10th UCAAT

User Conference on Advanced Automated Testing

ETSI The Standards People

Continuous Auditing Based Conformity Assessment

Dorian Knoblauch

Fraunhofer FOKUS

15/11/2023

CABCA and its Importance for MLOps/ML

Current:

- Automated testing → High iteration cycles.
- DevOps: Rapid, iterative pinnacle.
- Traditional certification: Slow & outdated.
- Need for audited changes in AI & ML.
- Establish trust in AI & ML systems.

Solution:

- CABCA: Aligns ML to standards & quality.
- Filling the gap with real-time assessments.

Example

- AI in Traffic Management
  - Vehicle Classification System
  - Utilization of Open-Source AI Models
    - Enhancement with own data

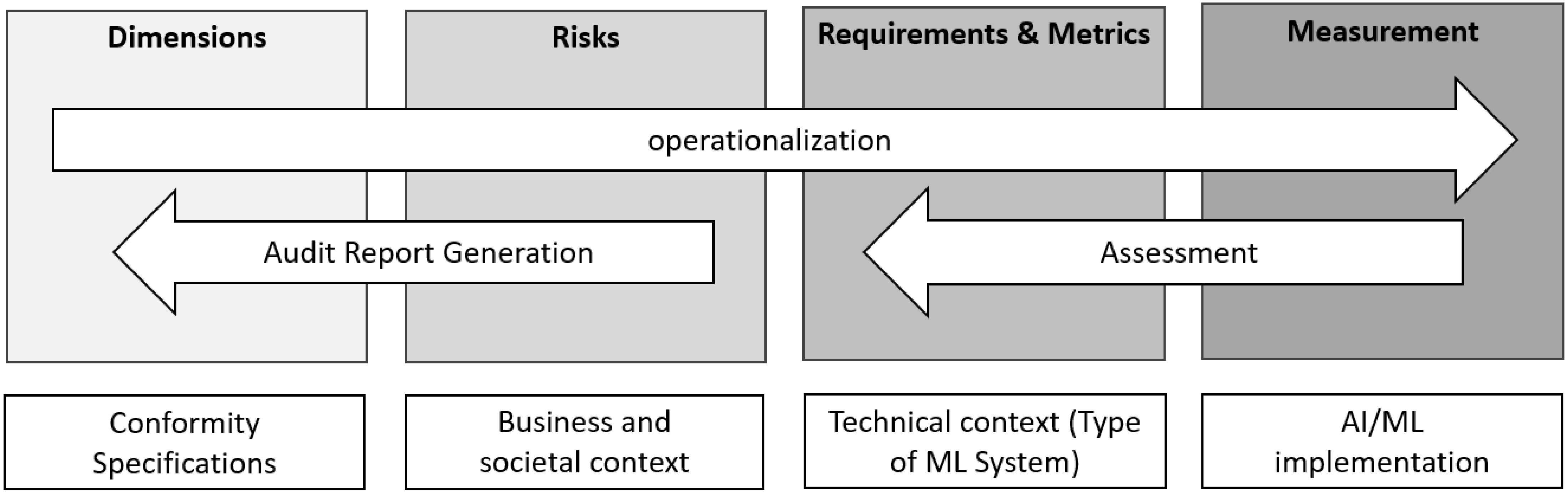
Compliance with Privacy and Security Regulations:

System Robustness and Data Integrity

Conformity Specifications for CABCA

- Conformity Specifications refer to high-level documents that specify the types of conformity required in a particular context.
- Sources vary based on industry, market standards, and organizational needs.
- Examples: ISO, National Standards like NIST, Industry Guidelines, Legislative Requirements, Ethical Guidelines.

Operationalization



Dimensions

Risks

Requirements & Metrics

Measurement

operationalization

Audit Report Generation

Assessment

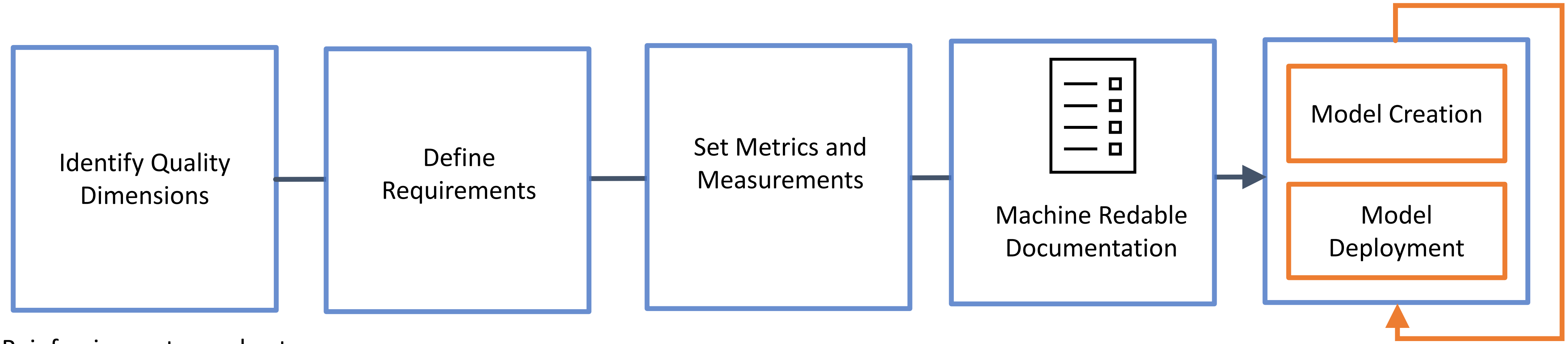
Conformity Specifications

Business and societal context

Technical context (Type of ML System)

AI/ML implementation

CABCA Process - Initalisation

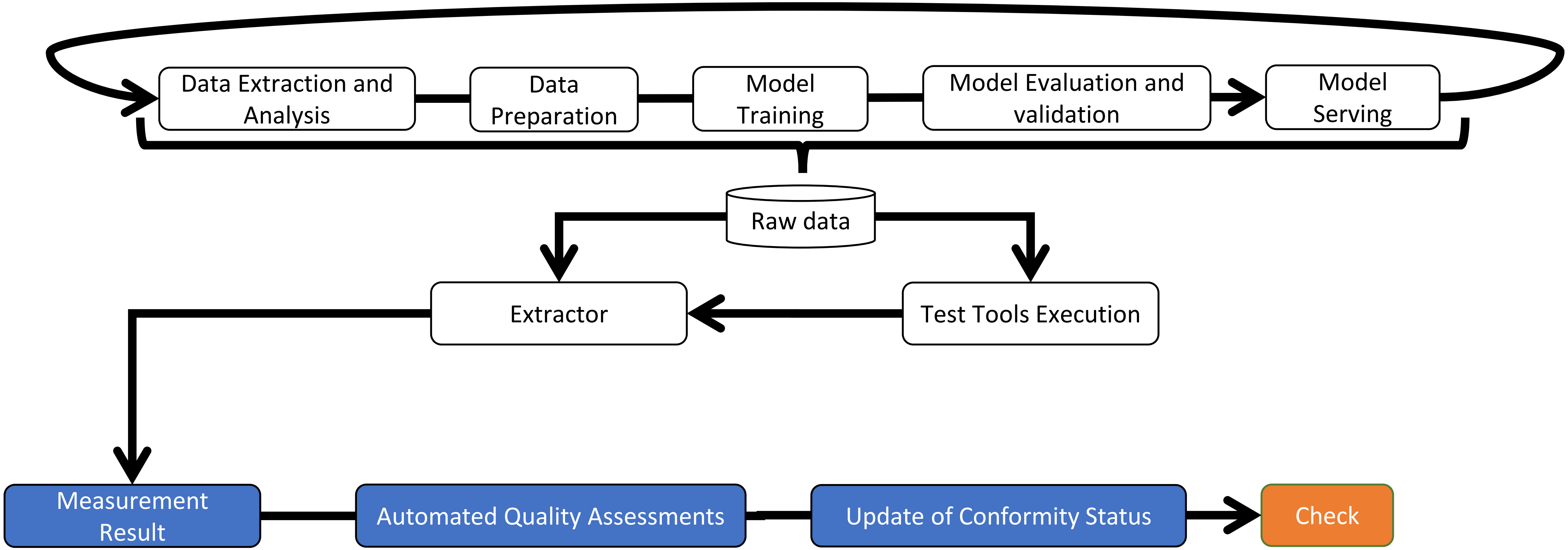

Identify Quality Dimensions
Define Requirements
Set Metrics and Measurements
Machine Redable Documentation
Model Creation
Model Deployment

- Reinforcing system robustness.
- Assuring compliance with data protection.
- Identifying and mitigating security threats.

- Removing Personal Identifiable Information (PII) from datasets.
- Enhancing defenses against adversarial attacks.
- Ongoing anomaly detection and management.

- Ensuring 0% PII in training data.
- Achieving a 10% resilience improvement against attacks.
- Continuous operational anomaly monitoring.

Evidence Collection, Assessment, and Reporting



Data Extraction and Analysis
Data Preparation
Model Training
Model Evaluation and validation
Model Serving
Raw data
Extractor
Test Tools Execution
Measurement Result
Automated Quality Assessments
Update of Conformity Status
Check

Stakeholder Trust

- CABCA enforces transparency & communication.
- Regular reporting & auditing through Audit Report Publication keeps stakeholders informed, enhancing understanding & compliance activities.

Benefits of CABCA

- Real-time quality improvement.
- Detect & mitigate risks early.
- Stay aligned with changing standards.
- Boost trust & confidence.

Challenges and Limitations

- Shifting from traditional methods: A challenge.
- Not fully automated: Manual assessment.
- Need expertise for Operationalization and Documentation.
- Still Operationalization can be subjective
- There is still a delta of aspect that are not measurable but play a role for the overall quality
- Secure data management & adhering to standards.

Conclusion & Current Works

- Conclusion:
  - CABCA: Essential for MLOps assessments.
  - CABCA = Quality, reliability, trust in evolving ML.
  - Boosts stakeholder trust & competitiveness.

- Current woks:
  - Technical specification draft in progress.
  - Part of MTS AI group.
  - reach you to me or Jürgen if you want to contribute

Any further questions?

Dorian Knoblauch
dorian.knoblauch@fokus.fraunhofer.de