ETSI TS 104 008 V1.1.1 (2026-01)

TECHNICAL SPECIFICATION

Methods for Testing & Specification (MTS); Continuous Auditing Based Conformity Assessment for AI-enabled systems

Reference
DTS/MTS-AI-00104008_ContAudit

Keywords
AI, assessment, conformity, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Executive summary 5
Introduction 6
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 7
3 Definition of terms, symbols and abbreviations 8
3.1 Terms 8
3.2 Symbols 9
3.3 Abbreviations 9
4 CABCA Motivation and Overview 10
4.1 Imperative of CABCA in AI System Assurance 10
4.2 Comparison of CABCA with Traditional Audit Processes 12
5 Fundamentals of CABCA 13
5.1 General 13
5.2 Mandatory Prerequisites for Implementing CABCA 15
5.2.1 General 15
5.2.2 Comprehensive Knowledge Base 15
5.2.3 Technical and Operational Expertise 16
5.2.4 Infrastructure and Methodological Framework 16
5.2.5 Risk Management and Stakeholder Engagement 16
5.3 Basic Assumptions of CABCA 16
5.3.1 General 16
5.3.2 AI System Heterogeneity and Dynamism 17
5.3.3 Universal Applicability and Transparency 17
5.3.4 Independence and Objectivity in Auditing 17
5.4 Principles of CABCA 17
5.4.1 General 17
5.4.2 Ongoing conformity 18
5.4.3 Stakeholder trust 18
5.4.4 Adaptability 18
6 Description of the CABCA Process Execution 18
6.1 General 18
6.2 Process Variations Based on CABCA Modes 20
6.2.1 Self-Assessment Path 20
6.2.2 Third-Party Assessment Path 20
6.2.3 Certification Path 21
6.3 Roles in Process Execution 21
6.3.1 General 21
6.3.2 Auditee 21
6.3.3 Auditing Party 22
6.3.4 Entity for Attestation of Conformity 23
7 Scoping (Identification of Conformity Specifications) 23
7.1 General 23
7.2 Sources and Integration Criteria for Conformity Specifications 23
7.2.1 Sources of Conformity Specifications 23
7.2.2 Criteria for Integrating Conformity Specifications in CABCA 24
8 Operationalization (Planning & Risk Assessment, Automation Setup) 25

8.1 Process of Operationalization 25
8.1.1 General 25
8.1.2 Identification of Quality Dimensions 26
8.1.2.1 Requirements for Defining Quality Dimensions 26
8.1.2.2 Criteria for Defining Quality Dimensions 26
8.1.3 Identification of Risks 26
8.1.3.1 Requirements for Defining Risks 26
8.1.3.2 Criteria for Identifying Risks 26
8.1.4 Deriving Measurable Compliance Requirements and Metrics 27
8.1.4.1 Requirements for Deriving Measurable Compliance Requirements and Metrics 27
8.1.4.2 Criteria for Deriving Measurable Compliance Requirements 27
8.1.4.3 Criteria for Deriving Metrics 27
8.1.5 Implementing Measurements 28
8.1.5.1 Requirements for Implementing Measurements 28
8.1.5.2 Criteria for Implementing Measurements 28
8.2 The Operationalization Specification 28
8.2.1 General 28
8.2.2 Requirements for the Operationalization Specification 29
8.2.3 Criteria for the Operationalization Specification 29

9 Continuous Assessment Process 30
9.1 Continuous Evidence Gathering & Measurement 30
9.2 Assessment Evidence 31
9.2.1 General 31
9.2.2 Sources of Evidence During Development and Training 31
9.2.3 Sources of Evidence During Operation 32
9.3 Persistence of Assessment Results 32
9.4 Updating Conformity Status 33
9.4.1 Conformity Status Updates 33
9.4.2 Transparency in Reporting and Updates 33
9.4.3 Effective Communication with Stakeholders 33
9.4.4 Building and Maintaining Stakeholder Trust 34

10 Documentation of the CABCA Process and its Outcome 34
10.1 General 34
10.2 CABCA Documentation Items 34
10.2.1 General 34
10.2.2 Conformity Specification 35
10.2.3 Operationalization Specification 35
10.2.4 Measurement Results and Evidence 35
10.3 Traceability and Consistency 35
10.4 Stakeholder Documentation Profiles 36

Annex A (informative): Examples 37

A.1 General 37

A.2 PII Leakage Control for a Support Ticket Assistant 37
A.2.1 Use Case Description 37
A.2.2 CABCA Implementation Example 37
A.2.2.1 General 37
A.2.2.2 Scoping and Operationalization Specification 37
A.2.2.3 Continuous Assessment Report 39

A.3 Use Case: Data Drift Monitoring for Demand Forecasting 40
A.3.1 Use Case Description 40
A.3.2 CABCA Implementation Example 40
A.3.2.1 General 40
A.3.2.2 Scoping and Operationalization Specification 40
A.3.2.3 Continuous Assessment Report 42
History 44

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Methods for Testing and Specification (MTS).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document specifies the key aspects of Continuous Auditing-Based Conformity Assessment (CABCA) to ensure that AI-enabled systems maintain conformity with evolving standards and regulations throughout their lifecycle. CABCA enables automated, continuous assessment and reporting of AI system compliance, addressing the limitations of traditional point-in-time audits.

Introduction

Artificial Intelligence (AI) systems are increasingly deployed in critical domains, where their compliance with regulations, standards, and ethical guidelines should be continuously assured. The dynamic and adaptive nature of AI, coupled with stringent requirements under frameworks like the EU Artificial Intelligence Act, creates a need for robust, continuous assessment methodologies. CABCA addresses this need by introducing a structured approach to ongoing auditing, replacing static, periodic evaluations with automated, real-time conformity checks. The present document outlines the principles, prerequisites, processes and documentation practices for implementing CABCA within organizations. It emphasizes stakeholder trust, adaptability, and transparency as core principles for sustainable AI assurance. By operationalizing high-level requirements into measurable metrics and continuous evidence collection, CABCA enables organizations to demonstrate reliable and verifiable AI system conformity throughout the entire lifecycle.

1 Scope

The present document specifies the key aspects of Continuous Auditing-Based Conformity Assessment (CABCA) as an audit methodology to evaluate and assess an AI system's conformity to relevant standards and regulations in a continuous manner. The present document applies to all types of organizations involved in the quality management of any of the lifecycle stages of AI systems as well as to any AI stakeholder roles.

The present document specifies:

- Principles underlying CABCA, including independence, reliability, stakeholder trust and transparency.
- CABCA assessment process, covering architecture, roles and procedures.
- Outcome of the assessments, including the issuance or revocation of conformity status.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] ISO/IEC 42001:2023: "Information technology — Artificial intelligence — Management system".

[2] ISO 19011:2018: "Guidelines for auditing management systems" (Edition 3, 2018).

[3] ISO 9001:2015: "Quality management systems — Requirements" (Edition 5, 2015).

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] P. Pfeiffer et al.: "Towards a Standard Process enabling AI-support for Safety and Conformity of Medical Devices", 2022.

[i.2] J. Mökander et al.: "Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation", Minds and Machines, vol. 32, pp. 241-268, 2022.

[i.3] L. Floridi et al.: "capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act", SSRN Electronic Journal, 2022.

[i.4] C. A. Sánchez: "Role of Measurement in Conformity Assessment", in Handbook of Quality System, Accreditation and Conformity Assessment, Springer, 2024.

[i.5] T. Granlund et al.: "On Medical Device Software CE Compliance and Conformity Assessment", arXiv preprint arXiv:2103.06815, 2021.

[i.6] ETSI TR 103 910: "Methods for Testing and Specification (MTS); AI Testing; Test Methodology and Test Specification for ML-based Systems".

[i.7] K. Lam et al.: "A Framework for Assurance Audits of Algorithmic Systems", in Proc. ACM FAccT '24, 2024.

[i.8] National Institute of Standards and Technology (NIST): "Artificial Intelligence Risk Management Framework (AI RMF 1.0)", NIST AI 100-1, 2023.

[i.9] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[i.10] High-Level Expert Group on AI: "Ethics guidelines for trustworthy AI", European Commission, Apr. 8, 2019.

[i.11] ETSI TR 104 119: "Methods for Testing & Specification (MTS); AI Testing; Guidelines for Documentation of AI-enabled Systems".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

AI - risk management frameworks: guidelines and best practices for identifying, assessing, and mitigating risks associated with Artificial Intelligence (AI) systems, such as machine learning models, to ensure their safe and responsible use

AI system: machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions

AI system lifecycle: entire sequence of activities relating to an AI system, from its initial ideation, requirements gathering, and design, through its development, deployment, operation, monitoring and eventual decommissioning

assessment engine: software component that automates the evaluation of collected artifacts against predefined quality criteria to generate quality assessment outcomes

assessment report: document providing detailed information on the AI System's compliance status

NOTE: The assessment report involves regularly updating stakeholders by mapping measurement results to specific requirements categorized under relevant quality dimensions, ensuring transparency and building trust in the adherence to relevant standards and regulations.

conformity assessment: process of evaluating and determining whether a product, service, or system complies with specified requirements, such as standards or regulations

conformity specification: foundational document outlining the required standards and guidelines, originating from sources like international bodies, national standards, industry guidelines, internal policies, and legislative requirements, to ensure systems meet the necessary compliance criteria

continuous assessment: automated collection and evaluation of measurement results against predefined metric thresholds operating in a continuous manner

continuous auditing: ongoing process of collecting, analysing, and reporting audit-related information, typically conducted in real-time or near-real-time, to provide stakeholders with timely insights into an organization's operations and compliance status

metrics and measurements: set of defined parameters and established quantification methods assigned to requirements in CABCA

NOTE: These are crucial for the auditable and applicable framework provided by CABCA for continuous assessment.

ML life cycle: technical process that is a subset of the broader AI System Lifecycle, comprising the stages of data preparation, model engineering, evaluation, and deployment, which culminate in the creation and operationalization of a model

MLOps: set of practices and methodologies for managing the lifecycle of Machine Learning (ML) models, including development, deployment and maintenance

model: technical component or representation of learned knowledge within an AI system, such as a neural network or a foundation model, derived from a machine learning process

operationalization: process in CABCA of translating high-level Conformity Specifications into actionable steps and machine-readable metrics

NOTE: This process includes the documentation of operational decisions and the setup of automated assessments.

operationalization specification: specification that ensures the proper instantiation of the CABCA measurement and evidence collection system

quality dimensions: fundamental aspects in CABCA used to assess AI compliance, including accuracy, robustness, avoidance of unwanted bias, accountability, privacy and security

NOTE: Each dimension is broken down into specific, manageable components for precise auditing.

risk traceability: capability in CABCA ensuring that each risk mitigation action is linked back to its original risk and source specification, maintaining clarity and accountability

stakeholder: individual, group, or organization that has an interest or concern in an AI system

NOTE: Stakeholders can affect or be affected by the AI system's actions, objectives, and policies.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AI	Artificial Intelligence
API	Application Programming Interface
CABCA	Continuous Auditing-Based Conformity Assessment
CE	Conformité Européenne
ER	Entity-Relationship
ESO	European Standardization Organization
GDPR	General Data Protection Regulation
HEN	Harmonised European Standard
HIPAA	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MIL	Military
ML	Machine Learning
MLOp	Machine Learning Operations
NER	Named Entity Recognition

NIST	National Institute of Standards and Technology
QMS	Quality Management System
STD	Standard
TD	Technical Documentation
UL	Underwriters Laboratories

4 CABCA Motivation and Overview

4.1 Imperative of CABCA in AI System Assurance

The European Union's Artificial Intelligence Act (EU AI Act) [i.9] establishes comprehensive obligations for providers of high-risk AI systems, encompassing critical areas such as risk management (Art. 9), technical documentation (Art. 11), quality management (Art. 17), conformity assessment (Art. 43), the EU Declaration of Conformity (Art. 47), and post-market monitoring (Art. 72) [1], [i.2], [i.3]. These requirements form a tightly interlinked compliance framework demanding sustained conformity throughout the AI system's lifecycle. Satisfying these legal obligations effectively, especially at scale and given the dynamic nature of AI, necessitates an operational framework capable of translating legal specifications into verifiable, continuously monitored processes. This regulatory imperative creates a distinct demand for methodologies that can manage this complexity and ensure ongoing compliance, moving beyond traditional static assessments.

This need is driven significantly by regulations like the EU AI Act, which places organizations, including stakeholders like manufacturers, vendors, and providers, under increasing pressure to ensure their AI systems meet stringent quality and compliance standards. This necessity stems from a broad spectrum of stakeholders, including regulators, customers, and society at large, who demand assurance that AI systems are accurate, robust, fair, secure, and respect privacy [i.2], [i.3]. The challenge, however, lies in translating these high-level, often abstract, requirements into tangible and measurable attributes that can be assessed continuously throughout the AI system's lifecycle [i.1], [i.4]. Such assessment criteria are required by the European Standardisation Request on AI to underpin the European legislation on AI.

This is where CABCA emerges as a methodology, directly addressing the unique needs required by regulations like the EU AI Act and the inherent challenges of AI system assurance. CABCA addresses the specific needs of AI system operators in terms of quality management by operationalizing conformity in a manner distinct from traditional process-oriented management systems while also providing assurance for regulators, customers, and society. Whereas quality management systems that ensure compliance of AI systems address the broad processes of AI development, deployment, upkeep, and governance, CABCA targets the specificities of AI systems themselves. For this, CABCA defines how to translate high-level requirements (like those in the AI Act and related standards) into actionable metrics, ensuring that abstract standards become tangible and assessable [i.1], [i.5]. Moreover, the inherent dynamic nature of AI systems, characterized by frequent updates to models and changes in data sources - aspects directly relevant to the Act's post-market monitoring requirements (Art. 72) - demands a continuous conformity assessment methodology [i.3], [i.4]. CABCA rises to this challenge by supporting ongoing reassessment, thus ensuring that AI systems consistently align with evolving standards and regulations like the EU AI Act, enhancing their compliance and reliability over time for the benefit of all stakeholders. It is important to state that CABCA's specific continuous assessment approach is proposed as a method to effectively meet the Act's intent, particularly given the dynamic nature of AI, rather than being an explicitly mandated mechanism itself. However, this approach is forward-looking, anticipating that future harmonised standards will likely require continuous assessment to ensure ongoing compliance.

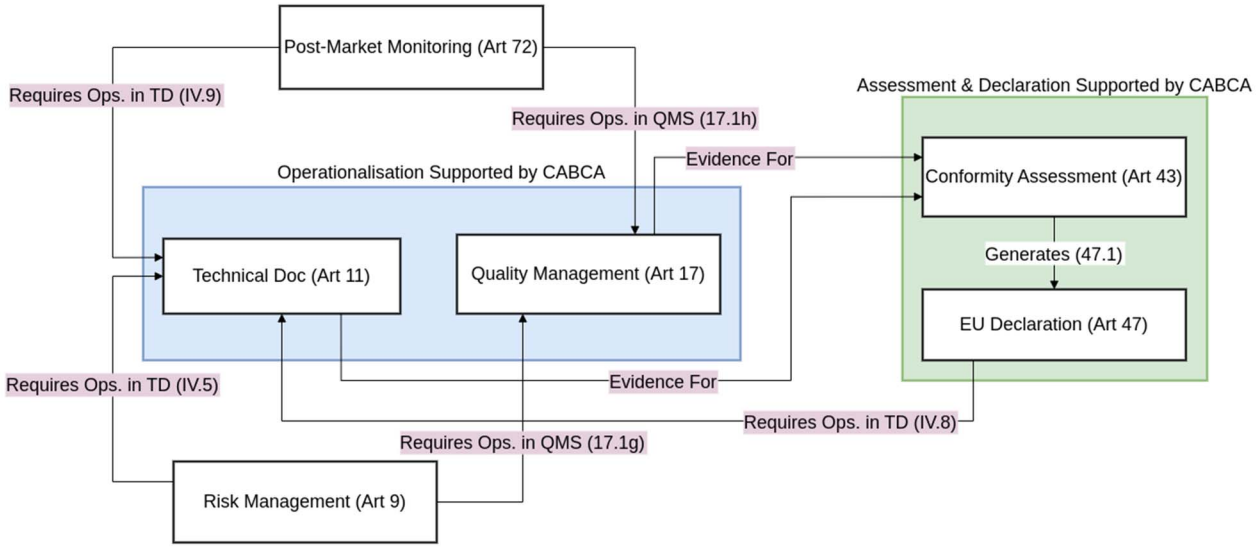

Figure 4.1-1: EU-AI Acts mapping to CABCA

The interrelationship between these key articles and CABCA's supporting role is illustrated in Figure 4.1-1, which details the interconnected compliance workflow for high-risk AI systems under the EU AI Act. The figure explains how foundational obligations are translated into operational evidence for formal assessment and declaration. The process begins with the core provider obligations of establishing a Risk Management (Art. 9) system and a Post-Market Monitoring (Art. 72) plan. These are not standalone activities; they should be integrated into the provider's operational framework. The arrows show this operationalization:

- The procedures, plans and results of these activities should be formally 'Documented in TD (Annex IV.5/IV.9)'. The Technical Documentation (TD) serves as the central repository of evidence about the AI system itself, detailing its design, capabilities, and the specific risk and monitoring measures applied to it.
- Simultaneously, the processes for conducting risk management and post-market monitoring should be 'Included in QMS (Art. 17(1)(g/h))'. This ensures these activities are embedded within the provider's organizational Quality Management System (QMS), demonstrating a systematic, repeatable and managed approach to compliance.

Together, the Technical Documentation (Art. 11, Annex IV) and the Quality Management System (Art. 17) form the comprehensive body of proof that serves as 'Evidence For' the Conformity Assessment (Art. 43 / Annex VII). During this assessment, an auditor evaluates this evidence to verify that the provider's claims of compliance are substantiated. Following a successful assessment, the provider 'Generates (47.1)' the formal EU Declaration of Conformity (Art 47). To close the evidence loop, a 'Copy kept in TD (Annex IV.8)' ensures this final declaration is included in the system's official documentation.

CABCA is designed to directly support the 'Operationalization' (blue) and 'Assessment & Declaration' (green) phases. It provides the structured methodology to translate abstract legal requirements into measurable controls and to continuously generate the verifiable, up-to-date evidence that populates the TD and QMS, thereby enabling a robust and manageable compliance lifecycle.

4.2 Comparison of CABCA with Traditional Audit Processes

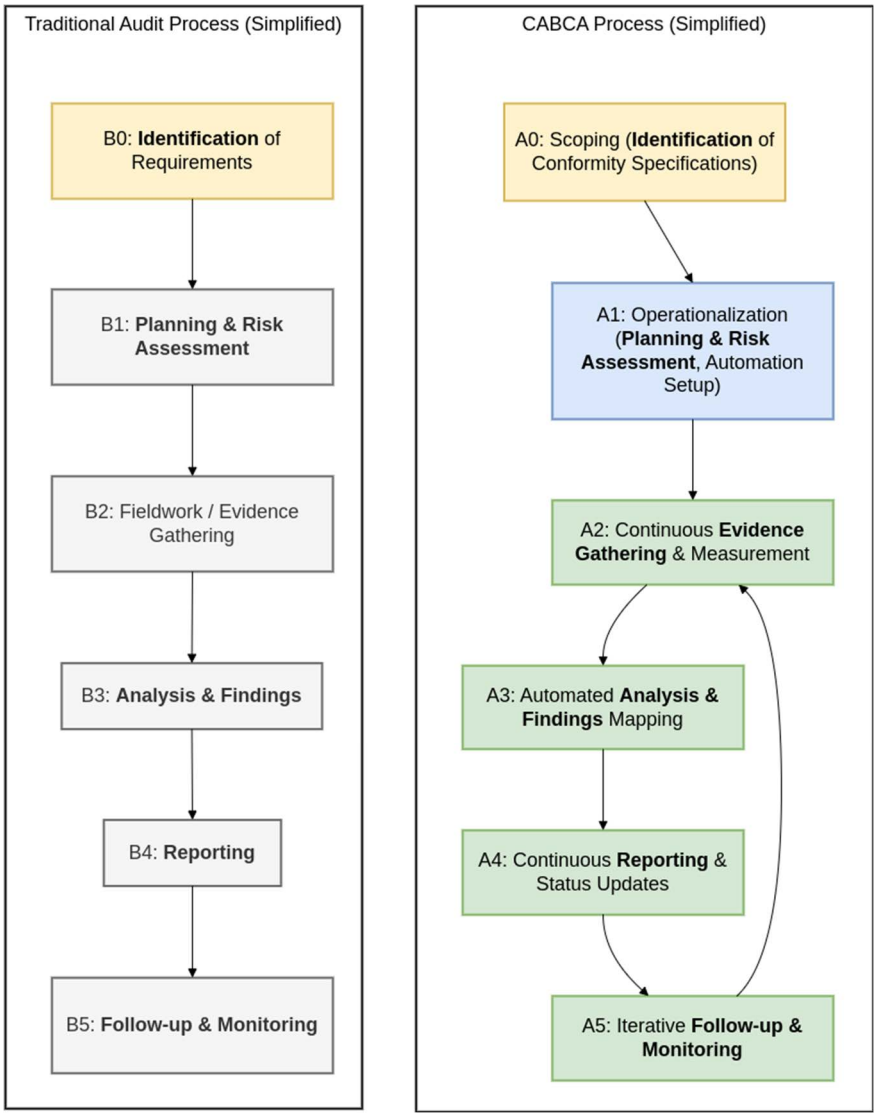

Figure 4.2-1: CABCA comparison to a traditional audit

While CABCA serves the fundamental audit objective of evaluating conformity against requirements, its operational structure differs significantly from a traditional generic audit process, such as one guided by ISO 19011:2018 [2]. The simplified process flows illustrated in Figure 4.2-1 highlights these key distinctions. In the CABCA framework, A0 Scoping is a standing organizational activity that produces a formal Conformity Specification prior to any CABCA run, whereas B0 Identification of Requirements belongs to a single traditional audit engagement and is performed once per audit as part of audit planning. The CABCA process is color-coded: the 'Scoping' phase (A0) is highlighted in yellow, the 'Operationalization' phase (A1) is highlighted in blue, while the continuous 'Assessment' cycle (A2-A5) is highlighted in green. The differences between the classic process and CABCA are described below, based on the structure of the classic process:

1) **Identifications of Requirements:** Both processes begin with determining the applicable requirements. In a traditional audit, this is the 'Identification of Requirements' (B0), a foundational activity performed as part of the initial audit planning to establish the audit criteria. In contrast, 'Scoping' (A0) is treated as a prerequisite governance activity that occurs within an organization before the CABCA methodology is implemented. The explicit output of this scoping phase - a formal Conformity Specification - is then used as the mandatory input for the first active CABCA phase, Operationalization (A1), thereby establishing a clear and traceable foundation for automation.

2) **Planning & Risk Assessment:** In a traditional audit, this is typically a distinct upfront phase (B1), involving defining objectives, scope, criteria, and applying a risk-based approach to determine the audit strategy and plan (ISO 19011:2018 [2], clause 6.3 Preparing audit activities, clause 6.3.2 Audit planning, clause 6.3.3 Assigning work to audit team, clause 6.3.4 Preparing documented information for audit)). For CABCA, "Operationalization" (A1) incorporates this phase. It includes the essential Planning & Risk Assessment steps but extends them to translate requirements into detailed, machine-readable metrics and set up the automation framework (clause 5). This phase effectively configures the continuous assessment engine, integrating planning directly into the mechanism for execution.

3) **Fieldwork / Evidence Gathering:** The traditional audit involves "Fieldwork / Evidence Gathering" (B2), where auditors manually collect and verify information through interviews, observations, and document review during a specific period (ISO 19011:2018 [2], clause 6.4 Conducting audit activities, clause 6.4.2 Collecting and verifying information). CABCA's "Continuous Evidence Gathering & Measurement" (A2) is fundamentally different. It is an automated, ongoing process that collects data from system artifacts (clause 6.2) using programmed measurements, replacing periodic manual collection with continuous monitoring. Both approaches adhere to the principle of obtaining sufficient, appropriate audit evidence (ISO 19011:2018 [2], clause 4 Principles of auditing - Evidence-based approach).

4) **Analysis & Findings:** Traditional audits involve analysing collected evidence against audit criteria to generate Analysis & Findings (B3), often requiring auditor judgment (ISO 19011:2018 [2], clause 6.5 Generating audit findings, clause 6.5.1 Evaluating audit evidence, clause 6.5.2 Identifying and recording audit findings). In CABCA, the "Automated Analysis & Findings Mapping" (A3) performs this step programmatically. Measurement results are automatically compared against predefined thresholds from the operationalization phase (clause 6.1), and deviations are identified as findings, enabling rapid identification of nonconformity.

5) **Reporting:** Reporting (B4) in a traditional audit typically involves issuing a formal Assessment Report upon completion of the engagement (ISO 19011:2018 [2], clause 6.6 Completing audit, clause 6.6.1 Assessment Report). CABCA's "Continuous Reporting & Status Updates" (A4) provides more frequent communication. It focuses on providing dynamic conformity status updates and reports based on the continuous analysis (clause 6.1 and 6.4), reflecting the real-time nature of the assessment.

6) **Follow-up & Monitoring:** The traditional audit process includes a distinct " Follow-up & Monitoring" phase (B5) where actions taken to address findings are verified (ISO 19011:2018 [2], clause 6.7 Completing audit, implicitly part of programme management to verify action effectiveness). In CABCA, "Iterative Follow-up & Monitoring" (A5) is integrated into the continuous loop (A5 --> A2). A change in conformity status triggers the need for corrective action, and the effectiveness of these actions is verified through the next cycle of continuous measurement and analysis, rather than a separate follow-up activity.

In essence, CABCA adapts the core principles and phases outlined in standards like ISO 19011:2018 [2], but re-engineers them for a continuous, automated application specifically suited for the dynamic evaluation of AI systems and similar technologies.

5 Fundamentals of CABCA

5.1 General

CABCA is a dynamic methodology designed for the continuous assessment of an AI system's adherence to relevant requirements. CABCA implementation is established on a per-system basis, as this allows for the necessary specificity in auditing. However, the framework and the operationalization logic developed for one system can often be adapted and reused for other, similar AI systems within an organization, promoting efficiency and consistency. The requirements that CABCA assesses can originate from various sources, including:

a) requirements in regulations like the AI Act as well as sector-specific legislation;

b) requirements set by bodies from standardization worldwide like ISO, ETSI and CEN;

c) additional market rules or internal company policies; and

d) customer demands.

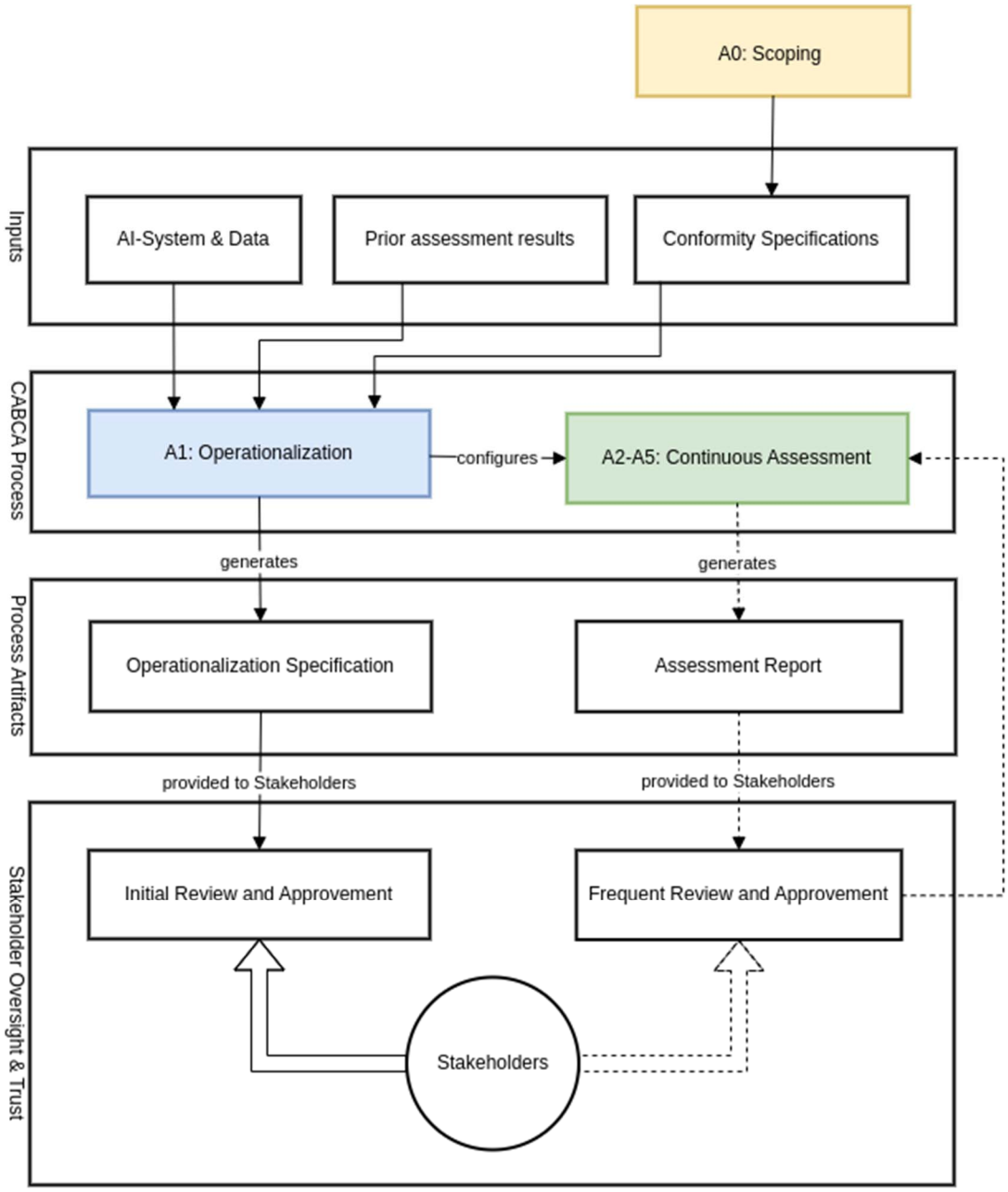

Figure 5.1-1: CABCA Process flow, for building Stakeholder Trust, showing initial setup (solid arrows) and frequent assessment (dashed arrows)

As illustrated in Figure 5.1-1, CABCA is structured to systematically generate and maintain stakeholder trust through transparent processes and verifiable artifacts. Distinct phases and actions of CABCA are visually differentiated by colors and arrow types. Inputs explicitly include prior assessment results (including corrective actions), data used by or produced from the AI system, and the measurement tools/methods configured for assessments (see clauses 7.2.1 and 8.1.5).

Foundational trust in the audit method is established through an initial setup process, indicated by solid arrows. This begins with the Inputs being fed into the "A1: Operationalization phase" (blue box). The key output of this foundational phase is the Operationalization Specification artifact. The present document, which details how conformity will be measured, is provided to Stakeholders for a formal Initial Review and Approvement, an action indicated by the double-lined arrow. This foundational approval process is conducted once at the start and is repeated only when significant changes are made to the AI-System, including its Data, or its Conformity Specifications. Prior assessment results also serve as an input to inform adaptations, ensuring that the audit method remains aligned and trusted.

Ongoing trust in the audit results is maintained through a frequent assessment cycle, indicated by dashed arrows. The approved A1 phase configures the "A2-A5: Continuous Assessment phases" (green box), which consists of Continuous Evidence Gathering & Measurement (A2), Automated Analysis & Findings Mapping (A3), Continuous Reporting & Status Updates (A4), and Iterative Follow-up & Monitoring (A5). These phases are triggered frequently. This phase generates a recurring "Assessment Report" that is provided for "Frequent Review and Approvement". To build trust, this report includes a clear conformity status, detailed findings mapped to specific requirements, and links to the underlying verifiable evidence, providing a transparent basis for the review process. The feedback from this recurring review informs the ongoing assessment cycle. By separating the foundational approval of the method from the frequent approval of the results, CABCA creates a robust and transparent framework for building and sustaining stakeholder confidence.

5.2 Mandatory Prerequisites for Implementing CABCA

5.2.1 General

Successful implementation and operation of the CABCA methodology shall be contingent upon the organization meeting specific mandatory prerequisites. These prerequisites represent the necessary input conditions and foundational capabilities required before CABCA can be effectively applied. They are distinct from the capabilities or outcomes facilitated by the CABCA process itself. Organizations intending to implement CABCA shall ensure the following requirements are met:

i) comprehensive knowledge base;

ii) technical and operational expertise;

iii) infrastructure and methodological framework; and

iv) risk management and stakeholder engagement.

These requirements are further explained in the following clauses.

5.2.2 Comprehensive Knowledge Base

Organizations shall possess and maintain a comprehensive knowledge base relevant to the AI systems under assessment, which shall include:

a) **Understanding of conformity requirements:** Organizations shall possess and maintain a deep and current understanding of the specific conformity requirements applicable to the AI systems. This understanding shall encompass relevant standards (e.g. ISO/IEC standards, including potentially relevant aspects from ISO/IEC 42001 [1] on AI management systems, and ETSI standards), regulations (e.g. the EU AI Act [i.9]), sector-specific rules, and ethical guidelines.

b) **Knowledge of standards and regulations linkage:** Familiarity with how international and regional standards relate to and support regulatory requirements. This capability shall support the correct interpretation and application of requirements, particularly when aiming for compliance via Harmonised European Standards (HEN).

c) **Understanding AI system risk classification:** The ability to correctly classify the organization's AI systems according to applicable regulatory frameworks (e.g. risk categories in the EU AI Act [i.9]: unacceptable, high, limited, minimal risk). This classification shall inform the scope, depth, and rigor of the CABCA implementation and associated risk management strategies.

d) **Synthesis of previous assessment results:** Consolidated learnings from prior system evaluations, including identified non-conformities and corrective actions, to inform subsequent requirements and measurements.

e) **AI literacy program:** An organization-wide AI literacy program for personnel involved in development, operation, assurance, and oversight of AI systems, proportionate to role and risk.

5.2.3 Technical and Operational Expertise

Organizations shall ensure they possess the necessary technical and operational expertise, including:

a) **Operationalization skills:** Demonstrated ability to translate high-level conformity specifications and requirements (from standards, regulations, and ethical guidelines) into specific, actionable, measurable, and machine-readable metrics suitable for continuous assessment within the CABCA framework. This shall involve expertise in both the AI domain and compliance/audit methodologies.

b) **AI-related technical expertise:** A thorough understanding of the design, development, deployment, and operational principles of the AI systems being assessed. This shall include in-depth knowledge of the algorithms employed, data management practices (including governance), model training and validation, and system architecture.

5.2.4 Infrastructure and Methodological Framework

Organizations shall have in place an adequate infrastructure and methodological framework, which shall include:

a) **Continuous monitoring infrastructure:** A robust and reliable technological infrastructure capable of supporting continuous monitoring, data collection, evidence processing, and automated analysis as required by CABCA.

b) **Awareness of auditing and compliance standards:** Organizational knowledge of established auditing processes and compliance standards relevant to technology systems and, where applicable, AI-specific assurance techniques (potentially referencing practices from ISO/IEC 42001 [1] or other relevant audit standards).

5.2.5 Risk Management and Stakeholder Engagement

Organizations shall demonstrate effective risk management and stakeholder engagement capabilities, including:

a) **Risk management proficiency:** Proficiency in identifying, assessing, and mitigating risks associated with AI systems, specifically tailored to the context of continuous auditing and conformity assessment as performed under CABCA.

b) **Stakeholder engagement strategy:** A defined approach for identifying relevant internal and external stakeholders, understanding their requirements and concerns related to AI conformity, and comprehending how CABCA outcomes impact them. This shall form the basis for effective communication and trust-building.

c) **Risk ownership:** Named owners are assigned for each assessed AI system with authority to allocate resources and accept/mitigate risks; ownership is recorded with the assessment status and persisted, see clause 9.3.

5.3 Basic Assumptions of CABCA

5.3.1 General

This clause describes the fundamental assumptions that underpin the CABCA framework that are also essential for quality management systems, including post-market monitoring and being in compliance with ISO 9001:2015 [3] - Quality management systems. These assumptions relate to the nature and characteristics of AI systems, the applicability and transparency of standards and regulations, and the independence and objectivity required in the auditing process.

5.3.2 AI System Heterogeneity and Dynamism

CABCA assumes that while AI systems vary widely in complexity, function, and application domain, they are subject to common, universal requirements. These requirements are often derived from high-level ethical principles, such as fairness, transparency, technical robustness, and accountability, which are foundational to ethical guidelines [i.10] and regulatory frameworks like the EU AI Act [i.9]. For instance, this could mean ensuring a hiring AI is free from gender bias (fairness), providing a clear rationale for a credit scoring decision (transparency), verifying that a self-driving system performs reliably in adverse weather conditions (technical robustness), and establishing a clear audit trail to address system-induced errors (accountability). This assumption acknowledges the diverse nature of AI systems while emphasizing a consistent approach to evaluating their adherence to fundamental requirements.

AI systems are dynamic, evolving over time due to data variability, algorithm updates, and operational environment changes. CABCA is adaptable to these evolutions by running frequent reassessment cycles that automatically collect fresh evidence, reevaluate metrics, and update the conformity status on a regular basis. These iterative cycles allow CABCA to adapt immediately to system changes, ensuring compliance remains current and thus trustworthy throughout the AI system's lifecycle.

5.3.3 Universal Applicability and Transparency

Building on the existence of common requirements, CABCA further assumes that the specific standards, regulations, and ethical guidelines selected for assessment can be consistently interpreted and practically operationalized (i.e. translated into measurable metrics and verifiable tests) for any type of AI system, ensuring the assessment framework's broad applicability.

Transparency and accountability are central to this approach. CABCA operationalizes these principles by continuously collecting and documenting evidence of system behaviour, decision logic, and performance metrics. This structured, traceable documentation, combined with automated reporting and clear mapping to compliance requirements, ensures that AI operations remain visible and auditable. As a result, CABCA enables stakeholders to understand, verify, and hold accountable both the AI systems and their operators for decisions and outcomes.

5.3.4 Independence and Objectivity in Auditing

The integrity and credibility of CABCA rely on maintaining independence and objectivity throughout the auditing process, whether internal or external. This is not only an assumption, but a fundamental requirement supported by several facets of the CABCA framework. Independence is fostered through several mechanisms. These include clearly defined roles (Auditee and Auditing Party, see clause 6.3), strict reliance on objective evidence derived from metrics and measurements (see clause 9.1), the option of third-party assessment modes (see clause 6.2), and the overall transparency of the process and its outcomes (see clauses 5.4.3 and 9.4.2).

Together, these mechanisms safeguard the impartiality of auditing and assessment under CABCA, thereby strengthening trust and reliability in the resulting conformity assessments. While stated here as a fundamental requirement, the specific implementation details of these mechanisms are elaborated in the referenced sections, including roles (clause 6.3), assessment modes (clause 6.2), evidence from measurements (clause 9.1), and transparent reporting (clause 9.4).

5.4 Principles of CABCA

5.4.1 General

CABCA is founded on three guiding principles: ongoing conformity, stakeholder trust, and adaptability [i.7], [i.8]. The rationale for their selection is as follows:

- Ongoing conformity was chosen to directly counter the limitations of traditional 'point-in-time' audits, which are inadequate for the dynamic nature of AI. Since AI systems evolve continuously with new data and model updates, this principle establishes the necessity of continuous assessment to ensure compliance is actively maintained throughout the system's lifecycle, not just verified at a single moment.

- Stakeholder's trust was selected because the complexity and societal impact of AI systems demand more than technical compliance; they require demonstrable trustworthiness. This principle mandates a transparent, verifiable, and communicative assessment process designed to build and maintain confidence among all stakeholders, including regulators, customers, and the public - which is crucial for the acceptance and responsible deployment of AI.
- Adaptability was included to ensure the long-term viability of the CABCA framework in a rapidly changing technological and regulatory landscape. This principle enables the methodology to evolve alongside new AI techniques, emerging risks, and updated standards, ensuring it remains relevant and effective without requiring fundamental redesign.

These principles offer distinct advantages over traditional periodic audits and self-assessment methods. They ensure a more standardized yet flexible approach to conformity assessment. Standardization is achieved through a common methodological framework and process, while flexibility is provided by the scoping and operationalization phases that adapt the assessment to specific systems and risks. These principles build confidence among stakeholders, provide an infrastructure for organizations to continually improve and adapt to new compliance challenges, and are central to maintaining transparency and demonstrating an ongoing commitment to quality and compliance.

5.4.2 Ongoing conformity

Traditional conformity assessment methodologies often offer a 'snapshot' of compliance at a particular moment in time. While this approach may suffice for static or slowly evolving systems, it is inadequate for rapidly changing environments, particularly in sectors like Machine Learning. CABCA shifts this paradigm by focusing on the continuous auditing of an organization's AI system's adherence to standards. This principle aligns closely with the core process of **Continuous Assessment**, which leverages real-time data for uninterrupted compliance status. This approach not only provides a more nuanced and current view of compliance but also integrates seamlessly with risk-based quality requirements and risk management strategies.

5.4.3 Stakeholder trust

Trust is a crucial element for any organization's success, especially in today's rapidly changing landscape. The CABCA methodology places a high value on transparency and open communication with stakeholders, which in turn fosters trust. As detailed in clause 5.1, CABCA achieves this by establishing foundational trust in the audit method itself when stakeholders review and approve the Operationalization Specification. This ensures the "how" of the assessment is agreed upon before it begins. Consistent and continuous auditing and reporting (as described in clause 9.1) keep stakeholders updated, enhancing awareness and understanding of the organization's compliance activities and status. This continuous flow of reliable information boosts confidence among stakeholders, allowing them to make well-informed decisions. This principle also incorporates the benefits of greater focus on stakeholder communication, ensuring that all parties involved have a clear understanding of the organization's commitment to maintaining ongoing compliance with relevant standards.

5.4.4 Adaptability

CABCA is designed for adaptability, enabling it to keep pace with changes in AI systems, emerging risks, and the external regulatory landscape. This principle is crucial for dynamically evolving systems like Machine Learning, where static auditing methods fall short. It is put into practice through the Operationalization process, which allows organizations to redefine the audit's scope and metrics in response to technological advancements or new regulations. This approach supports continuous improvement, ensuring that compliance processes remain effective over time.

6 Description of the CABCA Process Execution

6.1 General

The execution of a CABCA cycle involves several distinct phases, driven by specific triggers and resulting in a documented conformity status. The overall process flow, including variations based on the assessment mode, is visualised in Figure 6.1-1.

An assessment cycle can be considered a complete update of the conformity status, including measurement, evidence collection, and reporting. The process assumes that the initial Operationalization (A1) has been completed. As a result of this phase, the Operationalization Specification shall be available to configure the subsequent assessment steps.

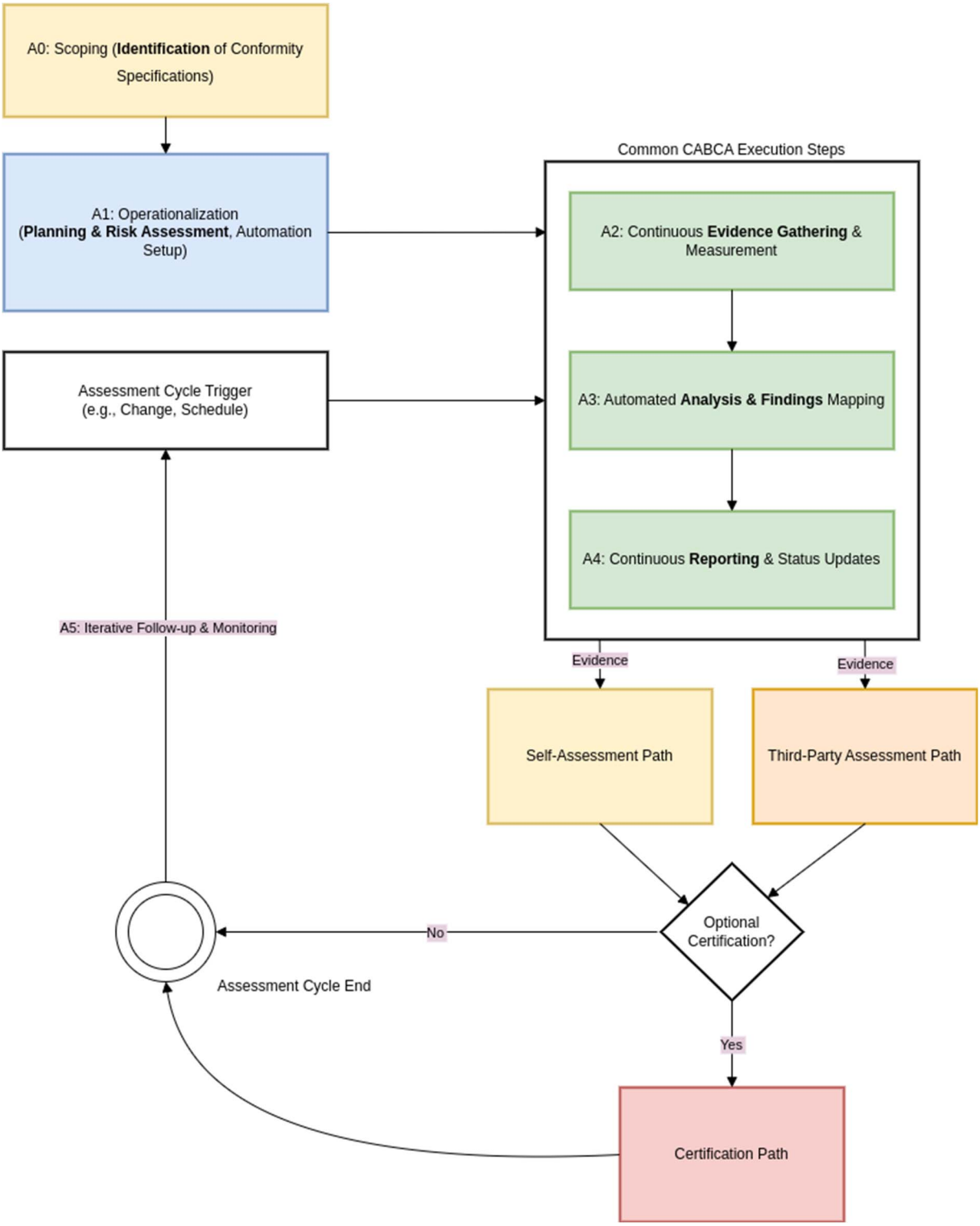

Figure 6.1-1: CABCA process flow diagram

Each Assessment Cycle shall be initiated by one or more defined **Assessment Cycle Triggers.** These triggers are classified into two main categories: proactive triggers, which are planned or scheduled (e.g. time-based reviews, system updates), and reactive triggers, which are event-driven and respond to emergent risks (e.g. significant data drift, performance degradation, or detected security anomalies). Regardless of the specific conformity assessment path chosen, this trigger shall lead into the "Common CABCA Execution Steps", which use the Operationalization Specification as their configuration:

- A2: Continuous Evidence Gathering & Measurement: This is an automated, ongoing process that collects data from system artifacts (e.g. log files, model parameters, data samples) using programmed measurements. The output of this step shall be the raw Measurement Results, which serve as the primary input for the next step.
- A3: Automated Analysis & Findings Mapping: This step shall take the Measurement Results from A2 as input. These results are automatically compared against the pre-defined thresholds and requirements documented in the Operationalization Specification (A1). The outcome of this step shall be Analysed Findings, an artifact that identifies any deviations or non-conformities.
- A4: Continuous Reporting & Status Updates: This step shall take the Analysed Findings from A3 as input and consolidate them into a structured, final output.

The common execution steps shall culminate in the generation of an Assessment Report and its associated Evidence, which consists of the raw data and artifacts (e.g. log files, test results, metric values) that substantiate the findings in the Assessment report. This artifact shall serve as the input for the subsequent assessment path chosen in clause 6.2.

The cycle concludes at the Assessment Cycle End. The overall methodology supports A5: Iterative Follow-up & Monitoring, leveraging the continuous evidence to potentially trigger subsequent assessment cycles.

6.2 Process Variations Based on CABCA Modes

6.2.1 Self-Assessment Path

In the Self-Assessment Path, the AI system provider acts as the auditing party to internally validate conformity. The primary input for this path shall be the Assessment Report. As shown in Figure 6.2-1, the AI system provider (acting as the auditing party) shall directly proceed to "Provider Reviews Results/Report". Based on this internal review against the established requirements, the provider shall then move to "Provider Records Conformity Status". The outcome of this path shall be the "Self-Assessment Status Recorded", an artifact that documents the system's compliance and can serve as an input for the Certification Path.

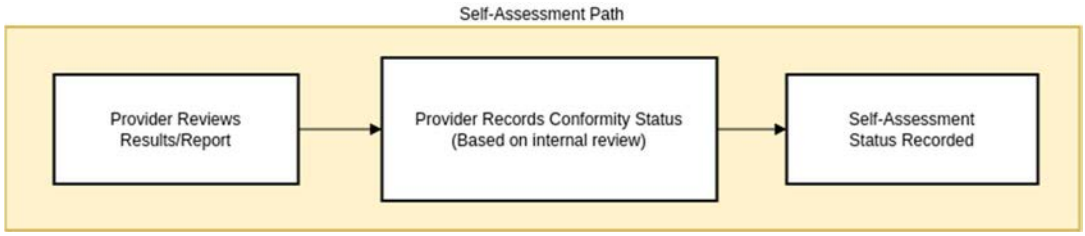

Figure 6.2-1: Self-Assessment Path

6.2.2 Third-Party Assessment Path

The Third-Party Assessment Path involves an independent external body and uses the Assessment Report as its primary input. The process, shown in Figure 6.2-2, begins when the AI system provider shall execute the step "Provider Makes Results/Report Available to Third-Party". The external body then shall proceed to "Third-Party Accesses Results/Report for Independent Assessment". The subsequent steps of the third-party assessment, including their determination of conformity, may occur externally. CABCA provides the structured Assessment Report and its underlying Evidence to facilitate this external evaluation. To achieve a fully automated assessment, the provider can expose the assessment results and evidence through a secure API, allowing the third-party's systems to programmatically and continuously ingest the data and update the assessment status automatically. The direct output of the CABCA process in this path shall be the "Third-Party Assessment Status Available".

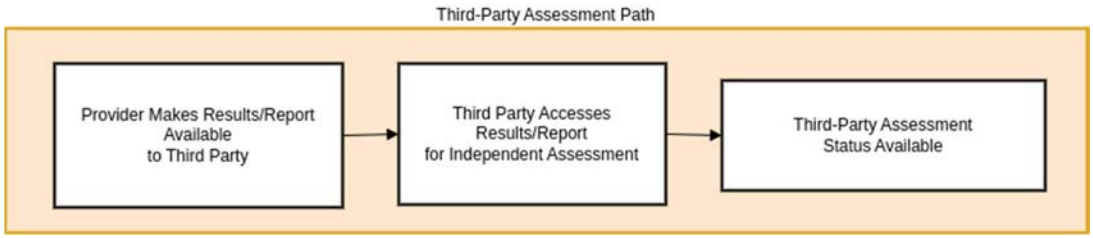

Figure 6.2-2: Third-Party Assessment Path

6.2.3 Certification Path

CABCA facilitates the optional Certification Path by providing the continuous stream of evidence generated through either the Self-Assessment or Third-Party Assessment modes. As detailed in Figure 6.2-3, the final Assessment Report from one of these preceding paths shall serve as the auditable proof of ongoing compliance necessary for obtaining and maintaining certification. This report, which includes a formal conformity status designated as either "Self-Assessment Status Recorded" or "Third-Party Assessment Status Available," is the primary input for this path. A "Certification Body Audits" this report and its supporting evidence to conduct its own assessment. By providing programmatic access to the continuous stream of evidence, this path can be highly automated, enabling a 'living certificate' where the Certification Body's systems continuously monitor compliance, potentially triggering automated updates, renewals, or revocations based on real-time data. This automated process is governed by a clear division of responsibilities: the AI Provider is liable for the continuous provision and integrity of the evidence via a secure interface, while the Certification Body is liable for the impartial and correct execution of the automated assessment and decision logic as codified in the certification scheme. The process culminates in a formal "Certification Outcome", which may be the issuance of a certificate or mark, or its revocation.

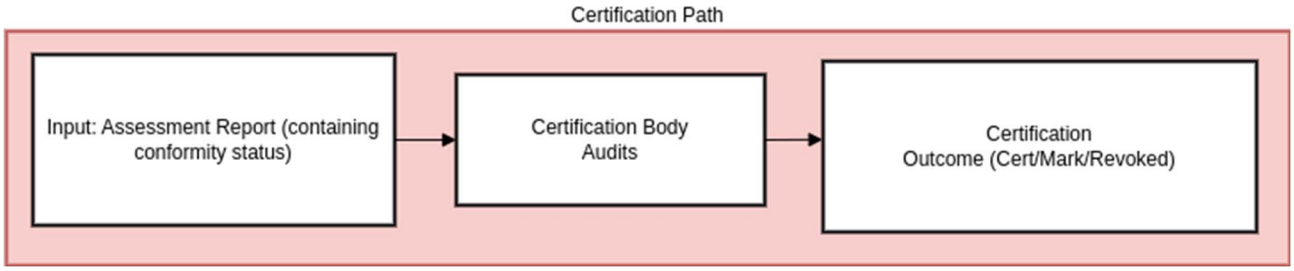

Figure 6.2-3: Certification Path

6.3 Roles in Process Execution

6.3.1 General

The CABCA process execution shall involve distinct roles with specific responsibilities as defined in clauses 6.3.2 to 6.3.4. The allocation of these roles shall be dependent on the CABCA mode (Self-assessment, Third-party assessment, or Certification support) being implemented.

6.3.2 Auditee

The entity acting as the Auditee, typically the AI System Provider, shall be responsible for the AI system undergoing CABCA.

Core Responsibilities (Applicable in all Modes):

a) The Auditee shall define the scope of the CABCA implementation, including the specific AI system(s) and the applicable conformity specifications (Scoping).

b) The Auditee shall lead and document the Operationalization phase (as defined in clause 8), which includes translating conformity specifications into measurable metrics, defining measurements, and establishing assessment criteria (Operationalization).

c) The Auditee shall implement and maintain the technical infrastructure necessary to execute measurements and checks as defined during Operationalization.

d) The Auditee shall ensure that system artifacts required for measurements are generated and made available to the measurement processes (Operationalization).

e) The Auditee shall oversee the automated execution of the continuous assessment cycles, including the "Execute Measurements & Checks" and "Generate Assessment Results / Evidence Report" steps (Continuous Assessment).

f) The Auditee shall perform internal reviews of assessment results and evidence reports (Continuous Assessment).

g) The Auditee shall implement and manage a review and update procedure to refine the CABCA process, operationalization, and measurement setup based on assessment outcomes and changes in conformity specifications or the AI system (Scoping and Operationalization).

h) The Auditee shall ensure the continuous operation of its CABCA loop to maintain ongoing conformity (Continuous Assessment).

Mode-Specific Responsibilities:

a) The Auditee shall record the conformity status of the AI system based on internal reviews in Self-Assessment mode.

b) In the context of Third-Party Assessment or Certification, the Auditee shall make the assessment results and evidence reports available to the designated Auditing Party or Certification Body.

6.3.3 Auditing Party

The entity acting as the Auditing Party shall be responsible for conducting the assessment of the AI system's conformity. The Auditing Party shall be the Auditee itself in Self-Assessment mode, or an independent external body in Third-Party Assessment or Certification modes:

a) The Auditing Party shall conduct assessments based on the evidence provided by the Auditee and according to the rules and criteria defined in the operationalization documentation and conformity specifications (Continuous Assessment).

b) The Auditing Party shall, where applicable (e.g. third-party mode), verify or formally accept the scope and operationalization defined by the Auditee (Scoping and Operationalization).

c) The Auditing Party shall participate in or inform the review and update procedure by providing feedback on the assessment process and findings (Operationalization and Continuous Assessment).

d) The Auditing Party shall maintain independence and objectivity in its assessment activities, consistent with the principles outlined in clause 5.3.4.

Mode-Specific Responsibilities

a) In Self-Assessment mode, the Auditee, acting as the Auditing Party, shall review assessment results/reports and record the conformity status.

b) In Third-Party Assessment mode, the external Auditing Party shall access the results/reports provided by the Auditee and conduct an independent assessment to determine conformity.

c) For Certification, the Auditing Party shall be an accredited Certification Body, which shall conduct its assessment based on the evidence and operationalization documentation provided by the Auditee.

6.3.4 Entity for Attestation of Conformity

The entity responsible for attesting to the conformity status of the AI system shall provide the official conformity statement to stakeholders:

a) The Entity for Attestation of Conformity shall communicate the confirmed conformity status to relevant stakeholders.

b) In Self-Assessment mode, the Auditee shall act as the Entity for Attestation of Conformity, based on its recorded conformity status.

c) In Third-Party Assessment mode, the external Auditing Party shall typically provide the attestation of conformity (e.g. an audit opinion or report).

d) In Certification mode, the accredited Certification Body, acting as the Auditing Party, shall be the Entity for Attestation of Conformity, issuing a formal certificate if conformity is determined.

e) The attestation provided shall be based on the outcomes of the CABCA process, as recorded by the Auditee (in self-assessment) or determined by the external Auditing Party/Certification Body.

7 Scoping (Identification of Conformity Specifications)

7.1 General

Before the CABCA methodology can be operationalized, an organization should conduct a foundational Scoping process. This process involves the systematic identification, selection, and compilation of all relevant requirements that apply to a specific AI system. This activity is a fundamental practice in any robust compliance or quality management framework and is not unique to CABCA. It is the standard process of determining the applicable legal, technical, and ethical landscape for a product or system.

The primary goal of the Scoping phase is to produce a definitive and auditable Conformity Specification. This document consolidates the applicable requirements from various sources, such as legislation, harmonised standards, industry best practices, and internal policies. The resulting Conformity Specification serves as the authoritative and formal input for the subsequent Operationalization phase (see clause 8), where these high-level requirements are translated into a concrete, measurable, and continuously auditable framework.

7.2 Sources and Integration Criteria for Conformity Specifications

7.2.1 Sources of Conformity Specifications

The Scoping process relies on identifying and selecting appropriate conformity specifications from various sources. This clause first identifies the diverse sources from which these specifications can originate and then details the essential criteria a specification should meet to be selected for inclusion in the final Conformity Specification (clause 7.2.2).

Conformity specifications, identified during the Scoping phase, are foundational documents that consolidate the requirements an AI system should meet. These can be international standards from ISO, IEC and ITU, European documents from ETSI, CEN and CENELEC, as well as other authoritative sources that outline the conditions or guidelines that shall be met. The sources of these specifications can vary widely, depending on factors such as the industry, market standards, and specific organizational needs. In cases where requirements from these diverse sources overlap or conflict, they shall be harmonized using a defined hierarchy of authority, where binding legal obligations prevail over harmonised standards, which in turn prevail over industry best practices and internal policies. This ensures that a single, coherent, and non-contradictory set of requirements is consolidated into the final Conformity Specification for operationalization. Examples of sources include:

- Legislative Requirements: Federal, state, or local laws that mandate certain types of conformity.

- Such can be the legislative requirements withing the European AI Act and the correspondent standardization request.
- International standards that often serve as a framework for conformity in various sectors.
- (Harmonised) European Standards.
- National Standards: Developed by national organizations like NIST in the United States.
- Industry Guidelines: Established best practices within specific industries.
- Internal Policies: Guidelines set within an organization.
- Quality Assurance Protocols: These could be part of internal governance or subject to external audits.
- Product Certifications: Such as UL, CE, or Common criteria labels that certify a product meets certain standards.
- Military Standards (MIL-STD): These are relevant to military applications.
- Healthcare Regulations: Such as HIPAA in the United States.
- Financial Regulations: Sarbanes-Oxley for corporate governance, GDPR for data protection, and so on.
- Vendor Agreements: Requirements from vendors that organizations shall adhere to.
- Ethical Guidelines: Ethical principles and frameworks, like fairness, transparency, and accountability, that apply specifically to AI development and deployment.
- Third-Party Audits: These may also dictate conformity requirements.
- Consumer Protection Laws: Regulations to ensure AI-driven consumer products meet safety and reliability standards, as well as disclosure requirements around data collection and usage.

Among the sources of conformity specifications, harmonised standards are becoming particularly significant, especially driven by legislation like the European AI Act [i.9]. Developed by European Standardization Organizations (ESOs like CEN, CENELEC, ETSI) based on formal requests (mandates) from the European Commission, HS serve a critical function: they translate the high-level, legally binding requirements of legislation (such as the essential requirements in the AI Act) into detailed, technical specifications. The key value of HS for frameworks like CABCA lies in their technical granularity and actionability. Unlike the broader legal text, HS provide concrete engineering details, potentially specifying:

- Precise test methods and procedures.
- Quantitative metrics and performance thresholds (e.g. for accuracy, robustness, bias detection).
- Specific requirements for data governance (e.g. dataset characteristics, provenance checks).
- Detailed documentation structures and content requirements.
- References to underlying international standards (e.g. from ISO/IEC).

This level of detail directly addresses CABCA's need for precision and clarity. While CABCA is designed to be adaptable, its effectiveness in enabling continuous auditing against clear, measurable benchmarks is significantly enhanced when operating with the precise, actionable requirements defined in harmonised standards.

7.2.2 Criteria for Integrating Conformity Specifications in CABCA

For a source document to be included in the final Conformity Specification and be effectively used by the CABCA framework, it should meet the following minimum requirements (criteria):

- **Operationalizability:** The conformity specification, which represents the quality objective to be achieved, for example an essential requirement from a HEN standard shall be translatable into practical steps for risk management, quality assurance, as well as other operational activities, in dependence of the quality goals to be achieved.

- **Coverage of key areas:** At a minimum, the conformity specifications shall cover the essential aspects (e.g. essential requirements in European Legislations) regarding the quality goals relevant to the system or industry under CABCA audit.
- **Credibility:** The conformity specification depicting the quality objectives to be achieved shall have some degree of recognition or authority within its respective industry.
- **Clear licensing and usage policies:** There shall be explicit terms defining how the specification can be used.
- **Capability to provide metrics:** The conformity specification shall either directly provide measurable parameters or be interpretable in a way that such metrics can be derived.
- **Auditability:** The conformity specification shall contain elements that are auditable on a continuous basis, aligning with CABCA's methodology.

8 Operationalization (Planning & Risk Assessment, Automation Setup)

8.1 Process of Operationalization

8.1.1 General

Operationalization is the cornerstone of the CABCA methodology. It is the process that takes the "Conformity Specification", as defined in the Scoping phase (see clause 7) and transforms its abstract, high-level requirements into concrete, measurable, and auditable requirements and metrics for a specific AI system and its data. This process is also informed by the results of prior assessments to allow for iterative refinement. This process ensures that regulatory, ethical, and quality-related intentions are preserved and implemented throughout the AI system's lifecycle. It begins with aligning the operationalization process with the requirements of the chosen conformity specifications. This alignment ensures that the specifications are operationalizable, credible, comprehensive, and applicable to the AI system. It establishes a foundation that respects both the intention of the specifications and the functional capabilities of the AI system. For example, the EU AI Act applies mostly to high-risk AI systems and General-Purpose AI systems, emphasizing the importance of the AI system's intended use.

Figure 8.1-1 illustrates the operationalization process, which consists of two interconnected flows. The forward *Operationalization* arrow shows the progression through four key stages: from Dimensions and Risks to Requirements & Metrics and finally Measurement. The blue boxes at the bottom specify the context and inputs for each corresponding stage, starting with Conformity Specifications and ending with the specific AI implementation. The reverse "Assessment" arrow indicates a feedback flow, where results from the measurement phase are used to evaluate the choices made in the preceding stages.

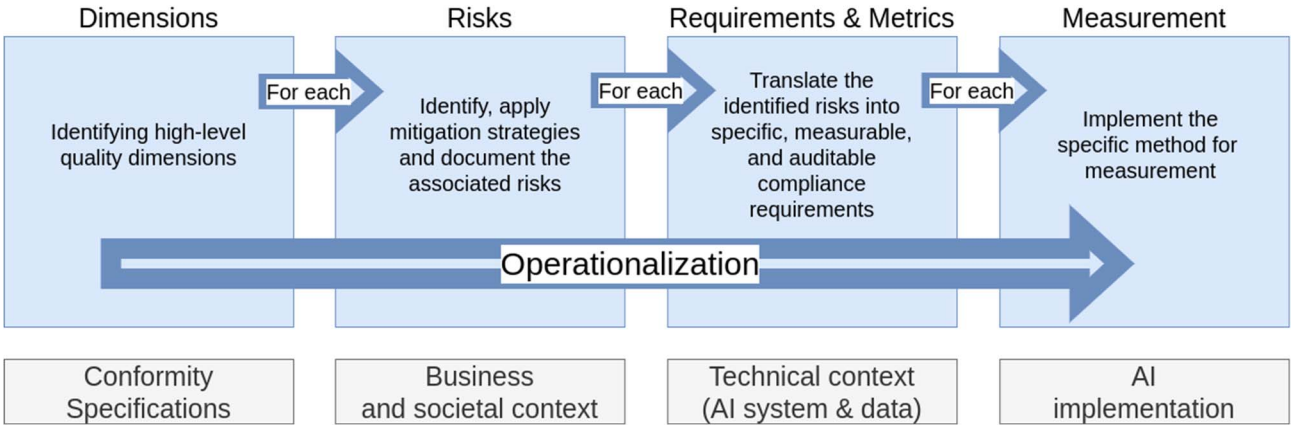

Figure 8.1-1: The Operationalization Process in CABCA

The following clauses present a stepwise breakdown of this transformation process, guided by specific goals and justified by their role in effective auditing and continuous conformity assessment.

8.1.2 Identification of Quality Dimensions

8.1.2.1 Requirements for Defining Quality Dimensions

Quality dimensions are the foundation of the operationalization process. They define the key aspects of an AI system under which specific requirements should be evaluated to ensure alignment with conformity specifications. These dimensions reflect societal, regulatory, and technical expectations and serve as entry points for further risk analysis and metric definition:

- The operationalization process shall identify quality dimensions relevant to the selected conformity specifications.
- These dimensions shall include, but are not limited to, avoidance of unwanted bias, accuracy, robustness, and cybersecurity.
- Identified quality dimensions shall act as high-level categories for auditing and evaluating system performance and conformity.

8.1.2.2 Criteria for Defining Quality Dimensions

The definition of quality dimensions shall adhere to the following criteria:

- **Granularity:** Quality dimensions shall be defined in a way that supports decomposition into manageable subcomponents for targeted assessment.
- **Suitability:** Quality dimensions shall be adaptable to evolving technologies, application contexts, or business scenarios, as permitted by the conformity specification.
- **Coverage & traceability:** Dimensions shall cover the relevant aspects required by the selected conformity specifications and enable traceability to those sources.
- **Operationalizability:** Dimensions shall be definable in terms that allow derivation of measurable requirements and metrics.

8.1.3 Identification of Risks

8.1.3.1 Requirements for Defining Risks

Risks linked to each quality dimension need to be documented to contextualize potential harms or non-conformities. This step ensures that all assessments are risk-informed and traceable to their underlying rationale in the conformity specification:

- For each identified quality dimension, the operationalization process shall identify and document associated risks by referencing the conformity specifications.
- The documented risks shall form the basis for developing risk mitigation strategies.
- Each identified risk shall be addressed by one or more defined requirements or mitigation actions.

8.1.3.2 Criteria for Identifying Risks

The identification and documentation of risks shall adhere to the following criteria:

- **Mitigatability:** Risks shall be evaluated based on the ability to implement risk mitigation strategies. Or the risk is accepted, then itis not part of the assessment.
- **Risk traceability:** Each mitigation action shall be demonstrably traceable to its originating risk and source specification.

8.1.4 Deriving Measurable Compliance Requirements and Metrics

8.1.4.1 Requirements for Deriving Measurable Compliance Requirements and Metrics

To assess risks effectively, concrete and measurable compliance requirements should be derived. These requirements should be directly traceable to risks and quality dimensions, and measurable using well-defined metrics. This formalization ensures that assessments are actionable and reproducible:

- The Operationalization Process shall define specific, measurable, and auditable requirements for the AI system under assessment, derived from the identified risks and their corresponding mitigation strategies:
  - Each requirement shall be traceable to an identified risk and its associated quality dimension.
  - Each requirement shall be directly linked to the initial conformity specification.
- For each requirement, the operationalization process shall establish one or more corresponding metrics:
  - Each metric shall be a concrete, measurable parameter that reflects the AI system's adherence to the specific requirement.

8.1.4.2 Criteria for Deriving Measurable Compliance Requirements

The derivation of measurable compliance requirements shall adhere to the following criteria:

- **Relevance:** Requirements shall be directly relevant to the AI system's intended purpose and application context.
- **Clarity:** Requirements shall be defined in a clear and unambiguous manner to prevent misinterpretation.
- **Measurability:** Each requirement shall be linked to one or more metrics that enable its quantitative evaluation.
- **Traceability:** Each requirement shall be traceable back to its originating risk and source specification.
- **Frequency:** The evaluation frequency for each requirement shall be explicitly specified.
- **Threshold justification:** For metrics with pass/fail or target thresholds, the acceptance threshold shall be justified by intended use and deployment context and referenced to the applicable risk classification.

8.1.4.3 Criteria for Deriving Metrics

The derivation of metrics shall adhere to the following criteria:

- **Precision:** Metrics shall be defined with sufficient clarity and precision to ensure unambiguous interpretation.
- **Relevance:** Each metric shall be directly and demonstrably related to the requirement and quality dimension being measured.
- **Unit specification:** A specific unit of measurement shall be defined for each metric's value.
- **Measurability:** Each metric shall be capable of being reliably and practically measured through a defined process.

8.1.5 Implementing Measurements

8.1.5.1 Requirements for Implementing Measurements

To enable automated and continuous assessment, concrete measurement methods should be defined for each metric. These methods serve as the procedural and technical basis for conformity checks and allow repeatable evaluations across time and system versions:

- For each defined metric, the operationalization process shall define and document the method(s) for its measurement:
  - The documentation for each measurement method shall specify the techniques, tools, or procedures to be used.
  - The defined measurement methods shall collectively establish the framework for the continuous, automated assessment of compliance.

8.1.5.2 Criteria for Implementing Measurements

The implementation of measurements shall adhere to the following criteria:

- **Automation:** Measurements shall be implemented with a high degree of tool-based automation to ensure repeatability and efficiency.
- **Output unit consistency:** The output unit of a measurement shall be consistent with the unit defined for the corresponding metric.
- **Automated result collection:** The collection of measurement results shall be automated to enable continuous auditing.
- **Evidence retention:** The retention period for measurement results, which serve as evidence, shall be explicitly specified.
- **Measurement uncertainty & repeatability:** Known sources of uncertainty (including non-determinism in tools and the AI system) shall be identified; variability should be quantified or otherwise documented (e.g. standard deviation, confidence intervals); repeatability considerations shall be described.
- **Tool accountability:** If the testing/evaluation tool contains AI components, the uncertainty assessment shall explicitly cover those components.

8.2 The Operationalization Specification

8.2.1 General

To address both human and machine processing needs, the Operationalization Specification is captured as a single, structured, machine-readable specification. From this source of truth, a human-readable documentation is rendered to inform stakeholders, while the specification itself is used directly to configure automated assessments. Both forms inherently adhere to common principles such as traceability, ensuring consistency between the documented rationale and its automated assessments. Given the complexity of multi-vendor AI systems, where different components like data sources, foundation models, and hosting might be managed by different entities, this specification also supports nested operationalization. This mechanism allows the final system provider's assessment to programmatically incorporate the conformity status of a third-party component. It is achieved by defining a measurement that queries the component supplier's assessment results via a machine-readable Assessment Interface. This structure creates a recursive "chain of assurance" and ensures clarity in roles and responsibilities, as each entity attests to the conformity of its own contribution. This structure ensures clarity in roles and responsibilities across all levels of system operation.

8.2.2 Requirements for the Operationalization Specification

The operationalization specification shall adhere to a defined structure that translates high-level Conformity Specifications into specific documentation items. This structure shall facilitate the creation of actionable, machine-readable records for continuous assessment and auditing by meeting the following requirements:

a) The specification shall be based on a formal documentation model that defines the required information elements for all documentation items, including but not limited to, Conformity Specifications, Dimensions, Requirements, Metrics, and Measurements. A core set of common information elements shall be identified for all items, which may be supplemented by specific elements where necessary.

b) The specification shall ensure that each documentation item is systematically described with the necessary information elements to enable automated evaluation and consistently capture all necessary descriptive and operational details.

c) The specification shall be structured to support machine readability and automation, enabling it to function directly as a configuration file for automated assessment engines and monitoring tools. This shall be achieved through the use of standardized information elements (such as Name, Assessor, AssessmentInterface, Frequency) to allow for automated parsing, integration with assessment tools, and the execution of continuous monitoring cycles.

d) The specification shall capture essential metadata required for robust auditability and traceability. Information elements (such as Name, Comment, ConfidentialityFlag, and Assessor) shall be used to allow auditors to verify the assessment process, responsibilities, evidence trails, and rationale. The documentation shall also support a hierarchical structure of items, linked by information elements (such as names), to ensure unambiguous linkage between them.

e) The specification shall ensure that the consistent capture of information facilitates stakeholder understanding, comparison, and review, aligning with recognized quality aspects of documentation.

f) The documentation structure shall support visualization using an Entity-Relationship (ER) diagram or an equivalent visual technique, as exemplified in Figure 8.2-1.

8.2.3 Criteria for the Operationalization Specification

The structuring of the Operationalization Specification shall adhere to the following criteria, which ensure the overall quality and utility of the documentation:

a) **Transparency:** The specification shall clearly outline the process of translating Conformity Specifications into operational steps, thus eliminating ambiguity. This includes clearly articulating the operationalization methods used, providing precise interpretations of Conformity Specifications to reduce regulatory uncertainties, and clearly stating quality requirements, expectations, and the scope of each assessment.

b) **Traceability:** The specification shall allow for each metric, requirement, and decision to be traced back to the original Conformity Specifications and its corresponding quality dimensions.

c) **Configurability:** The specification shall enable a straightforward translation into automated assessments by being structured to act as a configuration file.

d) **Nested Documentation Capability:** The specification shall ensure that operationalization documentation can be nested and can also nest documentation from other vendors, providing a comprehensive and integrated view of multi-vendor AI system components.

To visually represent how these criteria are met, the structure of the Operationalization Specification is depicted in Figure 8.2-1. This Entity-Relationship (ER) diagram illustrates the relationships between the core components, showing how high-level Conformity Specifications are linked down through Quality Dimensions, Requirements, and Metrics to the specific Measurements, thereby ensuring end-to-end traceability.

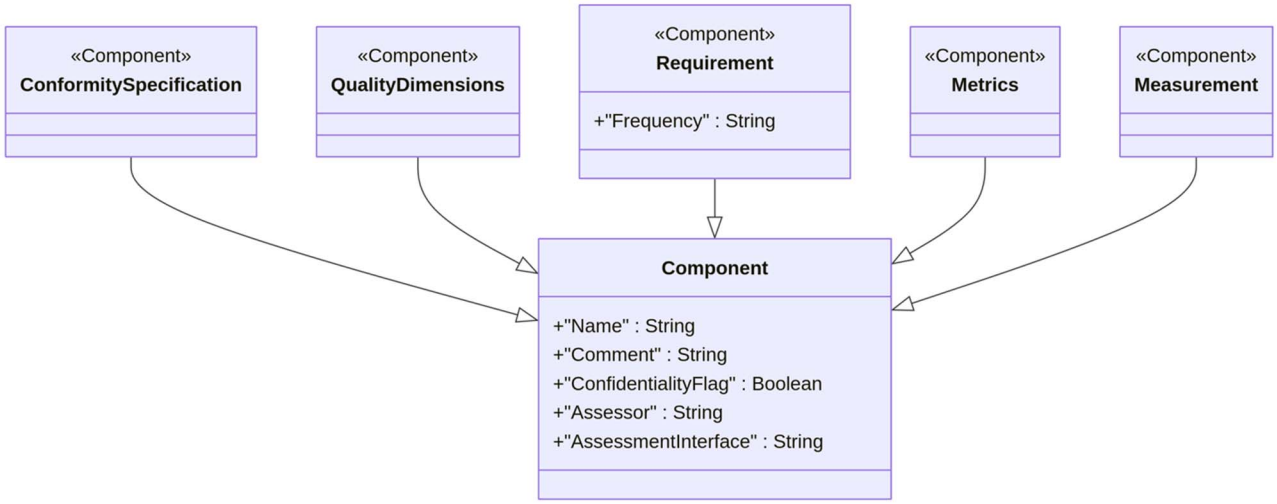

Figure 8.2-1: ER Diagram of Operationalization Specification Structure

9 Continuous Assessment Process

9.1 Continuous Evidence Gathering & Measurement

CABCA is designed to provide an ongoing assessment of AI systems to ensure they meet conformity specifications, quality goals, and manage risks effectively. This clause explains the steps involved in the CABCA assessment, focusing on how the operationalization documentation serves as a configuration file for the assessment.

Initial Setup: Using operationalization documentation

Before initiating the assessment process, the operationalization documentation, which lays down dimensions, requirements, metrics, and measurements, is used to set up the continuous assessment. This documentation enables automatic interpretation of audit criteria, metrics, and the corresponding measurements.

Frequency of assessments

The frequency for each assessment varies based on individual needs and is specified for each requirement within the configuration file. The assessment process is invoked every time a new model is deployed. During the operation phase, the frequencies for assessment are explicitly defined within the operationalization documentation.

1) **Measurements based on Artifacts of ongoing AI Operation:** Artifacts such as log files, model weights, and data samples are produced or utilized throughout the ML life-cycle and serve as inputs for these measurements. Some artifacts yield results directly through parsing, while others require comprehensive test suites (e.g. as described in ETSI TR 103 910 [i.6]) to obtain accurate data (see Figure 9.1-1).

2) **Measurement:** The artifacts are analyzed and processed to produce metric values, which are then prepared for transmission to the auditing entity. This enables real-time or frequency-based evaluations, triggered either after specific events (e.g. model deployment) or at predefined intervals tied to individual quality requirements. This corresponds to the "Measurement" phase in the diagram (see Figure 9.1-1).

3) **Assessment based on measurement results – Mapping to Requirements and Conformity Specifications:** The received measurement data are automatically evaluated, using the operationalization documentation as a configuration file, against predefined metric thresholds that reflect the AI system's quality goals. This automation makes the evaluation both rapid and fully consistent with the conformity specifications (see Figure 9.1-1).

4) **Report generation:** The resulting report shows which quality goals are met by mapping each measurement result to the relevant parts of the Conformity Specifications and indicating the degree of satisfaction. It is shared with stakeholders at varying levels of detail, for example, a concise executive summary for leadership and a technical annex for engineers and auditors, to communicate the AI system's current compliance status. This aligns with the "Report Generation" phase in the diagram (see Figure 9.1-1).

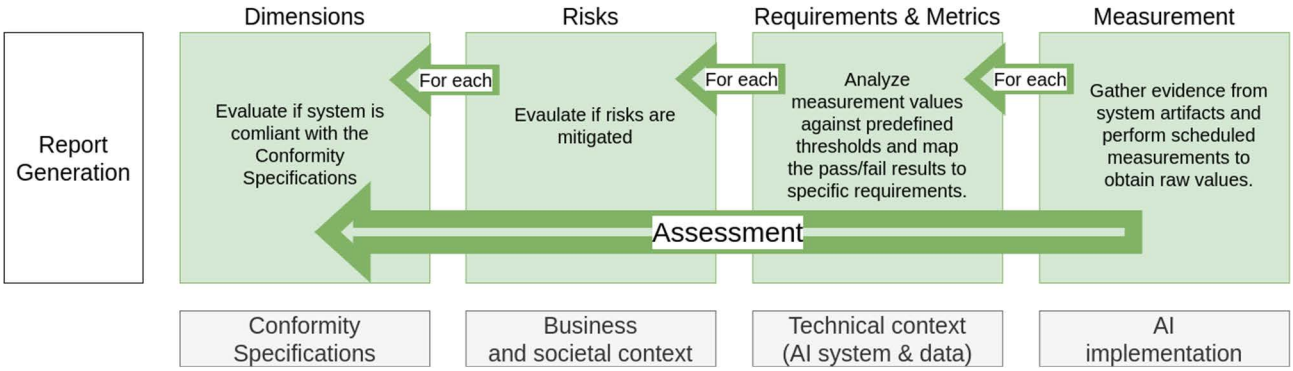

Figure 9.1-1: Continuous Evidence Gathering and Measurement

9.2 Assessment Evidence

9.2.1 General

The continuous assessment process within CABCA shall utilize evidence derived from operational outputs, system states and records:

a) Relevant operational outputs, system states, and records, along with their pertinent characteristics (information elements), shall be systematically captured and structured to constitute documentation items for assessment purposes.

b) The identification of these documentation items and the ensuring of the availability of their underlying sources shall be performed during the Operationalization phase (as defined in clause 5).

c) The documentation items, determined during planning based on the defined measurements, shall provide the necessary verifiable evidence for the continuous assessment process.

d) The underlying sources (e.g. log entries, model parameters) shall serve as inputs for measurements.

e) The structured record of these sources and their measurements shall constitute the verifiable documentation item used to evaluate conformity against specified requirements.

f) The operationalization documentation shall specify the documentation items to be used as evidence for each defined measurement.

g) For different stages of the AI system lifecycle, such as development/training and operation, specific documentation items shall be identified and utilized as evidence. These documentation items shall include, but are not limited to, those listed in clauses 6.2.1 and 6.2.2.

9.2.2 Sources of Evidence During Development and Training

Evidence for the development and training stages of an AI system shall include, as applicable:

a) Documentation of Log Files: This shall capture information elements related to system logs, application logs, and audit logs reflecting operational behaviour and interactions during development.

b) Documentation of Model Weights: This shall capture information elements detailing the parameters of machine learning models that are trained.

c) Documentation of Data Samples: This shall capture information elements describing instances of data used in model training, including input data, processed data and output data.

d) Documentation of Code Repositories: This shall capture information elements related to the source code and scripts used in developing the AI system.

e) Documentation of Configuration Files: This shall capture information elements detailing settings and parameters for model training and development processes.

f) Documentation of Test Results: This shall capture information elements detailing the outcomes of tests, such as unit tests and integration tests.

g) Documentation of Hyperparameters: This shall capture information elements describing the set of parameters that govern the training process of machine learning models.

9.2.3 Sources of Evidence During Operation

Evidence for the operational stage of an AI system shall include, as applicable:

a) Documentation of Log Files: This shall capture information elements from system, application, and audit logs detailing operational behaviour in a live environment.

b) Documentation of Loaded Model Weights: This shall capture information elements detailing the parameters of the deployed machine learning models.

c) Documentation of Inference Data: This shall capture information elements describing data used or generated by the AI systems during operation, including user input, system outputs, and intermediate processing data.

d) Documentation of Performance Metrics: This shall capture information elements detailing data on system performance, including accuracy, latency, throughput, and error rates during operation.

e) Documentation of Security Certificates and Logs: This shall capture information elements related to encryption certificates, security logs, and breach reports.

f) Documentation of Incident Reports: This shall capture information elements documenting any operational incidents or anomalies.

g) Documentation of Change Logs: This shall capture information elements recording updates, bug fixes, and feature additions post-deployment.

h) Documentation of Configuration Files: This shall capture information elements detailing operational settings and parameters under which the AI systems function post-deployment.

9.3 Persistence of Assessment Results

The results of each CABCA assessment shall be stored persistently for future reference, quality tracking, and for proving compliance in audits. The scope of this persistence shall include:

- **Measurement results:** All metrics, along with their corresponding values, are systematically stored. This includes data on system performance, measures on avoidance of unwanted bias, accuracy and other critical indicators essential for evaluating the system's alignment with specified standards.
- **Evaluation outcomes:** The outcomes of the comparisons between metrics and pre-defined quality goals are archived.
- **Assessment Reports:** The final reports generated after each assessment are saved.

The retention of these artifacts is governed by a policy that aligns with industry standards, legal requirements, and organizational guidelines. This policy is periodically reviewed and updated to remain congruent with the evolving technological and regulatory landscape.

Audit requirements for persistence:

The following audit requirements shall be considered:

- **Searchability:** Stored data is organized to facilitate easy and efficient retrieval. This includes advanced search capabilities to handle complex queries relating to the system's performance and compliance history;

- **Security:** Ensure that the stored data is encrypted and accessible only by authorized personnel;
- **Traceability:** Each stored item shall be traceable back to the specific assessment cycle and corresponding operationalization documentation;
- **Automated archiving:** An automated archiving system shall be in place to manage the lifecycle of stored data.

9.4 Updating Conformity Status

9.4.1 Conformity Status Updates

The outcome of quality assessments in CABCA is a critical component, involving a detailed evaluation of measurement results. These results shall be derived from various artifacts such as log files and model weights, and shall be assessed against predefined values. These values shall be based on expert knowledge and risk assessments integral to CABCA's methodology.

When measurement results align with the predefined values, a conformity status shall be issued, confirming the AI system's compliance with the required standards. Conversely, if the results deviate from these values, the conformity status shall be either revoked or adjusted. This highlights areas needing improvement and signals the necessity for enhanced risk management strategies.

An integral part of this process is the ongoing revision and updating of quality requirements. Changes in these requirements can significantly impact the assessment outcomes, reflecting CABCA's dynamic approach to conformity in rapidly evolving technological environments.

9.4.2 Transparency in Reporting and Updates

Transparency is a cornerstone of CABCA, especially in the documentation and communication of assessment outcomes to stakeholders. This process shall entail:

- **Clear system identification:** Including unambiguous references to the AI system name, type, and additional identification details for full traceability.
- **Provider information:** Documenting the name and address of the AI system provider or their authorized representative.
- **Compliance statement:** A direct statement indicating the AI system's conformity with applicable standards, regulations, and, where relevant, data protection requirements.
- **Reference to Standards:** Mentioning any relevant harmonised standards or specifications that have been used to declare conformity.

This documentation guides the automated assessment process and enhances stakeholder understanding of the conformity measures, ensuring that every operationalization decision is communicated transparently.

9.4.3 Effective Communication with Stakeholders

Communication in CABCA is designed to be clear, consistent, and tailored to the needs of various stakeholders. This involves defining specific communication channels and the scope of each, ensuring that stakeholders receive the most relevant and up-to-date information. The frequency and granularity of communication updates are carefully determined to keep stakeholders informed about the AI system's compliance status without overwhelming them with unnecessary details.

9.4.4 Building and Maintaining Stakeholder Trust

CABCA strengthens stakeholder trust by maintaining a steady flow of reliable information about the AI system's compliance status. This is achieved through the regular publication of Assessment Reports and updates on any changes in the conformity status. By ensuring open and clear communication and providing objective evidence of compliance through third-party audits when applicable, CABCA not only maintains but also bolsters stakeholder confidence in the organization's commitment to adhering to relevant standards and regulations regarding their AI systems.

10 Documentation of the CABCA Process and its Outcome

10.1 General

CABCA directly supports the documentation obligations under the **EU Artificial Intelligence Act (AI Act)** by enabling traceable, evidence-based assessments of AI systems against conformity requirements. It operationalizes continuous conformity monitoring and supports the production of living documentation that reflects the current compliance status, audit readiness, and risk posture of an AI application across its lifecycle. As such CABCA is designed to address the technical documentation obligations under the EU AI Act [i.9]. It supports:

- Article 11 and Annex IV documentation obligations (technical documentation),
- Article 17 (post-market monitoring system),
- Article 9 (risk management system),
- Article 15 (accuracy, robustness, and cybersecurity),
- Article 17 (quality management system, when relevant).

The CABCA documentation shall follow the structure, principles, and stakeholder-oriented perspective defined in ETSI TR 104 119 [i.11]. As per that specification, CABCA documentation shall be:

- Modular, separating concerns across assessment specification, execution and results.
- Traceable, enabling linkage from high-level conformity requirements to low-level metrics and evidence.
- Stakeholder-sensitive, supporting differentiated documentation profiles.
- Lifecycle-integrated, covering static, dynamic, and continuous assessment across development and operational phases.

10.2 CABCA Documentation Items

10.2.1 General

In line with ETSI TR 104 119 [i.11], documentation items refer to the specific artifacts, workflows, or components of CABCA that require structured and traceable documentation to support transparency, accountability, and regulatory compliance. Importantly, a documentation item is not the document itself, but rather the subject of documentation. Each documentation item is a source for generating information elements that describe its properties, context, and compliance-relevant attributes, such as performance metrics, system attributes, or measurement results.

CABCA shall organizes its main documentation items to reflect this structure, ensuring clear traceability, stakeholder relevance, and alignment with legal obligations, particularly those defined by the EU AI Act [i.9].

10.2.2 Conformity Specification

This documentation item, which is the output of the Scoping process (clause 7), shall serve as basis to document the normative and contextual basis for CABCA. Documentation derived from the conformity specification shall include the following information elements:

- Sources of requirements: Legal (e.g. EU AI Act), Regulatory (e.g. ISO/IEC 42001 [1], ETSI ENs), Domain-specific or internal (e.g. automotive safety standards, medical AI best practices) as outlined in clause 7.2.1.
- Structured conformity requirements: Organized by lifecycle phase and risk domain, assigned unique identifiers, linked to stakeholder concerns and tagged with applicability and criticality as outlined in clause 8.2.

10.2.3 Operationalization Specification

This documentation item shall serve as a basis to document how conformity requirements are translated into measurable quality constructs and embedded into the continuous assurance cycle. Documentation derived from the operationalization specification shall include the following information elements:

- Quality dimensions: Derived from stakeholder expectations and the conformity specification.
- Risk identification and treatment aligned with the quality dimensions.
- Metrics and measurement models: Mapped from quality dimensions, justified by relevance (i.e. risks), and defined with thresholds.
- Technical setup and infrastructure: Describes CABCA's measurement and monitoring architecture.
- Monitoring protocols: Frequency, granularity, triggers and escalation mechanisms.

10.2.4 Measurement Results and Evidence

This documentation item shall serve as a basis to document the results of assessment activities performed through CABCA's measurement pipeline. It shall include the following information items:

- Assessment outputs: Metric results contextualized by time and version.
- Interpretation and scoring: Deviation from expectation, anomaly detection and interpretation of deviations.
- Conformity status: Compliant / partially compliant / non-compliant.
- Evidence artefacts: Logs, data excerpts, explainability reports and statistical summaries.
- Timeliness and relevance: Versioned and timestamped, aligned with audit requirements.
- **Verdict**: Provide a comprehensive conclusion on the system's compliance status in relation to the set quality goals.

10.3 Traceability and Consistency

CABCA shall ensure bidirectional traceability throughout the documentation stack:

- Results → Metrics → Quality Dimensions → Risks → Conformity Requirements.
- All artefacts are version-controlled and machine/human-readable.
- Integrity checks support data provenance and auditability.

10.4 Stakeholder Documentation Profiles

CABCA shall support customized documentation profiles for different stakeholders as mandated by ETSI TR 104 119 [i.11].

Table 10.4-1: Documentation Profiles for different Stakeholders

Stakeholder	Documentation Items
AI Provider (Developer)	All documentation items (i.e. conformity specification, operationalization specification and measurement results and evidence). Full traceable across all layers, with design decisions and version control.
Conformity Assessment Body	Structured conformity mapping, test protocols, results, and audit logs.
Regulatory Authority	Conformity status, risk deviations, and legal requirement mappings.
AI Operator	Monitoring dashboards and alerts.
End User/Impacted Person	Public summaries on fairness, transparency, and safety.

Annex A (informative): Examples

A.1 General

This annex provides two illustrative, end-to-end use cases that demonstrate the practical application of the Continuous Auditing-Based Conformity Assessment (CABCA) framework. The examples walk through the core phases of Scoping (clause 7), Operationalization (clause 8), and Continuous Assessment (clause 9).

Each use case begins with a description of the application scenario and its associated risks. It then follows the CABCA process to show how high-level compliance goals are systematically translated into specific, automated measurements and verifiable reports. This approach is designed to showcase the complete, traceable path from a conformity requirement to its continuous, evidence-based assessment, as detailed throughout the present document.

A.2 PII Leakage Control for a Support Ticket Assistant

A.2.1 Use Case Description

Application Scenario and Risk: ACME Support Solutions develops an AI-powered assistant to help its customer support teams. The AI system reads incoming customer support tickets, summarizes them, and suggests draft replies for the human agent. A primary risk is that the AI model might inadvertently include Personally Identifiable Information (PII) - such as names, email addresses, or phone numbers, in its generated summaries or system logs. If this sensitive information is stored insecurely or included in a reply, it would constitute a significant data breach and a violation of privacy regulations like GDPR, leading to legal penalties and loss of customer trust.

A.2.2 CABCA Implementation Example

A.2.2.1 General

The following clauses illustrate how the CABCA framework is applied to mitigate the risk of PII leakage. The process begins with Scoping to define the conformity requirements, proceeds to Operationalization to create a measurable and auditable specification, and concludes with an example of a Continuous Assessment Report.

A.2.2.2 Scoping and Operationalization Specification

This example details the creation of the Operationalization Specification, which translates the high-level goal of preventing PII leaks into a concrete, machine-readable format for continuous auditing. The specification is built by defining the Conformity Specification, Quality Dimensions, Requirements, Metrics and Measurements.

The information is presented in Tables A.2-1 to A.2-5 below. Each component includes its attributes and a rationale explaining how it was derived in the context of the CABCA process.

Table A.2-1: Exemplary Conformity Specification for PII Leakage Control

Item Component	Attribute	Value / Description
Conformity Specification	*Name*	"CS-PII-01"
	Comment	"Consolidated requirement to prevent clear-text personal data in outputs and logs."
	ConfidentialityFlag	true
	Assessor	"Compliance"
	AssessmentInterface	"doc://conformity/CS-PII-01"
	sources	["EU_AI_Act_Art15", "GDPR_Art25"]
Explanation: This Scoping artifact (clauses 7.1, 7.2.1) consolidates applicable sources like GDPR Article 25 ("Data protection by design") and the EU AI Act's robustness requirements (Art. 15) into a single, actionable goal. It is selected based on the criteria in clause 7.2.2 and serves as the formal input for Operationalization and the documentation item in clause 10.2.2.		

Table A.2-2: Exemplary Quality Dimension Specification for PII Leakage Control

Item Component	Attribute	Value / Description
Quality Dimensions	*Name*	"QD-PII"
	Comment	"Dimensions relevant to CS-PII-01."
	ConfidentialityFlag	false
	Assessor	"Compliance"
	AssessmentInterface	"doc://dimensions/QD-PII"
	dimensions	["privacy", "accountability"]
Explanation: In accordance with clause 8.1.2, the high-level requirement is broken down into quality dimensions. Preventing data leaks is a core "privacy" concern, while the ability to prove that the system is functioning correctly relates to "accountability". These dimensions structure the subsequent risk analysis and metric definition.		

Table A.2-3: Exemplary Requirements Specification for PII Leakage Control

Item Component	Attribute	Value / Description
Requirement	*Name*	"R-PII-01"
	Comment	"No clear-text PII in answers or logs; traceable to CS-PII-01."
	ConfidentialityFlag	false
	Assessor	"Compliance"
	AssessmentInterface	"cfg://req/R-PII-01"
	Frequency	"weekly && on_deploy"
	fromConformitySpecification	"CS-PII-01"
	qualityDimensionsRef	"QD-PII"
	traceToSource	["GDPR_Art25"]

Explanation: The requirement is defined to be measurable and auditable (clause 8.1.4.1) and includes an explicit evaluation frequency (clause 8.1.4.2). The frequency is set to run weekly for ongoing monitoring and also `on_deploy`, as a new model version could introduce unexpected behaviour and should be checked immediately. Full traceability is maintained (clause 10.3).

Table A.2-4: Exemplary Metric Specification for PII Leakage Control

Item Component	Attribute	Value / Description
Metrics	*Name*	"M-PII-LEAK-RATE"
	Comment	"Proportion of outputs/log entries with detected PII."
	ConfidentialityFlag	false
	Assessor	"Quality Engineering"
	AssessmentInterface	"cfg://metric/M-PII-LEAK-RATE"
	metric	key: "pii_leak_rate"unit: "proportion"threshold: "<= 0,5 %"
	requirementRef	"R-PII-01"
Explanation: The metric defines a precise unit and threshold (clause 8.1.4.3) and is structured for machine-readable assessment (clause 8.2.2). While a zero-tolerance threshold (0 %) is ideal, it is often impractical due to potential false positives in detection tools. The engineering team documented that a leak rate below 0,5 % represents an acceptable level of risk.		

Table A.2-5: Exemplary Measurement Documentation for PII Leakage Control

Item Component	Attribute	Value / Description
Measurement	*Name*	"MEAS-PII-SCAN"
	Comment	"Combined NER and pattern scanning over outputs and logs."
	ConfidentialityFlag	true
	Assessor	"MLOps"
	AssessmentInterface	"runner://measurements/m_pii_scan"
	method	["ner_based_pii_scan", "pattern_scan"]
	inputArtifacts	["prod_logs/*.jsonl", "sampled_outputs/*.txt"]
	outputUnit	"proportion"
	automation	true
	evidenceRetentionDays	180
	metricRef	"M-PII-LEAK-RATE"
Explanation: The measurement specifies the technique, input artifacts, and automation details (clause 8.1.5). The inputs align with evidence sources (clause 9.2), and the retention period supports persistence requirements (clause 9.3). The MLOps team chose a hybrid approach of a NER model (to find names) and pattern scanning (for emails/phones) to achieve better detection coverage.		

A.2.2.3 Continuous Assessment Report

Table A.2-6 shows an excerpt from an Assessment Report, the final artifact of the Continuous Assessment Cycle (clause 9). This report is automatically generated, providing a verifiable record of the system's conformity status for the specified period.

Table A.2-6: Exemplary Assessment Report Excerpt for PII Leakage Control

Attribute	Value / Description
system_id	"TicketClassifier v1.4"
provider	"ACME GmbH"
window	"2025-07-01..2025-08-01"
requirementResults	requirementRef: "R-PII-01"metricRef: "M-PII-LEAK-RATE"measurementRef: "MEAS-PII-SCAN"value: "0.3%"threshold: "<= 0.5%"status: "pass"evidence: ["evid/pii_scan_2025-08-01.json"]
conformity_status	"conformant"
standards_refs	["EU AI Act Art.15", "GDPR Art.25"]
timestamp	"2025-08-01T09:15Z"
Explanation: This report demonstrates a successful "pass" case. The measured value of 0,3 % is below the specified threshold of 0,5 %. The report maps the measurement result back to the requirement (clause 9.1), persists the evidence link (clause 9.3), and clearly communicates the "conformant" status to stakeholders (clause 9.4). It forms a key part of the "Measurement Results and Evidence" documentation item (clause 10.2.3), providing end-to-end traceability.	

A.3 Use Case: Data Drift Monitoring for Demand Forecasting

A.3.1 Use Case Description

Application Scenario and Risk: ACME Retail Analytics Ltd. provides a demand forecasting AI model to a large e-commerce client. The model predicts sales for thousands of products for the upcoming week, helping the client optimize inventory. The primary risk is data drift. The model was trained on historical sales data, but if customer behaviour changes (e.g. due to a new trend, a competitor's campaign, or economic shifts), the live production data will no longer resemble the training data. If this drift goes undetected, the model's predictions will become inaccurate, leading to costly business errors like overstocking (wasted capital) or stockouts (lost sales).

A.3.2 CABCA Implementation Example

A.3.2.1 General

The following clauses illustrate the application of the CABCA framework to manage the risk of data drift. The example covers the creation of the Operationalization Specification and demonstrates how a non-conformity is handled in a Continuous Assessment Report.

A.3.2.2 Scoping and Operationalization Specification

This example details the Operationalization Specification for monitoring data drift. It translates the high-level goal of maintaining model robustness and accuracy into a concrete, measurable and automated process. See Table A.3-1.

Table A.3-1: Exemplary Conformity Specification for Data Drift Monitoring

Item Component	Attribute	Value / Description
Conformity Specification	*Name*	"CS-DRIFT-01"
	Comment	"Continuous monitoring of data/model drift affecting prediction quality."
	ConfidentialityFlag	false
	Assessor	"Quality Management"
	AssessmentInterface	"doc://conformity/CS-DRIFT-01"
	sources	["EU_AI_Act_Art9", "EU_AI_Act_Art15"]
Explanation: The Quality Management team identified data drift as a major operational risk falling under the EU AI Act's Article 9 (Risk Management System) and Article 15 (Accuracy, Robustness). This Scoping artifact consolidates these legal drivers into a focused compliance objective (clauses 7.1 and 7.2).		

Table A.3-2: Exemplary Quality Dimension Specification for Data Drift Monitoring

Item Component	Attribute	Value / Description
Quality Dimensions	*Name*	"QD-DRIFT"
	Comment	"Dimensions for drift control."
	ConfidentialityFlag	false
	Assessor	"Quality Management"
	AssessmentInterface	"doc://dimensions/QD-DRIFT"
	dimensions	["robustness", "accuracy"]
Explanation: Significant data drift directly impacts the model's "robustness" (its ability to handle new data) and its "accuracy" (the quality of its predictions). These dimensions were chosen as they directly map to the business risk and the conformity specification (clause 8.1.2).		

Table A.3-3: Exemplary Requirement Specification for Data Drift Monitoring

Item Component	Attribute	Value / Description
Requirement	*Name*	"R-DRIFT-01"
	Comment	"Significant population drift should be detected and addressed."
	ConfidentialityFlag	false
	Assessor	"Quality Engineering"
	AssessmentInterface	"cfg://req/R-DRIFT-01"
	Frequency	"daily && on_deploy"
	fromConformitySpecification	"CS-DRIFT-01"
	qualityDimensionsRef	"QD-DRIFT"
	traceToSource	["EU_AI_Act_Art9"]
Explanation: This requirement translates the abstract risk of drift into a concrete, testable rule. The daily frequency is chosen because market conditions can change quickly in retail. This adheres to the criteria in clause 8.1.4.		

Table A.3-4: Exemplary Metrics Specification for Data Drift Monitoring

Item Component	Attribute	Value / Description
Metrics	*Name*	"M-PSI"
	Comment	"Population Stability Index as drift indicator."
	ConfidentialityFlag	false
	Assessor	"Quality Engineering"
	AssessmentInterface	"cfg://metric/M-PSI"
	metric	key: "population_stability_index"unit: "index"threshold: "<= 0.20"
	requirementRef	"R-DRIFT-01"
Explanation: The Population Stability Index (PSI) is an industry-standard metric for data drift. A common rule is that PSI < 0,1 is stable, 0,1 - 0,25 is moderate drift, and > 0,25 is major drift. The team set a threshold of 0,20 as the trigger for an alert, providing a clear, unambiguous metric (clause 8.1.4.3).		

Table A.3-5: Exemplary Measurement Documentation for Data Drift Monitoring

Item Component	Attribute	Value / Description
Measurement	*Name*	"MEAS-PSI"
	Comment	"Compare training vs. production feature distributions."
	ConfidentialityFlag	true
	Assessor	"MLOps"
	AssessmentInterface	"runner://measurements/m_psi"
	method	"compare(train_feature_dist, prod_feature_dist)"
	inputArtifacts	["train_stats/*.json", "prod_stats/daily/*.json"]
	outputUnit	"index"
	automation	true
	evidenceRetentionDays	365
	metricRef	"M-PSI"
Explanation: The implementation statistically compares feature distributions between the original training data and recent production data, providing an automated and repeatable measurement process (clause 8.1.5).		

A.3.2.3 Continuous Assessment Report

The following excerpt from an Assessment Report demonstrates a "fail" case where data drift was detected, triggering a non-conformity status and a corrective action plan.

Table A.3-6: Exemplary Assessment Report Excerpt for Data Drift Monitoring

Attribute	Value / Description
system_id	"DemandForecaster v3.2"
provider	"ACME Retail Analytics Ltd."
window	"2025-08-01..2025-08-07"
requirementResults	requirementRef: "R-DRIFT-01"metricRef: "M-PSI"measurementRef: "MEAS-PSI"value: 0.27threshold: "<= 0.20"status: "fail"evidence: ["evid/psi_2025-08-07.json"]
nonconformities	id: "NC-DRIFT-20250807"description: "PSI above threshold for three consecutive days."corrective_action: { due: "2025-08-15", plan: ["retrain_on_recent_data", "update_feature_normalization"]}
conformity_status	"non-conformant (temporary)"
standards_refs	["EU AI Act Art.9", "EU AI Act Art.15"]
timestamp	"2025-08-07T06:30Z"
Explanation: This report shows a "fail" case. The measured PSI value of 0,27 exceeds the threshold of 0,20, triggering a non-conformity. The system status is updated to "non-conformant," and the report automatically documents the issue and outlines a corrective action plan (retrain the model). This demonstrates the full feedback loop of CABCA: detect, report, and plan for remediation, ensuring risks are actively managed (clauses 9.1 and 9.4).	

Note on traceability (both examples): Each chain follows Results → Metrics → Requirement → QualityDimensions/ConformitySpecification as required by clause 10.3, and all items are machine/human-readable to support automated execution and stakeholder review (clauses 8.2.2, 8.2.3, 10.1 and 10.2).

History

Document history		
V1.1.1	January 2026	Publication