calibration laboratories, equipment registers are primarily intended to demonstrate that measurement instruments are properly maintained, calibrated, and traceable to recognized standards. In the context of AI testing laboratories, however, the concept of equipment extends beyond physical devices and encompasses a broader ecosystem of software tools, computing infrastructure, datasets, benchmark suites, and digital environments that collectively influence the validity, reproducibility, and reliability of testing outcomes.

This broader interpretation is consistent with the characteristics of AI systems and with the objectives of the AI Act, which emphasizes data governance, technical documentation, record-keeping, accuracy, robustness, and cybersecurity throughout the lifecycle of AI systems.

Articles 10, 11, 12, and 15 highlight the importance of maintaining appropriate documentation regarding datasets, development and validation processes, technical environments, and performance evaluation activities. Consequently, laboratories performing AI assessments may benefit from maintaining records that provide visibility into the resources, tools, datasets, and infrastructures used during testing activities.

Unlike traditional metrological traceability, where measurement results are linked through an unbroken chain of calibrations to physical standards, traceability in AI testing is often achieved through the reproducible management of software, datasets, benchmark suites, and computing environments. Evaluation results may depend not only on the characteristics of the AI system under assessment but also on the specific versions of testing tools, software libraries, operating systems, hardware accelerators, datasets, and benchmark configurations used during the evaluation. As a result, maintaining comprehensive records of these elements can contribute to the transparency, repeatability, and technical credibility of testing activities.

The following five-step process illustrates one possible approach for constructing and maintaining an Equipment and Reference Data Log suitable for AI testing laboratories.

### C.3.1 Define Digital Equipment Types

A useful starting point consists of identifying and categorizing the technical resources that support testing activities. Restricting the inventory to physical servers or workstation hardware may provide only a partial view of the laboratory's capabilities. AI testing environments are frequently composed of multiple layers of software and infrastructure that collectively determine how evaluations are performed.

For example, a laboratory may maintain records of test execution software, including automation frameworks such as DeepEval<sup>1</sup> and Promptfoo<sup>2</sup>, vulnerability assessment tools such as Garak and PyRIT, robustness evaluation frameworks, benchmark execution engines, and other software used to generate or analyze test results. Operating environments may also be documented, including specific versions of operating systems, virtual machines, containers such as Docker, cloud configurations, orchestration platforms, and infrastructure management tools. Additional resources may include support utilities such as compilers, Python runtimes, database engines, dependency managers, synthetic data generators, and automation scripts used to support testing workflows.

Attention may also be given to reference datasets and benchmark suites. In the context of AI evaluations, datasets often play a role comparable to that of reference standards in conventional testing laboratories. Examples may include standardized input datasets, benchmark repositories, ground-truth datasets, baseline files, adversarial testing corpora, and domain-specific evaluation datasets used to assess system performance, robustness, fairness, or cybersecurity characteristics. Maintaining information regarding the provenance, intended use, version history, and known limitations of these datasets may contribute to the assessment of testing validity and support considerations related to data governance under the AI Act.

### C.3.2 Structure the Software Register

Once technical resources have been identified, a centralized register may be maintained to provide visibility into the assets that support testing activities. Such a register can facilitate traceability by linking evaluation results to specific versions of software tools, datasets, benchmark suites, and infrastructure configurations.

Typical records may include the software name, developer or vendor, and exact semantic version number, such as v3.4.2-build.8. Laboratories may also assign internal asset identifiers to facilitate lifecycle management and traceability. Additional information may include deployment locations, such as server identifiers, cloud instance paths, repository locations, or container registries. Integrity information, including SHA-256 hashes and digital signatures, may be recorded to support verification that software artifacts have not been altered. Information concerning software licensing, support agreements, and vendor maintenance periods may also be relevant, particularly when evaluation results depend on commercially supported tools.

### C.3.3 Establish Software “Metrological Traceability”

The concept of metrological traceability can be adapted to software-intensive testing environments by demonstrating that evaluation tools and testing procedures produce consistent and reproducible results under controlled conditions. In AI testing, this often involves maintaining a traceable relationship between evaluation outputs and the software, datasets, benchmarks, and infrastructure configurations used to generate them.

One approach consists of linking testing activities to recognized reference standards, benchmark suites, publicly available datasets, internet protocols, or international specifications. Depending on the evaluation domain, examples may include ISO/IEC standards, benchmark repositories, open datasets, or published evaluation methodologies. Traceability may further be strengthened by documenting source code repository commit hashes, software dependencies, library versions, operating system patch levels, container images, and infrastructure configurations. Such information can help establish an unbroken chain between evaluation results and the technical environment in which those results were produced.

Validation records may also form part of the traceability framework. Commercial tools may be accompanied by vendor validation documentation or compliance certifications, whereas internally developed scripts and

---

<sup>1</sup> <https://deepeval.com/>

<sup>2</sup> Promptfoo: <https://www.promptfoo.dev/>

open-source tools may be supported through internal validation reports, unit testing evidence, benchmark verification exercises, or documented performance assessments conducted using reference datasets.

### C.3.4 Maintenance and Verification

In software-intensive testing environments, maintenance and verification activities serve a function analogous to calibration and maintenance activities performed on physical measurement equipment. The objective is to ensure that testing resources continue to operate as intended and that evaluation results remain reproducible over time.

Verification activities may include the periodic execution of automated test suites against known reference datasets or benchmark corpora to confirm that software continues to produce expected results. Benchmark re-execution, comparison against ground-truth datasets, and validation of metric calculations using reference implementations may also contribute to confidence in testing processes. Software updates, security patches, infrastructure changes, benchmark revisions, and dataset modifications may be documented as maintenance events to preserve traceability between testing outcomes and the resources used to generate them.

Where defects are identified, laboratories may maintain records describing the nature of the issue, the affected testing activities, the potential impact on previously generated results, and the corrective actions implemented. Such records can contribute to transparency and support the investigation of anomalous or disputed testing outcomes.

### C.3.5 Access and Configuration Controls

The reliability of AI testing activities depends not only on the availability of appropriate tools and datasets but also on the ability to preserve the integrity of testing environments over time. Consequently, access control and configuration management mechanisms may play an important role in ensuring that software tools, benchmark suites, datasets, and infrastructure configurations cannot be modified without appropriate authorization.

Access control measures may include role-based permissions, approval workflows, privileged access management mechanisms, and documented responsibilities for approving software changes. Configuration management practices may include the use of version-control systems, Infrastructure-as-Code approaches, immutable container images, automated deployment pipelines, and configuration baselines. These mechanisms can help ensure that testing environments remain consistent with the configurations documented in the register and that evaluation results can be reproduced when required.

From the perspective of NCAs, maintaining such information may provide additional visibility into the technical capabilities, governance practices, and reproducibility mechanisms implemented by a laboratory. Although the specific tools, platforms, datasets, and infrastructures may vary depending on the laboratory's scope of activity, the underlying objective remains the same: to provide a transparent and traceable view of the technical ecosystem used to evaluate AI systems.

## C.4 ENVIRONMENT AND DATA CONSTRAINTS LOG

The Environment and Data Constraints Log provide a structured mechanism for documenting the technical, operational, and data-related conditions that may influence the validity, reproducibility, and reliability of AI testing activities. Unlike conventional testing laboratories, where environmental constraints are primarily associated with physical conditions affecting measurement equipment, AI testing laboratories operate within complex digital ecosystems in which testing outcomes may also depend on computing infrastructure, software environments, datasets, benchmark suites, model configurations, and supporting services.

Maintaining a documented inventory of these constraints can assist National Competent Authorities (NCAs) in understanding the context under which testing activities are performed and in evaluating whether laboratories possess adequate mechanisms to control factors that could influence testing outcomes. Such documentation also supports transparency, reproducibility, and traceability throughout the testing lifecycle.

The AI Act places particular emphasis on data governance, technical documentation, record-keeping, and the demonstration of appropriate levels of accuracy, robustness, and cybersecurity. Consequently, documenting

environmental and data-related constraints may contribute to the evidence supporting assessments performed under Articles 10, 11, 12 and 15 of the AI Act, as well as the technical documentation requirements described in Annex IV.

Similarly, ISO/IEC 17025 recognizes the importance of controlling facilities and environmental conditions that may affect the validity of laboratory activities, while acknowledging that such conditions should be interpreted according to the nature of the testing performed.

The following approach illustrates one possible method for constructing and maintaining an Environment and Data Constraints Log suitable for AI testing laboratories.

#### **C.4.1 Identification of Environmental Constraints**

The first step consists of identifying all environmental conditions that may influence the execution or interpretation of AI testing activities. While traditional laboratories primarily consider physical parameters such as temperature, humidity, vibration, or electromagnetic interference, AI testing laboratories frequently depend upon digital environments whose characteristics may significantly influence evaluation results.

Environmental information may therefore include both physical and digital components.

Physical environmental conditions may remain relevant for laboratories evaluating AI systems interacting with sensors or hardware devices. Examples include temperature and humidity ranges affecting embedded AI systems, ambient lighting conditions used during computer vision evaluations, acoustic characteristics for speech recognition testing, vibration levels for autonomous systems, or power supply stability for hardware-based AI platforms.

Digital environments may have an even greater influence on testing reproducibility. Laboratories may therefore document characteristics such as operating system versions, virtualization platforms, container technologies (e.g., Docker), orchestration platforms (e.g., Kubernetes), cloud deployment configurations, virtual machines, software libraries, hardware drivers, and runtime environments. Computing infrastructure may also be recorded, including CPU architecture, GPU models (e.g., NVIDIA A100 or H100 accelerators), memory configuration, storage architecture, networking characteristics, and cloud service providers where applicable.

Because many AI evaluation frameworks exhibit sensitivity to software dependencies and hardware architectures, documenting these environmental characteristics can significantly improve the reproducibility of testing activities and facilitate independent verification of reported results.

#### **C.4.2 Identification of Data and Benchmark Constraints**

Datasets constitute one of the most critical resources used during AI testing and are explicitly addressed by Article 10 of the AI Act through requirements relating to data governance, quality, representativeness, relevance, and appropriate management practices. Consequently, laboratories may maintain documented information describing any constraints associated with datasets and benchmark suites used during testing.

Data constraints may include limitations concerning dataset availability, licensing conditions, demographic representativeness, class imbalance, annotation quality, geographical coverage, language coverage, temporal validity, known biases, or minimum sample sizes required to obtain statistically meaningful evaluation results. Such constraints should not necessarily be viewed as deficiencies but rather as characteristics that may influence the interpretation of testing outcomes.

Information concerning dataset provenance, acquisition methods, version history, intended purpose, known limitations, and associated governance procedures may further support assessments relating to transparency, traceability, and reproducibility.

Where personal data is processed during testing activities, laboratories should also document the measures implemented to comply with applicable data protection legislation, including the General Data Protection Regulation (GDPR). Such measures may include anonymization or pseudonymization techniques, to log the operational constraints to the system used to strip personally identifiable information (PII) from raw biometric. It can include measures like data retention and purging to specify limits on how long raw biometric data can be retained in the testing environment before secure disposal or archiving.

### C.4.3 Structure of the Environment and Data Constraints Log

The Environment and Data Constraints Log may be maintained as a living document that evolves alongside the laboratory's technical infrastructure and testing capabilities. Rather than serving solely as an inventory, the log may provide contextual information enabling assessors to understand how identified constraints are monitored, controlled, and considered during testing activities.

Each recorded constraint may include a unique identifier together with a description of the affected component, the category of constraint, the potential impact on testing activities, and the measures implemented to control or mitigate associated risks. Categories may include physical environment, computing infrastructure, software dependencies, datasets, benchmark suites, cloud services, cybersecurity considerations, data governance, or hardware limitations.

Descriptions should clearly identify the constraint being documented. Examples may include ambient lighting exceeding acceptable thresholds for computer vision evaluations, insufficient demographic diversity within an evaluation dataset, dependency upon a specific GPU architecture for executing benchmark workloads, restrictions associated with cloud-hosted testing environments, or version incompatibilities between software libraries used during evaluation.

The documentation may further describe how each constraint could influence testing validity, reproducibility, uncertainty, or performance measurements, together with the mechanisms implemented to mitigate these effects. Such mechanisms may include environmental monitoring, benchmark normalization procedures, automated verification scripts, software dependency management, dataset version control, redundancy of computing resources, or configuration management practices.

Finally, the log may identify the verification activities performed to demonstrate that mitigation measures remain effective. Examples include routine execution of benchmark suites using reference datasets, periodic verification of software dependencies, infrastructure integrity checks, validation of dataset integrity using cryptographic hashes, or monitoring of cloud deployment configurations.

### C.4.4 Relying on existing framework

Such AI testing labs will typically be accredited against standard like ISO/IEC 17025. This is likely to be the case for AI testing labs in the EU as well. Therefore, it will be useful to ensure that the testing lab environment aligns to the requirements of this standard (i.e. clause 6.3: Facilities and environmental conditions).

Moreover, demonstrate how the data constraints align with the General Data Protection Regulation (GDPR) and other national regulations, such as the Revised Swiss Data Protection Act (FADP) in Switzerland should be considered.

## C.5 METHOD, SOFTWARE AND TECHNICAL RESOURCE VALIDATION REGISTRY

The Method, Software and Technical Resource Validation Registry provide a structured mechanism for documenting the validation status of the technical resources used to perform AI testing activities. Unlike conventional laboratories, where validation primarily concerns measurement methods and physical instruments, AI testing laboratories rely on an ecosystem of software tools, datasets, benchmark suites, computing infrastructure, and evaluation platforms whose combined performance directly influences the reliability and reproducibility of testing outcomes.

The objective of the registry is to provide National Competent Authorities (NCAs) with evidence that the laboratory has evaluated the suitability of its technical resources before they are used in conformity assessment or independent testing activities. Maintaining such documentation may also assist laboratories in demonstrating that testing activities are performed using validated methods, controlled software environments, and appropriately governed datasets.

Within the context of the AI Act, maintaining documented information regarding testing methodologies, software tools, datasets, benchmark suites, and computing environments contributes to the preparation of technical documentation and supports traceability, reproducibility, and performance evaluation. Although the AI Act does not prescribe specific validation methods for laboratory resources, maintaining a validation registry

may facilitate the assessment of the laboratory's technical competence and the consistency of its testing activities.

For example, in an AI biometrics lab where physical measuring tapes are replaced by neural networks and mathematical scripts this registry is the core pillar of the accreditation and/or notification audit.

The registry should include sufficient information to demonstrate the algorithmic and mathematical integrity of the test software of the lab. For example, where applicable, the registry should include benchmarking results produced by the test-code for datasets for which ground-truth is available.

Such results not only prove the mathematical integrity of the test-software but also support traceability by demonstrating that successive code updates do not change the results on standard test datasets. Finally, if an AI product approved by a testing lab fails in the real world, this registry will serve to shield the test lab from legal liability, by affirming that the testing process has not been compromised by faulty digital tools.

The following sections illustrate one possible approach for constructing and maintaining such a registry.

### C.5.1 Identification of Technical Resources Subject to validation

The first step consists of identifying all technical resources that may influence the validity of testing activities. Validation should not be limited to software applications but should encompass the broader technical ecosystem supporting AI evaluation.

Resources requiring validation may include AI evaluation platforms, automated testing frameworks, software libraries, benchmark execution engines, cybersecurity assessment tools, explainability frameworks, fairness assessment tools, and statistical analysis software.

Supporting software components may also require validation. Depending on the laboratory's activities, validation may also extend to virtualization platforms, cloud computing services, GPU drivers, firmware versions, operating systems, and hardware accelerators.

Validation activities may include verifying dataset integrity, version consistency, annotation quality, completeness, and suitability for the intended testing purpose.

### C.5.2 Validation of Testing Methods

Testing methodologies should be demonstrated to be technically appropriate for the AI systems and performance characteristics being evaluated. Method validation provides confidence that testing procedures produce reliable, repeatable, and scientifically meaningful results under the intended conditions of use.

Validation activities may include the evaluation of repeatability, reproducibility, sensitivity, robustness, statistical confidence, uncertainty analysis where applicable, and comparison against recognized reference methodologies. Laboratories may also evaluate whether testing methods remain valid when applied to different model architectures, deployment environments, demographic populations, languages, or operating conditions.

Where recognized international standards exist, laboratories may reference these documents when establishing validation procedures. Examples include ISO/IEC 17025 for laboratory competence, ISO/IEC 42001 for AI management systems, ISO/IEC 23894 for AI risk management, ISO/IEC 22989 for AI concepts and terminology, ISO/IEC TR 24028 for AI trustworthiness, ISO/IEC TS 4213 for AI system performance testing, and ISO/IEC 25059 for quality models applicable to AI systems. Depending on the application domain, additional sector-specific standards or evaluation protocols may also be considered.

Table 2 and Table 3 comprise an example of the Methods and Software Registry for hypothetical biometrics testing lab applying for accreditation and/or notification.

Table 2 shows an example of a Methods Registry. The Methods Registry proves that the operational procedures of the lab, for evaluating the biometrics recognition and PAD accuracy of biometrics products, are aligned with international standards.

|            | Method Name / Description                                   | Reference Standard                              | Validation Verification Type                                       | Linked Software Assets | Validation Report Ref | Review Re-val. Cycle              | Status   |
|------------|-------------------------------------------------------------|-------------------------------------------------|--------------------------------------------------------------------|------------------------|-----------------------|-----------------------------------|----------|
| MET-ACC-01 | Facial Recognition Accuracy & Performance Testing           | ISO/IEC 19795-2 (Biometric performance testing) | Verification (Standard method adopted unchanged)                   | SW-CORE-01, SW-CALC-01 | VR-MET-ACC-2026-v1    | Annual (Next: June 2027)          | Approved |
| MET-PAD-02 | Presentation Attack Detection (PAD)                         | ISO/IEC 30107-3 (Testing and reporting for PAD) | Validation (Non-standard extension for synthetic morphing attacks) | SW-CORE-02, SW-PAD-01  | VR-MET-PAD-2026-v2    | 12 Months or upon standard update | Approved |
| MET-FP-03  | Fingerprint Recognition Accuracy under Environmental Stress | ISO/IEC 19795-4 (Interoperability performance)  | Verification (Standard method)                                     | SW-CORE-01, SW-CALC-01 | VR-MET-FP-2026-v1     | Annual (Next: August 2027)        | Approved |

Table C.2: Example of a Method Validation Registry used by Biometrics Testing Lab

### C.5.3 Validation of Software and AI Evaluation Platforms

Software validation aims to demonstrate that evaluation tools operate correctly, consistently, and according to their intended purpose. Validation activities should consider both functional correctness and the reproducibility of evaluation results.

Validation records may include software identification, developer or vendor, semantic version number, internal asset identifier, deployment environment, supported operating systems, software dependencies, licensing status, and validation status. Integrity verification may be supported through cryptographic mechanisms such as SHA-256 hash values or digitally signed software packages, allowing laboratories to confirm that software has not been modified after validation.

Where software updates occur, laboratories may assess whether revalidation is necessary before the updated version is introduced into operational testing activities. Validation evidence may consist of vendor documentation, internal verification reports, unit testing results, regression testing, comparison against reference outputs, interoperability testing, or participation in collaborative evaluation exercises.

Table 3 shows how to structure a ISO/IEC 17025 Software Registry. The Software Registry demonstrates that the testing code, algorithms, and dependencies are version-controlled, mathematically accurate, and completely secure. In this context, it is important to include the SHA-256 hash for each piece of software in this table, so as to prevent unapproved hot-fixes to the testing code.

|            | Tool Script Name /                      | Vers-ion | Crypto-graphic Hash (SHA-256) | Type Source /                            | Purpose                                                                       | Validation Report Ref.                                         | Re-Validation Trigger                    | Status   |
|------------|-----------------------------------------|----------|-------------------------------|------------------------------------------|-------------------------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------|----------|
| SW-CORE-01 | Python Biometric Evaluation Environment | v3.11.4  | <insert hash>                 | Core Environment (Anaconda / Linux Mint) | Base OS and interpreter hosting testing pipelines.                            | VR-SW-ENV-2026                                                 | Base OS update; Core Python patch.       | Approved |
| SW-CORE-02 | InsightFace AI Framework                | v0.7.3   |                               | Open-Source Library                      | Extracting face embeddings, facial landmarks, and alignment steps.            | VR-SW-INSIGHT-01                                               | Upstream updates or library model swaps. | Approved |
| SW-COTS-01 | SQLite Database Engine                  | v3.45.1  |                               | Commercial Off-the-Shelf (COTS)          | Storing anonymised reference metadata and test configurations.                | Storing anonymised reference metadata and test configurations. | Minor/Major engine upgrades.             | Approved |
| SW-CALC-01 | Biometric_Metrics_Lib.py                | v2.1.0   |                               | In-house Custom Script                   | Calculates FMR, FNMR, APCER, BPCER, and ROC curves with confidence intervals. | VR-SW-CALC-002                                                 | Any change to the Python script.         | Approved |
| SW-PAD-01  | PAD_Artifact_Analyzer.py                | v1.0.4   |                               | In-house Custom Script                   | Automates spoof texture evaluation.                                           | VR-SW-PAD-004                                                  | Changes in script or any dependency.     | Approved |

Table C.3: Software Validation Registry Example

### C.5.4 Validation of Datasets and Benchmark Suites

Datasets and benchmark suites play a central role in AI testing because they directly influence the interpretation of evaluation results. Consequently, laboratories may establish documented procedures to verify that datasets remain suitable for their intended testing objectives.

Validation activities may include verification of dataset provenance, version history, completeness, annotation consistency, demographic representativeness, statistical balance, and known limitations. Laboratories may additionally verify the integrity of datasets using cryptographic hash values and maintain records describing any preprocessing or transformation activities performed before testing.

Benchmark validation may include confirmation that benchmark implementations correspond to published evaluation protocols, that scoring methodologies remain unchanged, and that benchmark versions are clearly identified within testing reports. Where benchmark suites evolve over time, laboratories may retain historical benchmark versions to preserve the reproducibility of previously completed evaluations.

As part of reference-data traceability the laboratory could use integrity and versioning mechanisms (content hashing, immutable snapshots). This is the dataset analogue of reference-material traceability in classical metrology and is cheap to implement.

These activities support several objectives identified within Article 10 of the AI Act concerning data governance and contribute to the technical documentation expected under Annex IV.

### C.5.5 Validation of Computing Infrastructure

The computing environment forms an integral part of AI testing activities and may significantly influence testing performance, execution time, numerical reproducibility, and system behaviour. Consequently, laboratories may document the validation status of the computing infrastructure used during evaluations.

Validation information may include processor architecture, GPU models, memory configuration, operating system versions, virtualization technologies, container platforms, cloud service providers, orchestration platforms, storage infrastructure, and network configurations. Examples may include NVIDIA A100 or H100 accelerators, Docker containers, Kubernetes clusters, Microsoft Azure, Amazon Web Services, or Google Cloud Platform environments.

Where infrastructure changes occur, laboratories may evaluate whether testing results remain comparable with previous evaluations and whether additional validation activities are necessary.

### C.5.6 Validation Records and Traceability

Each validated resource may be supported by documented evidence demonstrating that the validation activities have been completed successfully. Validation records may identify the resource being validated, the applicable validation methodology, the personnel responsible, the date of validation, the validation outcome, supporting documentation, and any identified limitations.

To facilitate traceability, laboratories may maintain links between validation records, software repositories, dataset versions, benchmark suites, configuration management systems, and technical documentation. Version control systems such as Git or Subversion (SVN) may provide additional evidence regarding software evolution, while configuration management databases may support infrastructure traceability.

Maintaining such relationships contributes to reproducibility and enables independent reviewers to reconstruct the technical environment used during previous testing activities.

### C.5.7 Periodic Review and Revalidation

Validation should not be considered a one-time activity. Software tools, datasets, benchmark suites, AI models, and computing infrastructures evolve continuously, potentially affecting the validity of testing methods and previously established validation evidence.

Laboratories may therefore establish periodic review procedures to determine whether technical resources continue to satisfy their intended purpose. Events that may trigger revalidation include software updates, changes to benchmark methodologies, introduction of new datasets, modifications to AI evaluation platforms, updates to operating systems or software libraries, replacement of computing infrastructure, migration to cloud environments, or significant revisions to testing procedures.

Documenting these activities may assist laboratories in maintaining confidence in the consistency and reliability of their testing activities over time.

D. ANNEX D: CHECKLIST AUDIT

D.1 LABORATORY AUDIT INFORMATION

|                           | DETAILS                                     |                                       |                                        |
|---------------------------|---------------------------------------------|---------------------------------------|----------------------------------------|
| Audit Reference No.       |                                             |                                       |                                        |
| Audit Type                | <input type="checkbox"/> Initial Assessment | <input type="checkbox"/> Surveillance | <input type="checkbox"/> Re-assessment |
| Laboratory Name           |                                             |                                       |                                        |
| Laboratory Address        |                                             |                                       |                                        |
| Date(s) of Audit          |                                             |                                       |                                        |
| Lead Auditor              |                                             |                                       |                                        |
| Technical Expert(s)       |                                             |                                       |                                        |
| Laboratory Representative |                                             |                                       |                                        |
| Scope of Assessment       |                                             |                                       |                                        |

D.2 AUDIT AREA 1- LEGAL AND ORGANIZATIONAL FRAMEWORK

D.2.1 Objective

To verify the laboratory has an appropriate legal status, governance structure and organizational arrangements to perform conformity assessment activities.

D.2.2 Verification Activities

|                              |           | Needs to be verified during the audit (Yes / No) | Verified during the audit (Yes / No) |
|------------------------------|-----------|--------------------------------------------------|--------------------------------------|
| Legal Establishment Verified |           |                                                  |                                      |
| Organizational Documented    | Structure |                                                  |                                      |

|                                     |  |  |
|-------------------------------------|--|--|
| Responsibilities Defined            |  |  |
| Reporting Lines Established         |  |  |
| Governance Supports Accountability  |  |  |
| Scope of Activities Clearly Defined |  |  |

D.3 AUDIT AREA 2- INDEPENDENCE AND IMPARTIALITY

D.3.1 Objective

To determine whether the laboratory maintains independence, impartiality and freedom from conflicts of interest.

D.3.2 Verification Activities

|                                          | Needs to be verified during the audit (Yes / No) | Verified during the audit (Yes / No) |
|------------------------------------------|--------------------------------------------------|--------------------------------------|
| Impartiality Policy Implemented          |                                                  |                                      |
| Conflict of Interest Process Established |                                                  |                                      |
| Staff Declaration Available              |                                                  |                                      |
| Consultancy Activities Prevented         |                                                  |                                      |
| Independence Safeguarded                 |                                                  |                                      |
| Impartiality Risks Periodically Reviewed |                                                  |                                      |

D.4 AUDIT AREA 3- PERSONNEL COMPETENCE

D.4.1 Objective

To verify that personnel possess the competence required to perform conformity assessments activities.

D.4.2 Verification Activities

|  | Needs to be verified during the audit (Yes / No) | Verified during the audit (Yes / No) |
|--|--------------------------------------------------|--------------------------------------|
|--|--------------------------------------------------|--------------------------------------|

|                                     |  |  |
|-------------------------------------|--|--|
| Competence Criteria Defined         |  |  |
| Competence Matrix Maintained        |  |  |
| Qualifications Verified             |  |  |
| AI Technical Expertise Available    |  |  |
| Cybersecurity Expertise Available   |  |  |
| Training Program Implemented        |  |  |
| Personnel Authorizations Maintained |  |  |

D.5 AUDIT AREA 4- EQUIPMENT AND INFRASTRUCTURE

D.5.1 Verification Activities

|                                   | Needs to be verified during the audit (Yes / No) | Verified during the audit (Yes / No) |
|-----------------------------------|--------------------------------------------------|--------------------------------------|
| Equipment Inventory Maintained    |                                                  |                                      |
| Calibration Records Available     |                                                  |                                      |
| Computing Infrastructure suitable |                                                  |                                      |
| Secure Testing Environment        |                                                  |                                      |
| Cloud Services Controlled         |                                                  |                                      |
| Access to facilities Controlled   |                                                  |                                      |

D.6 AUDIT AREA 5- QUALITY MANAGEMENT SYSTEM

D.6.1 Verification Activities

|                          | Needs to be verified during the audit (Yes / No) | Verified during the audit (Yes / No) |
|--------------------------|--------------------------------------------------|--------------------------------------|
| Quality Manual Available |                                                  |                                      |

|                              |  |  |
|------------------------------|--|--|
| Procedures Documented        |  |  |
| Document Control Implemented |  |  |
| Internal Audits Conducted    |  |  |
| Management Reviews Completed |  |  |
| Corrective Actions Effective |  |  |
| Risk Management Implemented  |  |  |

## D.7 AUDIT AREA 6- CONFORMITY ASSESSMENT ACTIVITIES

### D.7.1 Verification Activities

|                                  | Needs to be verified during the audit (Yes / No) | Verified during the audit (Yes / No) |
|----------------------------------|--------------------------------------------------|--------------------------------------|
| Assessment Procedures Documented |                                                  |                                      |
| Test Methods Validated           |                                                  |                                      |
| Technical Reviews Performed      |                                                  |                                      |
| Assessment Decisions Justified   |                                                  |                                      |
| Certificates Controlled          |                                                  |                                      |
| Assessment Records Traceable     |                                                  |                                      |

## D.8 AUDIT AREA 7- EXTERNAL PROVIDERS

### D.8.1 Verification Activities

|                            | Needs to be verified during the audit (Yes / No) | Verified during the audit (Yes / No) |
|----------------------------|--------------------------------------------------|--------------------------------------|
| External Experts Qualified |                                                  |                                      |
| Subcontractors Evaluated   |                                                  |                                      |

|                                   |  |  |
|-----------------------------------|--|--|
| Contacts Established              |  |  |
| Confidentiality Agreements Signed |  |  |
| Performance Monitored             |  |  |

D.9 AUDIT AREA 8- INFORMATION SECURITY AND CYBERSECURITY

D.9.1 Verification Activities

|                                   | Needs to be verified during the audit (Yes / No) | Verified during the audit (Yes / No) |
|-----------------------------------|--------------------------------------------------|--------------------------------------|
| Cybersecurity Policy Implemented  |                                                  |                                      |
| Access Controls Established       |                                                  |                                      |
| Incident Management Process       |                                                  |                                      |
| Backup Procedures Implemented     |                                                  |                                      |
| Technical Documentation Protected |                                                  |                                      |
| AI Datasets Securely Managed      |                                                  |                                      |

D.10 AUDIT AREA 9- CONFIDENTIALITY

D.10.1Verification Activities

|                                        | Needs to be verified during the audit (Yes / No) | Verified during the audit (Yes / No) |
|----------------------------------------|--------------------------------------------------|--------------------------------------|
| Confidentiality Procedures Established |                                                  |                                      |
| NDAs Signed                            |                                                  |                                      |
| Secure Storage of Information          |                                                  |                                      |

|                               |            |  |
|-------------------------------|------------|--|
| Confidential Disposal Process |            |  |
| Staff Awareness Verified      |            |  |
| Confidentiality Established   | Procedures |  |

D.11 AUDIT AREA 10- STANDARDIZATION AND REGULATORY MONITORING

D.11.1Verification Activities

|                                       | Needs to be verified during the audit (Yes / No) | Verified during the audit (Yes / No) |
|---------------------------------------|--------------------------------------------------|--------------------------------------|
| Relevant AI Standards Monitored       |                                                  |                                      |
| Regulatory Changes Tracked            |                                                  |                                      |
| Staff Informed of Updates             |                                                  |                                      |
| Participation in Technical Activities |                                                  |                                      |

D.12 AUDIT SUMMARY

| Audit Area                       | Need to be verified (tick if yes) | Verified (tick if yes)   |
|----------------------------------|-----------------------------------|--------------------------|
| Legal & Organizational Framework | <input type="checkbox"/>          | <input type="checkbox"/> |
| Independence & Impartiality      | <input type="checkbox"/>          | <input type="checkbox"/> |
| Personnel Competence             | <input type="checkbox"/>          | <input type="checkbox"/> |
| Equipment & Infrastructure       | <input type="checkbox"/>          | <input type="checkbox"/> |
| Quality Management System        | <input type="checkbox"/>          | <input type="checkbox"/> |

|                                  |                          |                          |
|----------------------------------|--------------------------|--------------------------|
| Conformity Assessment Activities | <input type="checkbox"/> | <input type="checkbox"/> |
| External Providers               | <input type="checkbox"/> | <input type="checkbox"/> |
| Information Security             | <input type="checkbox"/> | <input type="checkbox"/> |
| Confidentiality                  | <input type="checkbox"/> | <input type="checkbox"/> |
| Standardization                  | <input type="checkbox"/> | <input type="checkbox"/> |

## E. ANNEX E: TRAINING CURRICULUM TEMPLATE

### E.1 PURPOSE

During the development of this deliverable, it was recognized that the training curriculum dedicated to third-party laboratory notification constitutes one thematic component of the broader CERTAIN capacity-building program coordinated by 28Digital under T8.5.

This Annex outlines the scope of the future capacity-building module related to the notification of third-party evaluation laboratories, which will be developed under T8.5. The module will build upon the framework, tools and templates developed in D6.2 to explain the notification process and how stakeholders can use these outputs to prepare for notification. The detailed training format, learning activities and delivery approach will be developed within the broader CERTAIN capacity-building programme coordinated by 28Digital under T8.5, where it will be aligned with the overall modular structure and adapted to the needs of the relevant target groups.

The training will consider the different targets of the notification of 3<sup>rd</sup> party evaluation laboratories as mentioned in the master document of D6.2, namely:

- The third-party laboratories, whether private or academics, to explain the notification framework, and how the D6.2 toolkit can be used when preparing for accreditation and/or notification;
- The entities actually in charge of accreditation (e.g., [COFRAC](#) in France) or the notification;
- The entities that will need a notified 3<sup>rd</sup> party evaluation laboratory such as
  - The National Competent authorities or other Notified bodies;
  - The Market Surveillance authorities;
  - The AI systems providers.

The module will build upon the outputs developed in D6.2 in the other annexes, namely:

- The laboratory application form
- The competence matrix
- The technical capability inventory,
- The audit checklist,
- The proposed reporting template,
- The monitoring of notified laboratories, including notification revisions as necessary and complaints handling

Under T8.5, these materials will be organised into audience-specific capacity-building modules. The objective will be to explain the notification framework, its expected outputs and how the D6.2 toolkit can be applied by the different stakeholder groups, rather than to provide the internal technical training that notified laboratories remain responsible for developing for their own personnel.

The following preliminary outline will be further aligned with the common structure, learning objectives and delivery approach of the CERTAIN capacity-building program.

1. Why notifying 3<sup>rd</sup> party independent labs to perform tests in the context of AI act compliance
2. How a 3<sup>rd</sup> party lab should handle competencies and technical capabilities, with examples
3. The accreditation and notification: actors and process
4. Proposed forms (application, audit checklist, reporting)

F. ANNEX F: REPORTING TEMPLATE

F.1 PART I- REPORT IDENTIFICATION AND ADMINISTRATIVE INFORMATION

|                                       |  |
|---------------------------------------|--|
| Report Reference Number:              |  |
| Date of Audit:                        |  |
| Date of Report Issuance:              |  |
| ISSUING AUTHORITY REFERENCE           |  |
| Name of National Competent Authority: |  |
| Member State:                         |  |
| Address:                              |  |
| Contact person:                       |  |
| Email:                                |  |

F.1.1 Audit Team Composition

|                           |  |
|---------------------------|--|
| LEAD AUDITOR              |  |
| Name                      |  |
| Title                     |  |
| Qualification             |  |
| TECHNICAL EXPERT #1       |  |
| Name                      |  |
| Title                     |  |
| Expertise - Qualification |  |

| TECHNICAL EXPERT #2       |  |
|---------------------------|--|
| Name                      |  |
| Title                     |  |
| Expertise - Qualification |  |
| TECHNICAL EXPERT #3       |  |
| Name                      |  |
| Title                     |  |
| Expertise - Qualification |  |
| Observers                 |  |
|                           |  |

The composition of the audit team reflects the requirement established under Article 28(7) of Regulation (EU) 2024/1689 (the EU AI Act), which states that notifying authorities must have an adequate number of competent personnel with the necessary expertise in information technologies, artificial intelligence, law, and the supervision of fundamental rights.

F.1.2 Laboratory Under Audit

| LABORATORY REFERENCE                                              |  |
|-------------------------------------------------------------------|--|
| Full legal name of the laboratory:                                |  |
| Legal form and registration number:                               |  |
| Address:                                                          |  |
| Name and title of laboratory representative present during audit: |  |
| Email:                                                            |  |

Type of Audit:

☐ Initial assessment audit

- ☐ Periodic surveillance audit
- ☐ Re-evaluation audit
- ☐ Extraordinary audit (triggered by complaint, incident, or change notification)

**A site visit has been performed by the NCA?**

- ☐ Yes
- ☐ No

**F.1.3 Scope of notification sought/ under review:**

The laboratory is seeking notification to conduct conformity assessment activities in relation to AI systems falling within one or more of the following categories.

**F.1.3.1 Category A - High-Risk AI Systems by virtue of their intended purpose in a regulated product (*Article 6(1) of the AI Act*)**

These are AI systems that are themselves safety components of products, or that are products, covered by Union harmonization legislation listed in *Annex I of the AI Act*, and which are required to undergo a third-party conformity assessment under that legislation. This category includes, but is not limited to, AI systems embedded in or constituting machinery, medical devices, in vitro diagnostic medical devices, civil aviation equipment, motor vehicles, radio equipment, and other regulated products.

- ☐ AI systems that are safety components of products covered by Union harmonization legislation listed in *Annex I of the AI Act* and subject to third-party conformity assessment under that legislation.

If ticked, specify the relevant Union harmonization legislation and product category:

**F.1.3.2 Category B - High-Risk AI Systems by virtue of their area of application (*Article 6(2) and Annex III of the AI Act*)**

- ☐ Biometric identification and categorization of natural persons
- ☐ Management and operation of critical infrastructure
- ☐ Education and vocational training
- ☐ Employment, workers management and access to self-employment
- ☐ Access to and enjoyment of essential private services and public services and benefits
- ☐ Law enforcement
- ☐ Migration, Asylum and border control management
- ☐ Administration of justice and democratic processes

**F.1.3.3 Category C - AI Systems not classified as High-Risk**

Under the AI Act, AI systems that do not fall within Categories A or B above are not classified as high-risk and are therefore not subject to the conformity assessment obligations applicable to high-risk AI systems. However, NCAs may extend the scope of notification to cover evaluation activities in relation to such systems, for example in the context of transparency obligations under *Article 50 of the AI Act*, voluntary conformity assessments, or national evaluation frameworks that go beyond the minimum requirements of the Act.

☐ AI systems not classified as high-risk

Specify:

**Note on scope boundaries:** A laboratory may seek notification for one or more of the categories above. The scope of notification granted by the NCA will be limited to the specific categories and sub-categories for which the laboratory has demonstrated the requisite technical competence, independence, and procedural capability during the audit. The claimed scope must be clearly delimited and may not be extended without a specific supplementary assessment conducted by the NCA.

Describe the specific types of AI systems and conformity assessment tasks within the claimed scope, specifying for each category ticked above the techniques, methodologies, and standards the laboratory proposes to apply:

| Categories | Method Principles | Methodology reference used |
|------------|-------------------|----------------------------|
|            |                   |                            |
|            |                   |                            |
|            |                   |                            |
|            |                   |                            |
|            |                   |                            |

F.2 PART II – REGULATORY BASIS AND PURPOSE OF THE AUDIT

This audit report documents the assessment conducted by the National Competent Authority (NCA) acting in its capacity as notifying authority pursuant to *Article 28 of Regulation (EU) 2024/1689*, which requires each Member State to designate or establish at least one notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation, and notification of conformity assessment bodies, and for their ongoing monitoring.

The purpose of this audit is to verify whether the laboratory under review satisfies all requirements applicable to fulfil its conformity assessment tasks, as well as suitable cybersecurity requirements. The audit also verifies whether the laboratory satisfies the independence, impartiality, and competence requirements that condition its suitability to carry out conformity assessment activities in relation to high-risk AI systems.

## F.3 PART III- ASSESSMENT OF LEGAL STATUS AND ORGANIZATIONAL STRUCTURE

### F.3.1 Legal Status

*Article 31(1) of the AI Act* requires that to be established under the national law of a Member State and have legal personality.

|                       | LEGAL STATUS                                                                                                  |                                              |                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
| Verification Item     | Evidence of legal establishment under national law (certificate of incorporation, official register extract): |                                              |                                         |
| Proof                 | <input type="checkbox"/> Provided                                                                             | <input type="checkbox"/> Not provided        | <input type="checkbox"/> Incomplete     |
| Comments on proof     |                                                                                                               |                                              |                                         |
| Status                | <input type="checkbox"/> Satisfactory                                                                         | <input type="checkbox"/> Partially completed | <input type="checkbox"/> Unsatisfactory |
| Comment / Findings    |                                                                                                               |                                              |                                         |
| Date of establishment |                                                                                                               |                                              |                                         |

| SPECIFIC REQUIREMENTS                                  |                              |           |
|--------------------------------------------------------|------------------------------|-----------|
| Legal personality confirmed?                           | <input type="checkbox"/> Yes | Comments: |
|                                                        | <input type="checkbox"/> No  |           |
|                                                        | <input type="checkbox"/> N/A |           |
| Registered in the relevant national or Union register? | <input type="checkbox"/> Yes | Comments: |
|                                                        | <input type="checkbox"/> No  |           |
|                                                        | <input type="checkbox"/> N/A |           |

### F.3.2 Organizational Structure, Reporting Lines, and Accountability

*Article 31(3) of the AI Act* requires that the organizational structure, allocation of responsibilities, reporting lines, and operation shall ensure confidence in performance and in the results of the conformity assessment activities conducted

|                       |                                                                                                                                          |                                              |                                         |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
|                       | Organizational Structure, Reporting Lines, and Accountability                                                                            |                                              |                                         |
| Verification Item     | Evidence of compliance is demonstrated through clear structure, roles, and reporting lines ensuring confidence in assessment activities. |                                              |                                         |
| Proof                 | <input type="checkbox"/> Provided                                                                                                        | <input type="checkbox"/> Not provided        | <input type="checkbox"/> Incomplete     |
| Comments on proof     |                                                                                                                                          |                                              |                                         |
| Status                | <input type="checkbox"/> Satisfactory                                                                                                    | <input type="checkbox"/> Partially completed | <input type="checkbox"/> Unsatisfactory |
| Comment / Findings    |                                                                                                                                          |                                              |                                         |
| Date of establishment |                                                                                                                                          |                                              |                                         |

| SPECIFIC REQUIREMENTS                                                                                 |                              |           |
|-------------------------------------------------------------------------------------------------------|------------------------------|-----------|
| Organizational chart provided and reviewed?                                                           | <input type="checkbox"/> Yes | Comments: |
|                                                                                                       | <input type="checkbox"/> No  |           |
|                                                                                                       | <input type="checkbox"/> N/A |           |
| Allocation of responsibilities for conformity assessment activities clearly documented?               | <input type="checkbox"/> Yes | Comments: |
|                                                                                                       | <input type="checkbox"/> No  |           |
|                                                                                                       | <input type="checkbox"/> N/A |           |
| Reporting lines between technical staff, management, and quality function clearly defined?            | <input type="checkbox"/> Yes | Comments: |
|                                                                                                       | <input type="checkbox"/> No  |           |
|                                                                                                       | <input type="checkbox"/> N/A |           |
| The governance structure supports accountability and traceability of conformity assessment decisions? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                       | <input type="checkbox"/> No  |           |
|                                                                                                       | <input type="checkbox"/> N/A |           |

## F.4 PART IV- ASSESSMENT OF INDEPENDENCE AND IMPARTIALITY

*Article 31(4) of the AI Act* highlights the importance of being independent

- of the provider of any high-risk AI system in relation to which a conformity assessment activity will be performed, and
- of any other operator having an economic interest in assessed high-risk AI systems, as well as
- of any competitors of the provider.

*Article 31(5)* further mentions that neither the top-level management, nor the personnel responsible for conformity assessment tasks may be directly involved in the design, development, marketing, or use of high-risk AI systems. Additionally, they should not represent parties engaged in those activities or engage in any activity that might conflict with the independence of judgement or integrity of the assessor, especially consultancy services. *Article 31(6)* requires to be organised and operated to safeguard the independence, objectivity, and impartiality of conformity assessment activities, and that a structure and procedures to safeguard impartiality throughout their organisation, personnel, and assessment activities are documented and implemented.

|                       | Assessment of Independence and Impartiality                                                                                                               |                                              |                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
| Verification Item     | Evidence of compliance is demonstrated through independence from operators and safeguards ensuring impartiality and objectivity in assessment activities. |                                              |                                         |
| Proof                 | <input type="checkbox"/> Provided                                                                                                                         | <input type="checkbox"/> Not provided        | <input type="checkbox"/> Incomplete     |
| Comments on proof     |                                                                                                                                                           |                                              |                                         |
| Status                | <input type="checkbox"/> Satisfactory                                                                                                                     | <input type="checkbox"/> Partially completed | <input type="checkbox"/> Unsatisfactory |
| Comment / Findings    |                                                                                                                                                           |                                              |                                         |
| Date of establishment |                                                                                                                                                           |                                              |                                         |

| SPECIFIC REQUIREMENTS                                                          |                              |           |
|--------------------------------------------------------------------------------|------------------------------|-----------|
| Written policy on independence and conflict of interest in place and reviewed? | <input type="checkbox"/> Yes | Comments: |
|                                                                                | <input type="checkbox"/> No  |           |
|                                                                                | <input type="checkbox"/> N/A |           |
|                                                                                | <input type="checkbox"/> Yes | Comments: |

|                                                                                                                                              |                              |           |
|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------|
| Conflict of interest declarations obtained from all personnel involved in conformity assessment?                                             | <input type="checkbox"/> No  |           |
|                                                                                                                                              | <input type="checkbox"/> N/A |           |
| No member of top-level management holds a position or financial interest in any AI provider operating in the scope of notification?          | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                              | <input type="checkbox"/> No  |           |
|                                                                                                                                              | <input type="checkbox"/> N/A |           |
| No personnel responsible for conformity assessment tasks are involved in the design, development, marketing, or use of high-risk AI systems? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                              | <input type="checkbox"/> No  |           |
|                                                                                                                                              | <input type="checkbox"/> N/A |           |
| The laboratory does not provide consultancy services to AI providers in areas covered by its conformity assessment scope?                    | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                              | <input type="checkbox"/> No  |           |
|                                                                                                                                              | <input type="checkbox"/> N/A |           |
| Documented procedures for safeguarding impartiality reviewed and assessed as adequate?                                                       | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                              | <input type="checkbox"/> No  |           |
|                                                                                                                                              | <input type="checkbox"/> N/A |           |
| Mechanisms for identifying and resolving conflicts of interest operational?                                                                  | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                              | <input type="checkbox"/> No  |           |
|                                                                                                                                              | <input type="checkbox"/> N/A |           |

## F.5 PART V-ASSESSMENT OF HUMAN RESOURCES AND TECHNICAL COMPETENCE

*Article 31(10)* of the AI Act requires to carry out all conformity assessment tasks with the highest degree of professional integrity and the requisite competence in the specific field.

*Article 31(11)* highlights that sufficient internal competences shall exist to effectively evaluate tasks conducted by external parties on behalf. Additionally, it requires permanent availability of sufficient administrative, technical, legal, and scientific personnel possessing experience and knowledge relating to the relevant types of AI systems, data and data computing, and the substantive requirements applicable to high-risk AI systems.

Article 31(8) requires having procedures for the performance of activities that take due account of the size of the provider, the sector in which it operates, its structure, and the degree of complexity of the AI system concerned.

### F.5.1 Management of External Experts and Subcontractors

|                       |                                                                                                                                                          |                                              |                                         |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
|                       | Management of External Experts and Subcontractors                                                                                                        |                                              |                                         |
| Verification Item     | Evidence of compliance is demonstrated through high professional competence, adequate expertise, and procedures adapted to the complexity of AI systems. |                                              |                                         |
| Proof                 | <input type="checkbox"/> Provided                                                                                                                        | <input type="checkbox"/> Not provided        | <input type="checkbox"/> Incomplete     |
| Comments on proof     |                                                                                                                                                          |                                              |                                         |
| Status                | <input type="checkbox"/> Satisfactory                                                                                                                    | <input type="checkbox"/> Partially completed | <input type="checkbox"/> Unsatisfactory |
| Comment / Findings    |                                                                                                                                                          |                                              |                                         |
| Date of establishment |                                                                                                                                                          |                                              |                                         |

| SPECIFIC REQUIREMENTS                                                                            |                              |           |
|--------------------------------------------------------------------------------------------------|------------------------------|-----------|
| Procedures for commissioning external experts and subcontractors documented and reviewed?        | <input type="checkbox"/> Yes | Comments: |
|                                                                                                  | <input type="checkbox"/> No  |           |
|                                                                                                  | <input type="checkbox"/> N/A |           |
| Internal competence to evaluate and supervise work carried out by external parties demonstrated? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                  | <input type="checkbox"/> No  |           |
|                                                                                                  | <input type="checkbox"/> N/A |           |
| Confidentiality and impartiality obligations extended to subcontractors by contract?             | <input type="checkbox"/> Yes | Comments: |
|                                                                                                  | <input type="checkbox"/> No  |           |
|                                                                                                  | <input type="checkbox"/> N/A |           |

## F.5.2 Management of External and Rented Equipment and Facilities

*Article 31(2)* of the AI Act requires to satisfy the resource requirements necessary to fulfil conformity assessment tasks. This includes not only human resources but also the technical infrastructure, equipment, and facilities used in the conduct of assessment activities. Where a laboratory does not own all the equipment or facilities it uses, for example where testing instruments, computing infrastructure, secure data environments, or specialized hardware are rented, leased, or borrowed from a third party, the laboratory must demonstrate that it retains full operational control over such resources during their use, that the integrity and confidentiality of assessment activities conducted using those resources are not compromised, and that the use of external resources does not affect its independence or impartiality as required under *Article 31(4)* and *Article 31(6)* of the AI Act.

|                       | Management of External Experts and Rented Equipment and Facilities                                                                                                      |                                              |                                         |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
| Verification Item     | Evidence of compliance is demonstrated through adequate resources, controlled use of external infrastructure, and safeguards ensuring independence and confidentiality. |                                              |                                         |
| Proof                 | <input type="checkbox"/> Provided                                                                                                                                       | <input type="checkbox"/> Not provided        | <input type="checkbox"/> Incomplete     |
| Comments on proof     |                                                                                                                                                                         |                                              |                                         |
| Status                | <input type="checkbox"/> Satisfactory                                                                                                                                   | <input type="checkbox"/> Partially completed | <input type="checkbox"/> Unsatisfactory |
| Comment / Findings    |                                                                                                                                                                         |                                              |                                         |
| Date of establishment |                                                                                                                                                                         |                                              |                                         |

| SPECIFIC REQUIREMENTS                                                                                                                          |                              |           |
|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------|
| Inventory of all equipment and facilities used in conformity assessment activities that are not owned by the laboratory provided and reviewed? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                | <input type="checkbox"/> No  |           |
|                                                                                                                                                | <input type="checkbox"/> N/A |           |
| For each rented or leased item of equipment or facility, a formal agreement with the owner documenting the terms of use is in place?           | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                | <input type="checkbox"/> No  |           |
|                                                                                                                                                | <input type="checkbox"/> N/A |           |
|                                                                                                                                                | <input type="checkbox"/> Yes | Comments: |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                              |                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|------------------|
| <p>The rental or lease agreements guarantee the laboratory exclusive and uninterrupted access to the relevant equipment or facility for the duration of each conformity assessment activity?</p>                                                                                                                                                                                                                                                                                                              | <input type="checkbox"/> No  |                  |
| <p>The laboratory has documented procedures ensuring that rented or leased equipment is calibrated, maintained, and fit for purpose prior to use in conformity assessment activities, and that responsibility for calibration and maintenance is clearly assigned?</p>                                                                                                                                                                                                                                        | <input type="checkbox"/> Yes | <p>Comments:</p> |
| <p>The laboratory can demonstrate that the owner of rented or leased equipment or facilities has no economic interest in the outcome of any conformity assessment activity conducted using those resources, thereby ensuring compliance with the independence requirements of Article 31(4)?</p>                                                                                                                                                                                                              | <input type="checkbox"/> No  |                  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> N/A |                  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> Yes |                  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> No  |                  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> N/A |                  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> Yes |                  |
| <p>Where rented or leased computing infrastructure or data environments are used, for example cloud computing services or shared data processing facilities, the laboratory has documented measures ensuring that data accessed or generated in the course of conformity assessment activities, including technical documentation and datasets provided by AI providers, is protected against unauthorized access and remains confidential in accordance with Article 31(7) and Article 78 of the AI Act?</p> | <input type="checkbox"/> Yes | <p>Comments:</p> |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> No  |                  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> N/A |                  |
| <p>The third-party provider of any rented or leased equipment or facility is bound by a contractual confidentiality obligation preventing it from accessing, disclosing, or retaining any information relating to conformity</p>                                                                                                                                                                                                                                                                              | <input type="checkbox"/> Yes | <p>Comments:</p> |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> No  |                  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> N/A |                  |

|                                                                                                                                                                                                                                                                            |                              |           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------|
| assessment activities conducted using its resources?                                                                                                                                                                                                                       |                              |           |
| The laboratory maintains full operational control and responsibility over all conformity assessment activities conducted using rented or leased resources, and the use of such resources does not transfer any assessment decision-making authority to the resource owner? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                                                                                                                                            | <input type="checkbox"/> No  |           |
|                                                                                                                                                                                                                                                                            | <input type="checkbox"/> N/A |           |
| Records documenting the use of rented or leased equipment and facilities in each conformity assessment activity are maintained and traceable?                                                                                                                              | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                                                                                                                                            | <input type="checkbox"/> No  |           |
|                                                                                                                                                                                                                                                                            | <input type="checkbox"/> N/A |           |
| Where rented or leased equipment is shared with other organizations, the laboratory has procedures ensuring that no cross-contamination of data or information between assessment activities occurs?                                                                       | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                                                                                                                                            | <input type="checkbox"/> No  |           |
|                                                                                                                                                                                                                                                                            | <input type="checkbox"/> N/A |           |

## F.6 PART VI- ASSESSMENT OF QUALITY MANAGEMENT, PROCESSES, AND CYBERSECURITY

*Article 31(2) of the AI Act* requires to satisfy the organizational, quality management, resources, and process requirements necessary to fulfil conformity assessment tasks, as well as suitable cybersecurity requirements.

### F.6.1 Quality Management System

|                   |                                                                               |                                       |                                     |
|-------------------|-------------------------------------------------------------------------------|---------------------------------------|-------------------------------------|
|                   | Quality Management System                                                     |                                       |                                     |
| Verification Item | Evidence of an implemented and use of an efficient quality management system. |                                       |                                     |
| Proof             | <input type="checkbox"/> Provided                                             | <input type="checkbox"/> Not provided | <input type="checkbox"/> Incomplete |

|                       |                                       |                                              |                                         |
|-----------------------|---------------------------------------|----------------------------------------------|-----------------------------------------|
| Comments on proof     |                                       |                                              |                                         |
| Status                | <input type="checkbox"/> Satisfactory | <input type="checkbox"/> Partially completed | <input type="checkbox"/> Unsatisfactory |
| Comment / Findings    |                                       |                                              |                                         |
| Date of establishment |                                       |                                              |                                         |

| SPECIFIC REQUIREMENTS                                                                                                            |                              |                              |
|----------------------------------------------------------------------------------------------------------------------------------|------------------------------|------------------------------|
| Quality management system documented and operational?                                                                            | <input type="checkbox"/> Yes | Comments:                    |
|                                                                                                                                  | <input type="checkbox"/> No  |                              |
|                                                                                                                                  | <input type="checkbox"/> N/A |                              |
| Quality management system certified under ISO/IEC 17025 or equivalent standard applicable to conformity assessment laboratories? | <input type="checkbox"/> Yes | Comments:                    |
|                                                                                                                                  | <input type="checkbox"/> No  | (If Yes, Certificate Number) |
|                                                                                                                                  | <input type="checkbox"/> N/A |                              |
| Document control procedures reviewed and assessed as adequate?                                                                   | <input type="checkbox"/> Yes | Comments:                    |
|                                                                                                                                  | <input type="checkbox"/> No  |                              |
|                                                                                                                                  | <input type="checkbox"/> N/A |                              |
| Management review process documented and operational?                                                                            | <input type="checkbox"/> Yes | Comments:                    |
|                                                                                                                                  | <input type="checkbox"/> No  |                              |
|                                                                                                                                  | <input type="checkbox"/> N/A |                              |
| Corrective action procedures in place and applied?                                                                               | <input type="checkbox"/> Yes | Comments:                    |
|                                                                                                                                  | <input type="checkbox"/> No  |                              |
|                                                                                                                                  | <input type="checkbox"/> N/A |                              |

## F.6.2 Conformity Assessment Procedures

|                       |                                                                                                                   |                                              |                                         |
|-----------------------|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
|                       | Conformity Assessment Procedures                                                                                  |                                              |                                         |
| Verification Item     | Evidence of the existence of a procedure that allow the laboratory to carry out Conformity Assessment activities. |                                              |                                         |
| Proof                 | <input type="checkbox"/> Provided                                                                                 | <input type="checkbox"/> Not provided        | <input type="checkbox"/> Incomplete     |
| Comments on proof     |                                                                                                                   |                                              |                                         |
| Status                | <input type="checkbox"/> Satisfactory                                                                             | <input type="checkbox"/> Partially completed | <input type="checkbox"/> Unsatisfactory |
| Comment / Findings    |                                                                                                                   |                                              |                                         |
| Date of establishment |                                                                                                                   |                                              |                                         |

| SPECIFIC REQUIREMENTS                                                                                                                                                  |                              |           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------|
| Documented procedures for conducting conformity assessment activities in relation to high-risk AI systems within the claimed scope reviewed?                           | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                                        | <input type="checkbox"/> No  |           |
|                                                                                                                                                                        | <input type="checkbox"/> N/A |           |
| Procedures take adequate account of the size of the AI provider, the sector of operation, the organizational structure, and the degree of complexity of the AI system? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                                        | <input type="checkbox"/> No  |           |
|                                                                                                                                                                        | <input type="checkbox"/> N/A |           |
| Procedures for issuing, suspending, and withdrawing conformity assessment certificates documented?                                                                     | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                                        | <input type="checkbox"/> No  |           |
|                                                                                                                                                                        | <input type="checkbox"/> N/A |           |
|                                                                                                                                                                        | <input type="checkbox"/> Yes | Comments: |

|                                                                                            |                              |  |
|--------------------------------------------------------------------------------------------|------------------------------|--|
| Are record-keeping procedures adequate to ensure traceability of all assessment decisions? | <input type="checkbox"/> No  |  |
|                                                                                            | <input type="checkbox"/> N/A |  |

### F.6.3 Cybersecurity Measures

|                       | Cybersecurity Measures                                                                     |                                              |                                         |
|-----------------------|--------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
| Verification Item     | Evidence that cybersecurity is taken into account during conformity assessment activities. |                                              |                                         |
| Proof                 | <input type="checkbox"/> Provided                                                          | <input type="checkbox"/> Not provided        | <input type="checkbox"/> Incomplete     |
| Comments on proof     |                                                                                            |                                              |                                         |
| Status                | <input type="checkbox"/> Satisfactory                                                      | <input type="checkbox"/> Partially completed | <input type="checkbox"/> Unsatisfactory |
| Comment / Findings    |                                                                                            |                                              |                                         |
| Date of establishment |                                                                                            |                                              |                                         |

| SPECIFIC REQUIREMENTS                                                                                           |                              |           |
|-----------------------------------------------------------------------------------------------------------------|------------------------------|-----------|
| Cybersecurity policy documented and reviewed?                                                                   | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                 | <input type="checkbox"/> No  |           |
|                                                                                                                 | <input type="checkbox"/> N/A |           |
| Information security measures in place to protect documentation and assessment data obtained from AI providers? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                 | <input type="checkbox"/> No  |           |
|                                                                                                                 | <input type="checkbox"/> N/A |           |
|                                                                                                                 | <input type="checkbox"/> Yes | Comments: |

|                                                                                                                                                       |                              |           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------|
| Access controls, data classification, and incident response procedures reviewed?                                                                      | <input type="checkbox"/> No  |           |
|                                                                                                                                                       | <input type="checkbox"/> N/A |           |
| Measures adequate given the sensitivity of technical documentation and datasets to which the laboratory may have access during conformity assessment? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                       | <input type="checkbox"/> No  |           |
|                                                                                                                                                       | <input type="checkbox"/> N/A |           |

F.7 PART VII- ASSESSMENT OF CONFIDENTIALITY OBLIGATIONS

Article 31(7) of the AI Act requires to have documented procedures ensuring that personnel, committees, subsidiaries, subcontractors, and any associated body or personnel of external bodies maintain the confidentiality of all information that comes into their possession during the performance of conformity assessment activities, except where disclosure is required by law. Staff must be obliged to observe professional secrecy in respect of all information obtained in carrying out their tasks, except in relation to the notifying authority of the Member State in which their activities are carried out.

|                       |                                                                                                                                                        |                                              |                                         |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
|                       | Assessment of Confidentiality Obligations                                                                                                              |                                              |                                         |
| Verification Item     | Evidence of compliance is demonstrated through confidentiality procedures and obligations ensuring protection of information and professional secrecy. |                                              |                                         |
| Proof                 | <input type="checkbox"/> Provided                                                                                                                      | <input type="checkbox"/> Not provided        | <input type="checkbox"/> Incomplete     |
| Comments on proof     |                                                                                                                                                        |                                              |                                         |
| Status                | <input type="checkbox"/> Satisfactory                                                                                                                  | <input type="checkbox"/> Partially completed | <input type="checkbox"/> Unsatisfactory |
| Comment / Findings    |                                                                                                                                                        |                                              |                                         |
| Date of establishment |                                                                                                                                                        |                                              |                                         |

SPECIFIC REQUIREMENTS

|                                                                                                                 |                              |           |
|-----------------------------------------------------------------------------------------------------------------|------------------------------|-----------|
| Documented confidentiality procedures reviewed?                                                                 | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                 | <input type="checkbox"/> No  |           |
|                                                                                                                 | <input type="checkbox"/> N/A |           |
| Confidentiality obligations extended in writing to all personnel, subcontractors, and external experts?         | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                 | <input type="checkbox"/> No  |           |
|                                                                                                                 | <input type="checkbox"/> N/A |           |
| Professional secrecy obligations included in employment contracts and subcontracting agreements?                | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                 | <input type="checkbox"/> No  |           |
|                                                                                                                 | <input type="checkbox"/> N/A |           |
| Exceptions to confidentiality limited to legally required disclosures and reporting to the notifying authority? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                 | <input type="checkbox"/> No  |           |
|                                                                                                                 | <input type="checkbox"/> N/A |           |
| Training on confidentiality obligations provided to relevant staff?                                             | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                 | <input type="checkbox"/> No  |           |
|                                                                                                                 | <input type="checkbox"/> N/A |           |

## F.8 PART VIII- ASSESSMENT OF LIABILITY INSURANCE

*Article 31(9) of the AI Act* requires to take out appropriate liability insurance for conformity assessment activities, unless liability is assumed by the Member State of establishment in accordance with national law, or that Member State is itself directly responsible for the conformity assessment.

|                       | Assessment of Liability Insurance                                                                                                                    |                                              |                                         |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
| Verification Item     | Evidence of compliance is demonstrated through appropriate liability insurance or equivalent state-assumed responsibility for assessment activities. |                                              |                                         |
| Proof                 | <input type="checkbox"/> Provided                                                                                                                    | <input type="checkbox"/> Not provided        | <input type="checkbox"/> Incomplete     |
| Comments on proof     |                                                                                                                                                      |                                              |                                         |
| Status                | <input type="checkbox"/> Satisfactory                                                                                                                | <input type="checkbox"/> Partially completed | <input type="checkbox"/> Unsatisfactory |
| Comment / Findings    |                                                                                                                                                      |                                              |                                         |
| Date of establishment |                                                                                                                                                      |                                              |                                         |

| SPECIFIC REQUIREMENTS                                                                                                                          |                              |           |
|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------|
| Evidence of appropriate liability insurance policy submitted and reviewed?                                                                     | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                | <input type="checkbox"/> No  |           |
|                                                                                                                                                | <input type="checkbox"/> N/A |           |
| Scope of insurance coverage assessed as adequate in relation to the conformity assessment activities within the claimed scope of notification? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                | <input type="checkbox"/> No  |           |
|                                                                                                                                                | <input type="checkbox"/> N/A |           |
| Validity period of current insurance policy:                                                                                                   |                              | Comments: |
|                                                                                                                                                |                              |           |
| Alternative: liability assumed by the Member State under national law, evidence provided?                                                      | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                                | <input type="checkbox"/> No  |           |

|  |                              |  |
|--|------------------------------|--|
|  | <input type="checkbox"/> N/A |  |
|--|------------------------------|--|

F.9 PART IX- ASSESSMENT OF PARTICIPATION IN COORDINATION AND STANDARDISATION

Article 31(12) of the AI Act requires to participate in coordination activities and to take part directly or indirectly in European standardization organizations, or to ensure awareness of and up-to-date knowledge in respect of relevant standards.

|                       |                                                                                                                                               |                                              |                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
|                       | Assessment of Participation in Coordination and Strandardisation                                                                              |                                              |                                         |
| Verification Item     | Evidence of compliance is demonstrated through participation in coordination activities and engagement with relevant standardization efforts. |                                              |                                         |
| Proof                 | <input type="checkbox"/> Provided                                                                                                             | <input type="checkbox"/> Not provided        | <input type="checkbox"/> Incomplete     |
| Comments on proof     |                                                                                                                                               |                                              |                                         |
| Status                | <input type="checkbox"/> Satisfactory                                                                                                         | <input type="checkbox"/> Partially completed | <input type="checkbox"/> Unsatisfactory |
| Comment / Findings    |                                                                                                                                               |                                              |                                         |
| Date of establishment |                                                                                                                                               |                                              |                                         |

| SPECIFIC REQUIREMENTS                                                                                                      |                              |           |
|----------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------|
| Evidence of participation in, or registration to participate in, the coordination activities established under Article 38? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                            | <input type="checkbox"/> No  |           |
|                                                                                                                            | <input type="checkbox"/> N/A |           |
| Participation in European standardization organizations (CEN, CENELEC, ETSI) or equivalent bodies documented?              | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                            | <input type="checkbox"/> No  |           |
|                                                                                                                            | <input type="checkbox"/> N/A |           |

|                                                                                                                                  |                              |           |
|----------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------|
| Procedures in place to monitor and incorporate updates to relevant harmonized standards applicable to high-risk AI systems?      | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                  | <input type="checkbox"/> No  |           |
|                                                                                                                                  | <input type="checkbox"/> N/A |           |
| Staff awareness of current relevant standards, including ISO/IEC standards applicable to AI and conformity assessment, assessed? | <input type="checkbox"/> Yes | Comments: |
|                                                                                                                                  | <input type="checkbox"/> No  |           |
|                                                                                                                                  | <input type="checkbox"/> N/A |           |

## F.10 PART X- OVERALL AUDIT FINDINGS AND SUMMARY TABLE

|                                                  | Status*                                                                           | Non-Conformities Identified |
|--------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------|
| Legal Status and Organizational Structure        | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |                             |
| Independence and impartiality                    | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |                             |
| Human resources and technical competence - AI    | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |                             |
| Human resources and technical competence - Data  | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |                             |
| Human resources and technical competence - Legal | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |                             |
| Management of external experts                   | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |                             |
| Quality management system                        | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |                             |
| Conformity assessment procedures                 | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |                             |
| Cybersecurity                                    | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |                             |
| Confidentiality                                  | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |                             |

|                                  |                                                                                   |  |
|----------------------------------|-----------------------------------------------------------------------------------|--|
| Liability insurance              | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |  |
| Coordination and standardization | <input type="checkbox"/> S <input type="checkbox"/> PS <input type="checkbox"/> U |  |

\* S = Satisfactory | PS = Partially Satisfactory | U= Unsatisfactory

|                                                    |  |
|----------------------------------------------------|--|
| Total number of major non-conformities identified: |  |
| Total number of minor non-conformities identified  |  |
| Total number of observations recorded:             |  |

## F.11 PART XI- NON-CONFORMITY REGISTER

For each non-conformity identified, the following record shall be completed:

| DISCREPANCY RECORD                  |                                |                                |
|-------------------------------------|--------------------------------|--------------------------------|
| Non-Conformity Reference (NC-[XXX]) |                                |                                |
| Classification                      | <input type="checkbox"/> Major | <input type="checkbox"/> Minor |
| Domain:                             |                                |                                |
| Applicable regulatory provision:    |                                |                                |
| Description of Findings             |                                |                                |

| ADOPTED ACTION PLAN (Provided by the Laboratory) |  |
|--------------------------------------------------|--|
| Findings of the Gap Analysis:                    |  |
| Roots Cause Analysis:                            |  |
| Corrective Action Required:                      |  |
| Deadline for corrective action:                  |  |
| Authorized Representative:                       |  |
| Date:                                            |  |

| REVIEW OF THE ACTION PLAN (by the auditor)                                                          |                              |                             |
|-----------------------------------------------------------------------------------------------------|------------------------------|-----------------------------|
| Relevance of the gap analysis, root cause analysis, proposed actions, and implementation timelines: | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| Comments:                                                                                           |                              |                             |
| Evaluator Name:                                                                                     |                              |                             |
| Date:                                                                                               |                              |                             |

**(Replicate as necessary for each non-conformity)**

## F.12 PART XII- NOTIFICATION RECOMMENDATION

Based on the assessment documented in this report, the audit team formulates the following recommendation to the NCA decision-making authority:

- ☐ **Notification recommended without conditions** - The laboratory satisfies all requirements of *Article 31 of Regulation (EU) 2024/1689* within the assessed scope. No non-conformities were identified. Notification may be granted.
- ☐ **Notification recommended subject to conditions** - The laboratory substantially satisfies the requirements of *Article 31* but presents minor non-conformities that must be resolved within the timeframe specified in Part XI. Notification may be granted subject to the laboratory submitting a satisfactory corrective action plan and completing all corrective actions within the specified deadline. A follow-up verification shall be conducted to confirm closure.
- ☐ **Notification deferred**- The laboratory presents major non-conformities that prevent Notification from being recommended at this time. The laboratory must address all major non-conformities identified in Part XI and submit documentary evidence of correction before a further assessment is conducted.
- ☐ **Notification refused** - The laboratory fails to satisfy fundamental requirements of *Article 31* that cannot be remedied within a reasonable timeframe or has demonstrated systemic deficiencies that preclude the granting of Notification.

In accordance with *Article 28(4)* of the AI Act, the decision on Notification shall be taken by competent persons of the NCA who are different from those who carried out the present assessment.

|                                                    |  |
|----------------------------------------------------|--|
| Scope of notification recommended (if applicable): |  |
| Proposed notification period:                      |  |
| Proposed next surveillance audit date:             |  |

## F.13 PART XIII- SIGNATURES AND VALIDATION

This report has been prepared and reviewed in accordance with the procedures of the NCA acting as notifying authority pursuant to *Article 28 of Regulation (EU) 2024/1689*. All information and documentation obtained

during this audit is subject to confidentiality obligations in accordance with *Article 78 of the AI Act* and *Article 28(6)* of the same Regulation.

|                                                                                    |  |
|------------------------------------------------------------------------------------|--|
| LEAD AUDITOR                                                                       |  |
| Name                                                                               |  |
| Signature                                                                          |  |
| Date                                                                               |  |
| TECHNICAL EXPERT #1                                                                |  |
| Name                                                                               |  |
| Title                                                                              |  |
| Signature                                                                          |  |
| Date                                                                               |  |
| TECHNICAL EXPERT #2                                                                |  |
| Name                                                                               |  |
| Title                                                                              |  |
| Signature                                                                          |  |
| Date                                                                               |  |
| TECHNICAL EXPERT #3                                                                |  |
| Name                                                                               |  |
| Title                                                                              |  |
| Signature                                                                          |  |
| Date                                                                               |  |
| Reviewed and validated by NCA decision-making authority (separate from audit team) |  |
| Name                                                                               |  |
| Title                                                                              |  |
| Signature                                                                          |  |

|                                                                                                                                      |  |
|--------------------------------------------------------------------------------------------------------------------------------------|--|
| Date                                                                                                                                 |  |
| <b>Acknowledgement by laboratory representative</b><br>I acknowledge receipt of this audit report and the findings contained therein |  |
| Name                                                                                                                                 |  |
| Title                                                                                                                                |  |
| Signature                                                                                                                            |  |
| Date                                                                                                                                 |  |

## G. ANNEX G- SURVEILLANCE AND COMPLAINT HANDLING

### G.1 PURPOSE OF THIS ANNEX

This Annex proposes elements for the monitoring of notified independent AI testing conformity assessment bodies.

This document does not define the rules and requirements for monitoring the notification process of such laboratories but proposes elements to help NCAs to go through or build this process.

National Competent Authorities if they are acting as notifying authority as defined in *article 28 of the EU AI Act* could follow it to enhance ongoing oversight of notified conformity assessment bodies and handling of complaints related to their activities. It supports the continuous monitoring obligations established under the EU AI Act, particularly those relating to notified conformity assessment bodies' continued compliance, operational integrity, and cooperation with notifying and market surveillance authorities.

The Annex covers two closely linked functions. First, surveillance, meaning the periodic monitoring of notified conformity assessment bodies after initial notification, including regular reviews, follow-up audits, review of corrective actions, and reassessment where significant changes occur.

Second, complaint handling, meaning the receipt, registration, investigation, resolution, and documentation of complaints concerning a conformity assessment body's competence, impartiality, performance, or compliance.

In line with the AI Act, the Annex proposes elements to ensure that notified conformity assessment bodies remain competent, independent, and capable of carrying out conformity assessment activities throughout the validity of their notification. It also provides a structured mechanism for NCAs to respond to where concerns are raised by providers, users, public authorities, or other stakeholders. The annex proposes minimum expectations for complaint intake, confidentiality, impartial investigation, escalation of serious findings, corrective action tracking, and reporting to the relevant authority where necessary.

### G.2 NOTIFICATION MONITORING, SURVEILLANCE AND COMPLAINT HANDLING

#### G.2.1 Regulatory Basis and Purpose of ongoing surveillance

The notification of a conformity assessment body is not a one-time event but an ongoing relationship between the National Competent Authority (NCA) and the notified entity. The AI Act establishes a continuous monitoring obligation that persists throughout the entire notification period, derived from *Article 28(1) of Regulation (EU) 2024/1689*, which requires each Member State to designate or establish at least one notifying authority responsible not only for initial assessment and designation but also for ongoing monitoring.

The NCA ensures that the conformity assessment body continues to always meet all notification criteria. The notification of a conformity assessment body does not confer a permanent status immune from review; it creates an ongoing obligation on the part of the notified entity to remain in continuous compliance, and a corresponding obligation on the NCA to verify that this compliance is maintained. This monitoring obligation is of particular significance in the context of AI evaluation conformity assessment bodies, given the pace at which AI technology evolves, the continuous development of new evaluation methodologies, and the possibility that technical competence, independence, or operational capacity may change over time. It is also the responsibility of the notified organization itself to ensure that its accreditation is maintained by the NAB and to inform the NCA in the event of non-compliance.

According to *Article 36 (1) of the EU AI Act*, the NCA shall notify the Commission and the other Member States of any relevant changes to the notification of a notified body via the electronic notification tool developed and managed by the Commission.

## G.2.2 Periodic surveillance audits

The primary instrument of ongoing surveillance is the periodic surveillance audit, conducted by the NCA at regular intervals. The purpose is to verify that the conformity assessment body continues to satisfy all applicable requirements, including legal status, organizational structure, independence, impartiality, technical competence, quality management, cybersecurity, confidentiality, and liability insurance, and that no material changes have occurred since the most recent audit.

The EU AI Act does not define a frequency for the monitoring of notified conformity assessment body. Usually audit frequency is determined in a risk-based approach, considering:

- The complexity and sensitivity of the conformity assessment activities within the notified scope.
- The track record of the conformity assessment body in previous audits.
- Any changes in organizational structure or personnel.
- Any complaints received in relation to the entity's activities.
- Any incidents or concerns brought to the NCA's attention through other means.

As a baseline, periodic surveillance audits should be conducted at least once every twelve months for conformity assessment bodies notified in particularly sensitive domains ( the classification follows Annex III categories ), and at least once every eighteen months for those in less sensitive domains. These intervals may be shortened at any time where the NCA identifies grounds for concern or following any significant change in circumstances.

A notification audit report prepared by the NCA indicates whether the conformity assessment body meets the designation criteria and obligations. The findings of each surveillance audit are recorded and form part of the evidence base for maintaining the notification and any subsequent renewal decision.

## G.2.3 Monitoring of changes notified

In addition to periodic audits, the surveillance framework relies on the notified entity's own duty to notify the NCA of any material changes that may affect its compliance

### G.2.3.1 Extension of the Scope of Notification

In case of extensions of the scope of the notification, the initial notification procedures laid down in *Articles 29 and 30 of the EU AI Act* shall start again.

### G.2.3.2 Cease of Conformity assessment activities

According to *Article 36 (3) of the EU AI Act*, where a notified body decides to cease its conformity assessment activities, it shall inform the notifying authority and the providers concerned as soon as possible and, in the case of a planned cessation, at least one year before ceasing its activities.

The certificates of the notified body may remain valid for a period of nine months after cessation of the notified body's activities, on condition that another notified body has confirmed in writing that it will assume responsibilities for the high-risk AI systems covered by those certificates.

The latter notified body shall complete a full assessment of the high-risk AI systems affected by the end of that nine-month-period before issuing new certificates for those systems. Where the notified body has ceased its activity, the notifying authority shall withdraw the designation.

### G.2.3.3 Other Cases

In addition to the cases already framed by the EU AI Act, the NCA could lay down rules to enforce notified conformity assessment body to inform the NCA without undue delay of any of the following:

- Changes to legal status or ownership structure.
- Changes to top-level management.
- Changes to personnel responsible for assessment activities, where such changes affect technical competence in areas within the notified scope.
- Loss of competences or tools that influence results of evaluation activities.

- Acquisition of any financial interest in a provider operating within the notified scope.
- Commencement of any consultancy or advisory activity that could conflict with independence.
- Any significant change to the quality management system.
- Any cybersecurity incident that may have affected the confidentiality of the information held.
- Any circumstance that could give rise to a conflict of interest.

Upon receipt of such a notification, the NCA assesses whether the change requires an immediate extraordinary audit, a targeted verification activity, a modification of the notified scope, or a suspension or withdrawal of notification.

In addition of the control triggered by a change declared by the notified conformity assessment body, according to *article 36 (4) of the EU AI Act*, where a NCA has sufficient reason to consider that a notified conformity assessment body no longer meets the requirements relating to Notified Bodies (*Article 31 of the EU AI Act*), or that it is failing to fulfil its obligations, the NCA shall without delay investigate the matter with the utmost diligence. In that context, it shall inform the notified conformity assessment body concerned about the objections raised and give it the possibility to make its views known.

If the notifying authority comes to the conclusion that the notified body no longer meets the requirements laid down in *Article 31* or that it is failing to fulfil its obligations, it shall restrict, suspend or withdraw the designation as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations.

The assessment and action taken should be recorded and the NCA shall notify the Commission and the other Member States of any relevant changes to the notification of a notified body via the electronic notification tool developed and managed by the Commission.

## G.2.4 Deviation

During an audit or assessment when the NCA finds that a designation criterion or obligation is not complied with, a deviation is recorded.

### G.2.4.1 Classification of Deviations

NCA usually defines different levels of deviation. A deviation could be considered: critical gap or non-critical gap.

A deviation may be considered **critical** when it demonstrates that the conformity assessment body is unable to meet the designation criteria or reveals a fundamental deficiency affecting its ability to perform reliable conformity assessment activities. Such a deviation calls into question the validity and reliability of the assessment results or the body's ability to consistently provide competent, impartial, and independent conformity assessment services. Critical deviations may arise from deficiencies in technical competence, such as the absence of essential expertise, qualified personnel, or the tools necessary to perform assessment activities. They may also result from circumstances that compromise the conformity assessment body's impartiality or independence, including unmanaged conflicts of interest, inappropriate external influence, or organizational arrangements that undermine the objectivity and credibility of its assessment activities.

A deviation could be considered non-critical when it concerns a deviation whose outcome does not, or is not likely to, directly and immediately affect the quality of conformity assessment services. For example, there is a lack of formalized process to inform its employees about modification of internal documentation.

In cases where a situation meets the requirements but appears fragile and could, if left unchecked, lead to a deviation, the assessor identifies a point to monitor. These situations should be monitored during the n+1 assessment to ensure that they have not led to a critical or non-critical gap. A point to monitor is not a deviation, nor is it a situation where there is doubt that the assessment has been unable to resolve. Nor is it a recommendation.

If the same point is identified repeatedly the assessor should determine whether it has become a non-critical or critical deviation requiring formal corrective action. If the underlying situation has deteriorated, this should lead automatically to a deviation.

#### G.2.4.2 Required Response

When a deviation is recorded, the conformity assessment body should respond by providing:

- An analysis of the extent of the gap and its causes.
- Corrective actions to address the deviation across the identified extent and prevent recurrence.
- A schedule for the implementation of corrective actions, including the deadline for correction.
- Where applicable, palliative actions are to be implemented while corrective measures take full effect, ensuring continuity of notification. Subcontracting assessment activities to another approved centre is among the possible remedial actions.

If the conformity assessment body disputes the finding, it should provide information to support its analysis and convinces the NCA that the finding is not substantiated.

The CAB should define a time period from the date of approval of the deviation to propose an action plan validated by the NCA. This period does not include processing time by the NCA. After this deadline, without a validated action plan and without cancellation of the deviation sheet, the notification of the conformity assessment body will be no longer valid.

In the case of critical gap, according to *Article 36 (4) of the EU AI Act*, if the NCA comes to the conclusion that the notified conformity assessment body no longer meets the requirements or that it is failing to fulfil its obligations, it shall restrict, suspend or withdraw the notification as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. The NCA shall immediately inform the Commission and the other Member States accordingly.

#### G.2.5 Enhanced Monitoring

When a critical deviation is recorded and the associated action plan is validated by the NCA, the conformity assessment body is de facto placed under enhanced surveillance. It is then subject to reinforced monitoring by the NCA while the action plan is being implemented, to ensure the correct execution of corrective actions according to the set schedule, as well as the application of palliative actions.

If, at the end of the fixed schedule, the NCA considers that the causes leading to the deviation have not been corrected, the following actions may be taken:

- Extension of surveillance, conditional on the prior validation of a new action plan by the NCA.
- Restriction of the scope of the notification.
- Suspension of the notification.
- Withdrawal of the notification.

In addition to the action selected, according to *article 36 (5) of the EU AI Act*, where its notification has been suspended, restricted, or fully or partially withdrawn, the notified conformity assessment body shall inform the providers concerned within 10 days.

#### G.2.6 Extraordinary Audits

Beyond periodic surveillance audits and responses to changes notifications, the NCA may conduct an extraordinary audit at any time where it has grounds to consider that the conformity assessment body may no longer satisfy one or more applicable requirements. According to article 36(4), where a notifying authority has sufficient reason to consider that a notified body no longer meets the requirements laid down in Article 31, or that it is failing to fulfil its obligations, the notifying authority shall without delay investigate the matter with the utmost diligence. In that context, it shall inform the notified body concerned about the objections raised and give it the possibility to make its views known. An extraordinary audit is the opportunity for the NCA to fulfil its duty and for the evaluated conformity assessment body to defend itself.

Grounds for an extraordinary audit may include:

- A complaint received concerning the conformity assessment body's conduct or the quality of its activities.
- Information from another national authority or the AI Office indicating concerns.
- Findings from the NCA's review of conformity assessment certificates issued by the conformity assessment body.
- Publicly available information suggesting a change in the conformity assessment body's circumstances.
- Any other information giving the NCA reasonable grounds for concern.

Extraordinary audits are conducted with the same rigor as periodic surveillance audits. Where the conformity assessment body is notified in advance, the notification period should be kept as short as is consistent with allowing necessary logistical arrangements, to ensure the audit reflects the conformity assessment body's actual operational state.

### G.2.7 Restriction, Suspension or Withdrawal of designation

A restriction, suspension or withdrawal is pronounced by the NCA by means of a notification letter signed, potentially after consultation with the Certification Steering Committee<sup>3</sup>. Where a surveillance audit reveals non-compliance that is more serious, the NCA may suspend or restrict notification.

Grounds for suspension or restriction could include non-exhaustively:

- Insufficient activity within the scope of notification.
- Loss of accreditation.
- Failure to validate an action plan within the allotted time following a deviation, or failure to convince the NCA the deviation was not proven.
- Following a critical deviation sheet, no palliative action identified and no scope modification possible to allow continued activity.
- Following enhanced monitoring, the NCA considers the deviation still unresolved by the end of the scheduled period.

During the period of suspension, no new evaluation may be initiated. The NCA decides on a case-by-case basis whether results of projects under evaluation are considered. The NCA must also consider the implications for any conformity assessment activities already in progress or recently completed.

The duration of the suspension is defined in the notification letter and depends on the causes and the timetable for implementing corrective actions.

At the end of the suspension period if the gap is not filled or where deviation is fundamental and cannot be remedied, or where the conformity assessment body persistently fails to address deviations in successive audits, withdrawal is required.

According to *article 36 of the EU AI Act*, where notification of the Conformity assessment body has been suspended, restricted, or fully or partially withdrawn, the notified conformity assessment body shall inform the providers concerned within 10 days.

---

<sup>3</sup> **Certification Steering Committee (CSC):** A committee responsible for making impartial decisions regarding the granting, maintenance, suspension, withdrawal, or modification of notification based on the results of assessment activities.

In the event of the restriction, suspension or withdrawal of a designation, the NCA shall take appropriate steps to ensure that the files of the notified body concerned are kept, and to make them available to notifying authorities in other Member States and to market surveillance authorities at their request.

In the event of the restriction, suspension or withdrawal of a designation, the NCA shall:

- a) assess the impact on the certificates issued by the notified conformity assessment body;
- b) submit a report on its findings to the Commission and the other Member States within three months of having notified the changes to the designation;
- c) require the notified conformity assessment body to suspend or withdraw, within a reasonable period of time determined by the authority, any certificates which were unduly issued, in order to ensure the continuing conformity of high-risk AI systems on the market;
- d) inform the Commission and the Member States about certificates' suspension or withdrawal of which it has required;
- e) provide other NCA of the Member State in which the provider has its registered place of business with all relevant information about the certificates of which it has required the suspension or withdrawal; that authority shall take the appropriate measures, where necessary, to avoid a potential risk to health, safety or fundamental rights.

### G.2.8 Renewal of Notification

Unless a conformity assessment body has notified the National Competent Authority (NCA) of its intention not to renew its notification, the renewal process may be initiated sufficiently in advance of the notification expiry date to allow adequate time for assessment and decision-making. As guidance, the NCA could request the renewal application several months before the expiry of the current notification, considering the complexity and scope of the conformity assessment body's activities.

The renewal assessment may be proportionate to the risks identified and the conformity assessment body's previous performance. Depending on the results of surveillance activities, significant organizational or technical changes, previous non-conformities, or changes in the scope of notification, the NCA may perform either a targeted reassessment focusing on selected areas or a more comprehensive reassessment equivalent to an initial designation assessment.

The renewal process may include a review of the conformity assessment body's continued compliance with the applicable designation criteria, including its technical competence, impartiality, independence, personnel qualifications, quality management system, technical resources, and implementation of corrective actions arising from previous assessments.

Where the NCA concludes that the applicable conditions continue to be met, a new notification may be issued for the applicable validity period.

If the renewal assessment cannot be completed before the expiry of the current notification, the NCA should determine how ongoing conformity assessment activities will be managed in accordance with its national procedures. This may include allowing the completion of evaluations already in progress, suspending the acceptance of new assessment activities until a decision has been reached, or applying other transitional measures to ensure continuity while maintaining confidence in the conformity assessment process.

### G.2.9 Complaint Handling

A formal complaint handling procedure is maintained by the NCA, enabling any natural or legal person to raise concerns regarding the conduct, competence, independence, or impartiality of a notified conformity assessment body. In accordance with Article 85 of the AI Act, any natural or legal person who has grounds to consider that there has been an infringement of the Regulation has the right to lodge a complaint with the relevant competent authority. The NCA should ensure that such complaints are duly assessed, investigated where appropriate, and taken into account as part of its surveillance and oversight activities.

Complaints may be submitted by:

- AI providers whose systems have been assessed and who have concerns about the conduct of the assessment.
- Deployers or users of AI systems with concerns about the reliability of a conformity assessment certificate.
- Competitors with concerns about compliance with independence or impartiality requirements.
- Civil society organizations or fundamental rights bodies with concerns about the quality or rigor of assessments in sensitive domains.
- Any other natural or legal person with a legitimate interest.
- EU Commission.

#### G.2.9.1 Processing of Complaints

Upon receipt of a complaint, the NCA should assign a unique reference number, acknowledge receipt to the complainant within a defined period, and conduct a preliminary admissibility assessment to determine whether the complaint falls within the NCA's supervisory responsibilities, contains sufficient information to warrant investigation, and is not manifestly unfounded.

Admissible complaints are investigated through a process that may include a request for information from the conformity assessment body, a targeted documentary review, an extraordinary audit, or a combination thereof, depending on the nature and seriousness of the concerns. The complainant is kept informed of progress and is notified of the outcome in writing, with a reasoned explanation of findings and any action taken. All complaints and their outcomes are recorded in the conformity assessment body's notification file and considered in planning subsequent surveillance audits.

All information obtained during complaint investigations is subject to the confidentiality obligations under *Article 78 of the AI Act*. The NCA ensures appropriate data handling arrangements are in place to protect complainant confidentiality, particularly where disclosure to the conformity assessment body under investigation could expose the complainant to adverse consequences.

#### G.2.10 Coordination with the AI Office and other National Authorities

The surveillance of notified conformity assessment bodies does not take place in isolation. Where concerns arise about the quality or reliability of conformity assessment activities in relation to AI systems also subject to the supervisory responsibilities of the AI Office, in particular systems built upon general-purpose AI models, the NCA should share relevant information with the AI Office and cooperate in any joint assessment or investigation.

Similarly, where the NCA identifies concerns that may be relevant to the activities of conformity assessment bodies in other Member States, for example where the conformity assessment body has conducted assessments of AI systems deployed across multiple Member States, or where the non-compliance identified may reflect a systemic issue affecting similar conformity assessment bodies in other jurisdictions, the NCA should communicate its findings to the relevant authorities of other Member States and to the Commission through applicable notification procedures. This cross-border dimension reflects the broader principle that the effective governance of AI systems in the Union requires consistent and coordinated action across national boundaries, and that the reliability of conformity assessment activities is a matter of common interest to all Member States.

## REFERENCES

- [1] European Parliament and Council of the European Union, “Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act),” *Official Journal of the European Union*, L 2024/1689, Jun. 2024. [Online]. Available: [Access EU AI Act \(Official Text\)](#)
- [2] European Parliament and Council of the European Union, “Regulation (EC) No 765/2008 of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products,” *Official Journal of the European Union*, vol. L 218, pp. 30–47, 2008. [Online]. Available: [Access Regulation \(EC\) No 765/2008](#)
- [3] European Union, “Artificial Intelligence Act – Article 9: Risk management system,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/9/>
- [4] European Union, “Artificial Intelligence Act – Article 10: Data and data governance,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/10/>
- [5] European Union, “Artificial Intelligence Act – Article 11: Technical documentation,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/11/>
- [6] European Union, “Artificial Intelligence Act – Article 12: Record-keeping,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/12/>
- [7] European Union, “Artificial Intelligence Act – Article 14: Human oversight,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/14/>
- [8] European Union, “Artificial Intelligence Act – Article 15: Accuracy, robustness and cybersecurity,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/15/>
- [9] European Union, “Artificial intelligence act – Article 78: Confidentiality,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/78/>
- [10] European Union, “Artificial Intelligence Act – Article 17: Quality management system,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/17/>
- [11] European Union, “Artificial Intelligence Act – Article 13: Transparency and provision of information to deployers,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/13/>
- [12] European Union, “Artificial Intelligence Act – Article 31: Requirements relating to notified bodies,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/31/>
- [13] European Union, “Artificial Intelligence Act – Article 33: Operational obligations of notified bodies,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/33/>
- [14] European Union, “Artificial Intelligence Act – Article 43: Conformity assessment,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/43/>
- [15] European Union, “Artificial Intelligence Act – Article 70: Obligations of market surveillance authorities,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/70/>
- [16] European Union, “Artificial Intelligence Act – Annex IV: Technical documentation referred to in Article 11,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/annex/4/>
- [17] European Union, “Artificial Intelligence Act – Annex VII: Conformity assessment based on assessment of the quality management system and assessment of the technical documentation,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/annex/7/>

- [18] *Artificial Intelligence Act – Article 28: Notifying authorities*, Artificial Intelligence Act EU, [online]. Available: <https://artificialintelligenceact.eu/article/28/>
- [19] *Artificial Intelligence Act – Article 32: Presumption of conformity of notified bodies*, Artificial Intelligence Act EU, [online]. Available: <https://artificialintelligenceact.eu/article/32/>
- [20] *Artificial Intelligence Act – Article 37: Challenge to the competence of notified bodies*, Artificial Intelligence Act EU, [online]. Available: <https://artificialintelligenceact.eu/article/37/>
- [21] *Artificial Intelligence Act – Article 38: Coordination of notified bodies*, Artificial Intelligence Act EU, [online]. Available: <https://artificialintelligenceact.eu/article/38/>
- [22] *Regulation (EU) 2024/... of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Article 6(1)*, European Union, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/6/>
- [23] *Regulation (EU) 2024/... of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Annex I*, European Union, 2024. [Online]. Available: <https://artificialintelligenceact.eu/annex/1/>
- [24] *Regulation (EU) 2024/... of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Annex III*, European Union, 2024. [Online]. Available: <https://artificialintelligenceact.eu/annex/3/>
- [25] *Regulation (EU) 2024/... of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Article 50*, European Union, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/50/>
- [26] *Regulation (EU) 2024/... of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Article 51*, European Union, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/51/>
- [27] European Union, “Artificial intelligence act – Article 72: Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/72/>
- [28] European Union, “Artificial intelligence act – Article 73: Reporting of serious incidents,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/73/>
- [29] European Union, “Artificial intelligence act – Article 74: Market surveillance and control of AI systems in the Union market,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/74/>
- [30] European Union, “Artificial intelligence act – Article 75,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/75/>
- [31] European Union, “Artificial intelligence act – Article 76: Supervision of testing in real world conditions by market surveillance authorities,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/76/>
- [32] European Union, “Artificial intelligence act – Article 77: Powers of authorities protecting fundamental rights,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/77/>
- [33] European Union, “Artificial intelligence act – Article 79: Procedure at national level for dealing with AI systems presenting a risk,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/79/>
- [34] European Union, “Artificial intelligence act – Article 80: Procedure for dealing with AI systems classified as non-high-risk under Annex III,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/80/>
- [35] European Union, “Artificial intelligence act – Article 81: Union safeguard procedure,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/81/>
- [36] European Union, “Artificial intelligence act – Article 82: Compliant AI systems which present a risk,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/82/>

- [37] European Union, “Artificial intelligence act – Article 83: Formal non-compliance,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/83/>
- [38] European Union, “Artificial intelligence act – Article 84: Union AI testing support structures,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/84/>
- [39] European Union, “Artificial intelligence act – Article 85: Right to lodge a complaint with a market surveillance authority,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/85/>
- [40] European Union, “Artificial intelligence act – Article 86: Right to explanation of individual decision-making,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/86/>
- [41] European Union, “Artificial intelligence act – Article 87: Reporting of infringements and protection of reporting persons,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/87/>
- [42] European Union, “Artificial intelligence act – Article 88: Enforcement of obligations for providers of general-purpose AI models,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/88/>
- [43] European Union, “Artificial intelligence act – Article 89: Monitoring actions,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/89/>
- [44] European Union, “Artificial intelligence act – Article 90: Alerts of systemic risks by the scientific panel,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/90/>
- [45] European Union, “Artificial intelligence act – Article 91: Power to request documentation and information,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/91/>
- [46] European Union, “Artificial intelligence act – Article 92: Power to conduct evaluations,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/92/>
- [47] European Union, “Artificial intelligence act – Article 93: Power to request measures,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/93/>
- [48] European Union, “Artificial intelligence act – Article 94: Procedural rights of economic operators of general-purpose AI models,” AI Act Explorer, 2024. [Online]. Available: <https://artificialintelligenceact.eu/article/94/>