ETSI TS 6756 V0.0.2 (2023-06)

MTS: Continuous Auditing Based Conformity Assessment for AI-enabled systems

<

**TECHNICAL SPECIFICATION**

Reference

DTS/MTS-6756

Keywords

Conformity,assesment

***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

***Important notice***

The present document can be downloaded from:
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at [www.etsi.org/deliver](http://www.etsi.org/deliver).

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at <https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

***Notice of disclaimer & limitation of liability***

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or

other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

***Copyright Notification***

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI yyyy.

All rights reserved.

Contents

Intellectual Property Rights 4

Foreword 4

Modal verbs terminology 4

Executive summary 4

Introduction 4

1 Scope 5

2 References 5

2.1 Normative references 5

2.2 Informative references 5

3 Definition of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 6

3.3 Abbreviations 6

4 CABCA Fundamentals 6

4.1 Definition of Continuous Auditing Based Conformity Assessment (CABCA) 6

4.2 Differences of CABCA compared to traditional "point-in-time" and self-assessment methods 6

Principles 7

CABCA Assessment Process 7

Architecture, Roles, Procedures 7

Compliance 7

Risk-based quality requirement definition 8

Operationalization of quality requirements 8

Automated Assessment 8

Automated quality assessments using an assessment engine 8

Outcome of the assessments (update of conformity status) 9

CABCA in MLOps 9

Quality requirement definition based on AI-Risk-Management Frameworks 9

CABCA implementation in MLOps 9

Collection of relevant artifacts generated during the ML lifecycle 9

Evaluation and reporting of collected evidence via an API and Assessment Engine 10

Publication of a live conformity status on a third-party platform 10

Conclusion 10

Summary of the key points discussed in the document 10

Annex A (normative or informative): Title of annex 11

Annex (informative): Bibliography 12

Annex (informative): Change History 13

History 14

# 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 Web server ([https://ipr.etsi.org](https://ipr.etsi.org/)).

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™**and **LTE™** 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 {ETSI Technical Committee|ETSI Project|<other>} <long techbody> (<short techbody>).

# 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](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx) (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

# Introduction

# 1 Scope

The present document specifies the key aspects of Continuous Auditing Based Conformity Assessment (CABCA) as an audit methodology to evaluate and asses an organization's conformity to relevant standards and regulations.

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 at <https://docbox.etsi.org/Reference>.

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]

## 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 are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1]

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the [following] terms [given in ... and the following] apply:

**Conformity Assessment:** The process of evaluating and determining whether a product, service, or system complies with specified requirements, such as standards or regulations.

**Continuous Auditing:** An ongoing process of collecting, analyzing, 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.

**MLOps:** A set of practices and methodologies for managing the lifecycle of machine learning (ML) models, including development, deployment, and maintenance.

**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.

**Assessment Engine:** A software component that automates the evaluation of collected artifacts against predefined quality criteria to generate quality assessment outcomes.

## 3.2 Symbols

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

## 3.3 Abbreviations

For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

**CABCA:** Continuous Auditing Based Conformity Assessment, a dynamic approach to evaluating and confirming an organization's adherence to relevant standards and regulations.

**ML:** Machine Learning, a subset of artificial intelligence that involves the development of algorithms and models capable of learning from and making predictions or decisions based on data.

**AI:** Artificial Intelligence, the development of computer systems capable of performing tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and natural language understanding.

**API:** Application Programming Interface, a set of rules and protocols that allow software components to interact and share data with each other.

**GDPR:** General Data Protection Regulation, a comprehensive data protection law in the European Union that governs the processing and handling of personal data.

**ISO:** International Organization for Standardization, an independent, non-governmental international organization that develops and publishes international standards.

# 4 CABCA Fundamentals

## 4.1 Definition of Continuous Auditing Based Conformity Assessment (CABCA)

This section provides a concise definition of CABCA, explaining what it is and what it entails.

* Continuous Auditing Based Conformity Assessment (CABCA) is a dynamic approach to evaluating and confirming an organization's adherence to relevant standards and regulations. CABCA emphasizes ongoing conformity, stakeholder trust, and adaptability by continuously monitoring and assessing the organization's processes and systems.
* Small explanation of the principles underlying CABCA
* Small overview of CABCA processes and their benefits

## 4.2 Differences of CABCA compared to traditional "point-in-time" and self-assessment methods

This section highlights the benefits of using CABCA over traditional certification and self-assessment methods

* Explanation of the differences between traditional certification, self-assessment, attestation approaches, and Continuous Auditing Based Conformity Assessment (CABCA)
* Benefits of CABCA, including real-time monitoring, adaptability, enhanced risk management, and stakeholder trust
* Comparison of the level of detail and depth of assessment in traditional certifications, self-assessments, and attestations vs. CABCA
* Advantages of CABCA in maintaining transparency, demonstrating an organization's ongoing commitment to quality, and fostering trust among stakeholders
* Emphasis on continuous improvement and adaptability, allowing organizations to adjust and refine their conformity assessment processes according to the evolving regulatory landscape and emerging risks
* Similarities in integration of risk-based quality requirements and risk management
* Greater focus on stakeholder awareness, communication, and trust-building status and commitment to maintaining adherence to relevant standards and regulations.

## Principles

This section outlines the basic principles that underpin CABCA, such as independence, reliability, stakeholder trust and transparency.

* Explanation of the guiding principles that underlie the CABCA assessment process
* Discussion of the core beliefs and values that drive the CABCA assessment methodology
* Outline of the criteria used to determine the suitability of standards and regulations for CABCA conformity assessment
* Ensuring a more standardized approach to conformity assessment
* Greater focus on stakeholder awareness, communication, and trust-building, ensuring that all parties involved have a clear understanding of the organization's conformity status and commitment to maintaining adherence to relevant standards and regulations
* Explanation of how CABCA helps organizations maintain transparency, foster trust among stakeholders, and demonstrate ongoing commitment to quality and compliance.
* Independence of the audit from the information retrieval and measurement.

# CABCA Assessment Process

## Architecture, Roles, Procedures

This section details the technical architecture of CABCA, including the components and their interactions, as well as the roles and procedures involved in the assessment process.

* Definition and description of the CABCA architecture
* Explanation of the roles and responsibilities involved in the CABCA process
* Details of the procedures involved in CABCA assessment, including evidence collection, assessment, and reporting
* Explanation of the separation of evidence collection and assessment to ensure independence of the audit.
* Overview of the technical requirements and protocols used to implement CABCA.

## Modes of CABCA

* Self-Assessment: Internal audits for compliance.
* Third-Party Audit: External audits for adherence to standards.
* Certification: Assistance in procuring certifications from accredited bodies.

## Understanding, Adapting, and Implementing Compliance

This section explains the concept of compliance and how it is used in CABCA to ensure that systems are in line with applicable standards or regulations.

* Compliance Categories:
	+ ISO Standards: It's about putting into practice and sticking to globally acknowledged benchmarks.
	+ Sector Regulations: Adhering to directives established by governing bodies in distinct sectors.
	+ Market Rules: Complying with the regulations that dominate specific markets or regions.
	+ Customer Demands: Fulfilling unique client needs, inclinations, and anticipations.
	+ Alternative Compliance Forms: Observing other relevant guidelines or norms.
* Adjusting Compliance Strategy: It's important to realize that compliance types can vary significantly in their precision and level of abstraction. Depending on these factors, different strategies, including risk management methods, may be needed to translate the compliance requirements into concrete operational measures.
	+ Different compliance types may necessitate various methods for deriving operational requirements. For example, high-precision compliance types might call for a direct translation of the given standards, while more abstract types might require methods like risk management to interpret and derive the necessary requirements.
	+ Not every element of a compliance or conformity document will be applicable to every system. It is necessary to identify which parts of the compliance document are relevant to our system and should be focused on during the operationalization process.
* Capability principles for the Operationalization Method
	+ Break down compliance needs to requirements

## Risk-based quality requirement definition

This section describes how quality requirements are defined and evaluated in CABCA, based on a risk-based approach.

* Definition of risk-based quality requirement definition
* Explanation of how CABCA uses risk management to determine quality requirements
* Overview of the steps involved in risk-based quality requirement definition for CABCA conformity status
* Discussion of the importance of considering emerging risks and how CABCA addresses this
* Discussion of the role of stakeholders in defining quality requirements
* Discussion of how CABCA adjusts quality requirements over time to respond to changing system conditions and emerging risks.

## Operationalization of quality requirements

This section explains how quality requirements are put into practice in CABCA, including how they are monitored and verified.

* Overview of the process of operationalizing quality requirements for CABCA conformity status
* Steps for defining and implementing quality requirements for the CABCA process
* Role of different stakeholders (e.g. certifying bodies, auditors, and end-users) in the operationalization process
* Considerations for defining quality requirements (e.g. data security, privacy, and accuracy)
* Methods for ongoing monitoring and updating of quality requirements
* Evidence-based approaches for verifying the operationalization of quality requirements.

## Operationalization Requirements

* Adapt, Define or derive requirements.
* Define metrics for each requirement.
* Define a frequency for each requirement for assessment
* Assign measurements to each requirement and metric.

## Building Stakeholder Trust through CABCA

CABCA builds trust by fostering transparency, facilitating effective communication, regularly updating compliance status, and incorporating third-party audits.

### Transparency Requirements

* Communicate risk mitigation methods.
* Reduce regulatory uncertainties by providing interpretations.
* Communicate quality requirements.
* Be transparent about how conformity is implemented and assessed, the scope of the assessment, and updates in the implementation.
* Openly communicate the results of the Conformity Assessment without revealing crucial insights into the ML System.

### Communication Requirements

* conformity status or other pertinent information.
* Define communication channels and the scope for each channel.
* Define the frequency of communication updates and their granularity.

### Inclusion of Third-Party Expertise

* Involve third-party audits for unbiased assessment and verification of the system’s compliance.
* Define the degree of third-party involvement in conformity implementation, assessment, and setup.
* Ensure separation between the ML System and the Audit System.

### Digital Records/Data/Evidence Collection and Storage

* Define the persistence of assessment results and necessary evidence.

# Automated Assessment

Collection of relevant artifacts

This section explains how relevant artifacts, such as data, models, and performance metrics, are collected and stored in CABCA.

* Explanation of relevant artifacts used in the CABCA assesment process
* Methods for collecting artifacts, including automating the monitoring and collection of data from different parts of the system
* Overview of secure protocols and access controls used to ensure data security and privacy during data transfer and storage
* Explanation of how the collected artifacts are used in the automated quality assessments.

## Automated quality assessments using an assessment engine

This section describes how the assessment engine uses pre-defined quality criteria to perform automated quality assessments.

* Overview of the automated quality assessment process using an assessment engine
* The role of the assessment engine in conducting continuous quality assessments
* Explanation of the pre-defined quality criteria used by the assessment engine
* Continuous quality assessments based on pre-defined quality requirements
* Implementing measurements for quality
* Overview of the data inputs required for the assessment engine (relevant artifacts)
* Mapping results of multiple measurement tools and other data to a combined input for the assessment
* Discussion of the assessment engine's evaluation methodology and decision-making process
* Explanation of the outcomes of the assessment

## Outcome of the assessments (update of conformity status)

This section describes the outcome of the quality assessments, including the update of the conformity status.

* Explanation of the outcome of the assessments performed by the assessment engine
* Evaluation of measurement results, taking artifacts as input, against predefined values derived from expert knowledge and risk assessment
* Issuance of conformity status if the measurement results align with predefined values, indicating compliance with required standards
* Revocation or adjustment of conformity status if the measurement results do not meet predefined values, highlighting areas for improvement and increased risk management
* Discussion of the process for updating or revising the pre-defined quality requirements and the corresponding impact on the assessment outcome

# CABCA in MLOps

## Quality requirement definition based on AI-Risk-Management Frameworks

This section explains how quality requirements for ML systems are defined in CABCA using AI-Risk-Management frameworks.

* Overview of AI-Risk-Management Frameworks and their relevance for CABCA
* Definition of quality requirements for CABCA in the context of AI-Risk-Management
* Integration of AI-Risk-Management Frameworks with CABCA processes
* Alignment of CABCA quality requirements with AI-Risk-Management best practices and standards
* Definition of risk-based quality requirements for AI systems, models and their components
* Continuous updating and refinement of quality requirements based on changes in the AI-Risk-Management landscape.

## CABCA implementation in MLOps

This section describes how CABCA is implemented in the context of MLOps, including the processes, procedures, and tools involved.

* Explanation of the integration of CABCA into the MLOps pipeline
* Overview of how CABCA fits into the ML lifecycle
* Discussion of the benefits of incorporating CABCA into MLOps
* Explanation of how CABCA can improve the quality and reliability of ML models
* Discussion of the role of CABCA in managing AI-related risks in MLOps
* Overview of the process for defining and implementing quality requirements for ML models in the context of CABCA.

## Collection of relevant artifacts generated during the ML lifecycle

This section explains how relevant artifacts generated during the ML lifecycle are collected and used for quality assessment in CABCA. Artifacts used for quality assessment (data, model, architecture, configurations, hyperparameters, algorithm, metrics, logs, etc.) - This subsection provides a list of the artifacts that are used for quality assessment in CABCA.

* Overview of relevant artifacts generated during the ML lifecycle
* Collection of artifacts relevant to the quality assessment process
* Examples of artifacts: data, model, architecture, configurations, hyperparameters, algorithm, metrics, logs, etc.
* Procedures and tools used to collect the artifacts
* Automated collection of artifacts at various stages of the ML lifecycle
* Record-keeping of collected artifacts for future reference.

## Evaluation and reporting of collected evidence via an API and Assessment Engine

This section describes how the collected evidence is evaluated and reported in CABCA, using an API and assessment engine.

* Overview of the process for collecting evidence related to the ML lifecycle
* Explanation of how the evidence is evaluated and reported through an API and assessment engine
* Details on how the API and assessment engine interface to produce a comprehensive evaluation report
* Discussion of how the report influences the conformity status update.

## Publication of a live conformity status on a third-party platform

This section explains how the results of the quality assessments are published in CABCA, including the publication of the conformity status.

* Explanation of the concept of publishing a live conformity status on a third-party platform
* Steps involved in publishing a live conformity on a governing body platform
* Details of the publishing platform, including its purpose, features, and accessibility
* Benefits of publishing a live status conformity on a governing body platform, such as increased transparency and credibility
* Explanation of how a live conformity status can be updated based on continuous quality assessments

# Conclusion

## Summary of the key points discussed in the document

This section provides a summary of the key points discussed in the document, highlighting the main benefits and drawbacks of CABCA.

Annex A (normative or informative):
Title of annex

Annex (informative):
Bibliography

Annex (informative):
Change History

| Date | Version | Information about changes |
| --- | --- | --- |
| <Month year> | <#> | <Changes made are listed in this cell> |
|  |  |  |
|  |  |  |
|  |  |  |

# History

|  |
| --- |
| **Document history** |
| <Version> | <Date> | <Milestone> |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*Latest changes made on 2022-03-14*