QI DIGITAL

Akkreditierung und Konformitätsbewertung im Kontext von Künstlicher Intelligenz

- Vorstellung des Arbeitsstandes (09/22) „Landkarte-Konformitätsbewertung“
- Ing. Prof. Dr. Raoul Kirmes M.Sc. Deutsche Akkreditierungsstelle

Agenda

1. Aufgabe der DAkkS in der QI und Grundlagen
2. Lebenszyklus eines KI-Systems als Anknüpfung
3. Funktionaler Ansatz der Konformitätsbewertung
4. KI-Landkarte als Strukturkarte
5. Identifizierte Lücken im System

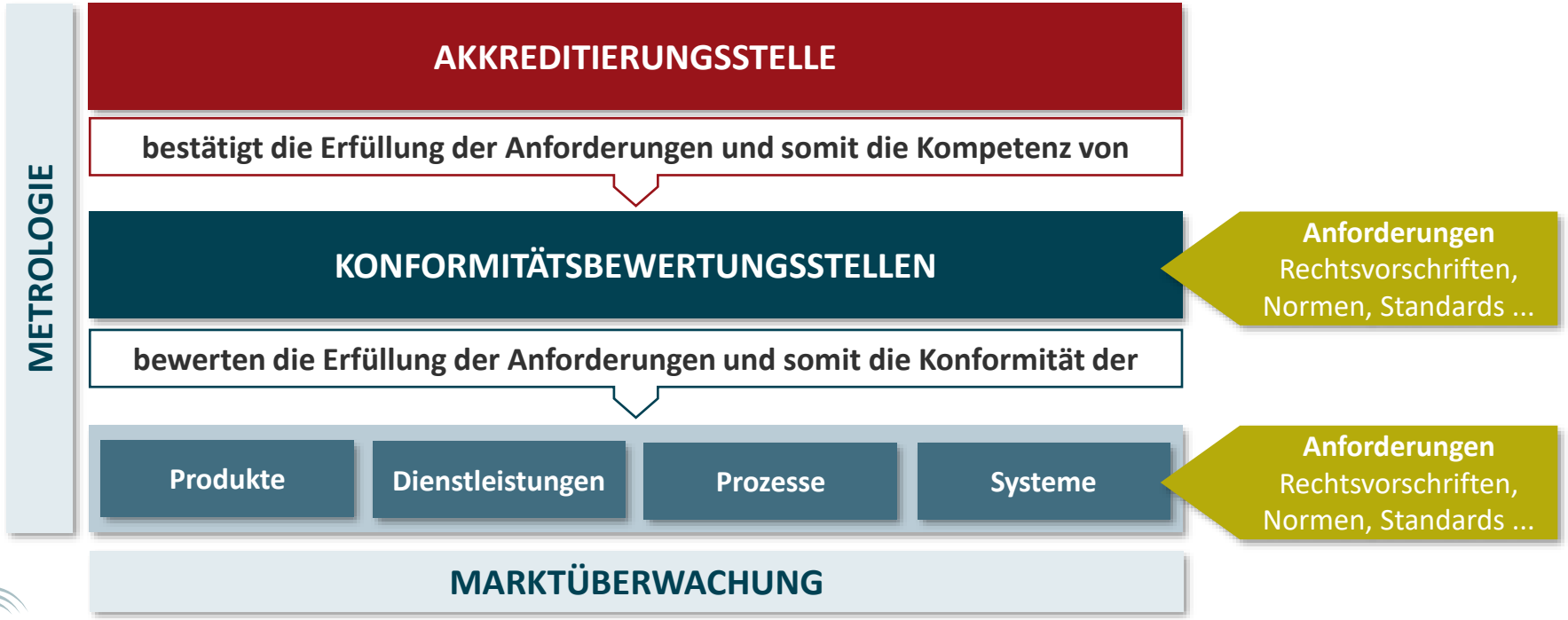
Aufgabe der DAkkS

ÜBER DIE DAKKS

Die DAkkS…

- ist **europäische und international anerkannt** als einzige Akkreditierungsbehörde Deutschlands
- hat einen **gesetzlichen Auftrag**: Beleihung durch BRD
- ist **unabhängig**, **überparteilich** und steht **nicht im Wettbewerb**
- ist zuständig für die **Akkreditierung von Konformitätsbewertungsstellen**
  - z.B. Laboratorien, Inspektions- und Zertifizierungsstellen
- Akkreditierung umfasst die **Begutachtung, Bestätigung und Überwachung** der fachlichen Kompetenz
- ist zentraler Akteur der deutschen **Qualitätsinfrastruktur**

Qualitätsinfrastruktur (QI)



HORIZONTALE QUALITÄTSINFRASTRUKTUR

Normungssystem der Akkreditierung

Einordnung Prüfverfahren in Levelstruktur

DAkkS Deutsche Akkreditierungsstelle

Level 1

- **17011** ← Anforderungen an Akkreditierung

Level 2

- **Kalibrieren**
- **Prüfen**
- **Inspizieren**
- **Zertifizieren**
- **Verifizieren**
- **EP Anbieten**
- **RM Herstellen**

← Tätigkeiten der Konformitätsbewertung

Level 3

- 17025
- 17025
- 15189
- 17020
- 17021-1
- 17065
- 17024
- 17029
- 17043
- 17034

← Anforderungen an KBS und Prozesse

Level 4

- **Sektorale Ergänzungen zu Level 3** ← Erhöhung des Mindeststandards aus Level 3
- **Konformitätsbewertungsprogramme gemäß ISO/IEC 17067; ISO/IEC 17030** ← Reproduzierbarkeit/ Kennzeichnung/ Kompetenz etc.
- **Sektorspezifische Spezifikation von Prüfverfahren und Methoden** ← Anforderungen an Verfahren und Methoden zu sektoral spezifischen KI-Systemen

Level 5

Anforderungen an den <u>Gegenstand</u> der Bewertung (KI-System).
→ Stand-alone KI-System und KI-System als Teil eines Produktes.
z.B.
ISO/IEC 23053: — Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
ISO/IEC CD 25059: — Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI systems

← **ISO/IEC 17007:2021, 4.2**
Strikte Trennung von Anforderungen „an den Gegenstand der Bewertung“ (Level 5) und „Prüfverfahren“ (Level 3 und 4).

Lebenszyklus eines KI-Systems als erste Grundlage für Anknüpfung der Konformitätsbewertung und Akkreditierung

KI Lebenszyklus als Grundlage für Anknüpfungen

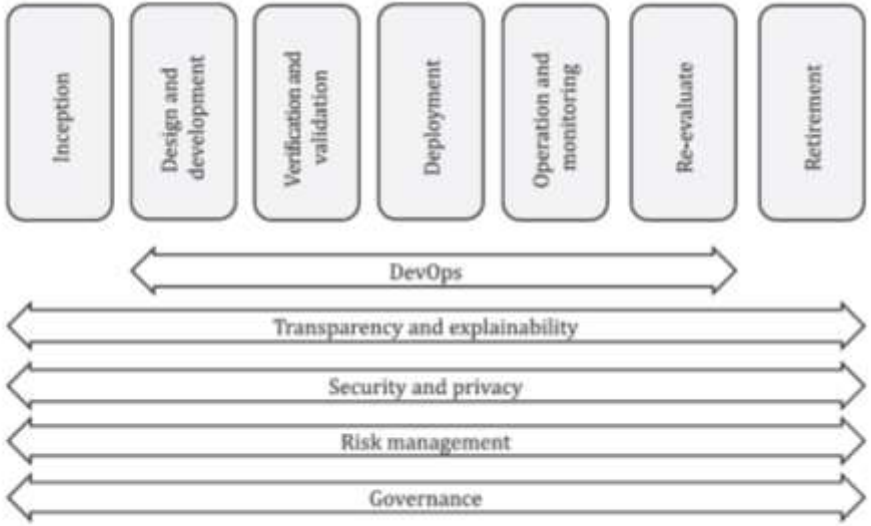


Figure 3 — Example of AI system life cycle model stages and high-level processes

Quelle: ISO/IEC 22989:2022

KI Lebenszyklus als Grundlage für Anknüpfungen

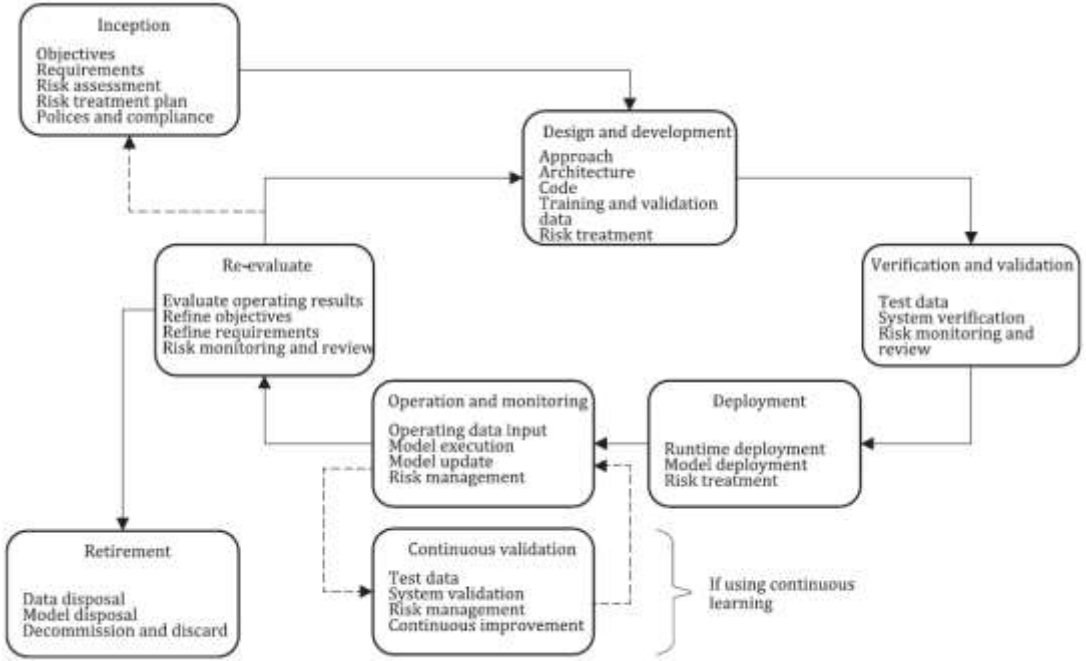
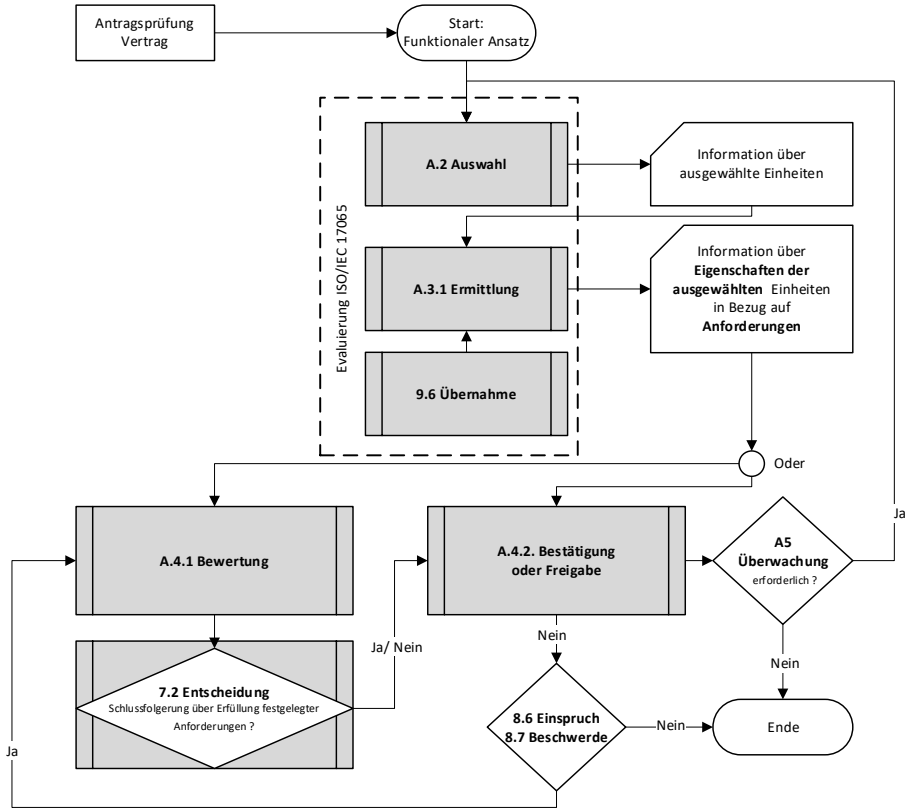


Figure 4 — Example AI system life cycle model with AI system-specific processes

Quelle: ISO/IEC 22989:2022

Funktionaler Ansatz der Konformitätsbewertung als zweite Grundlage für Anknüpfung Konformitätsbewertung und Akkreditierung

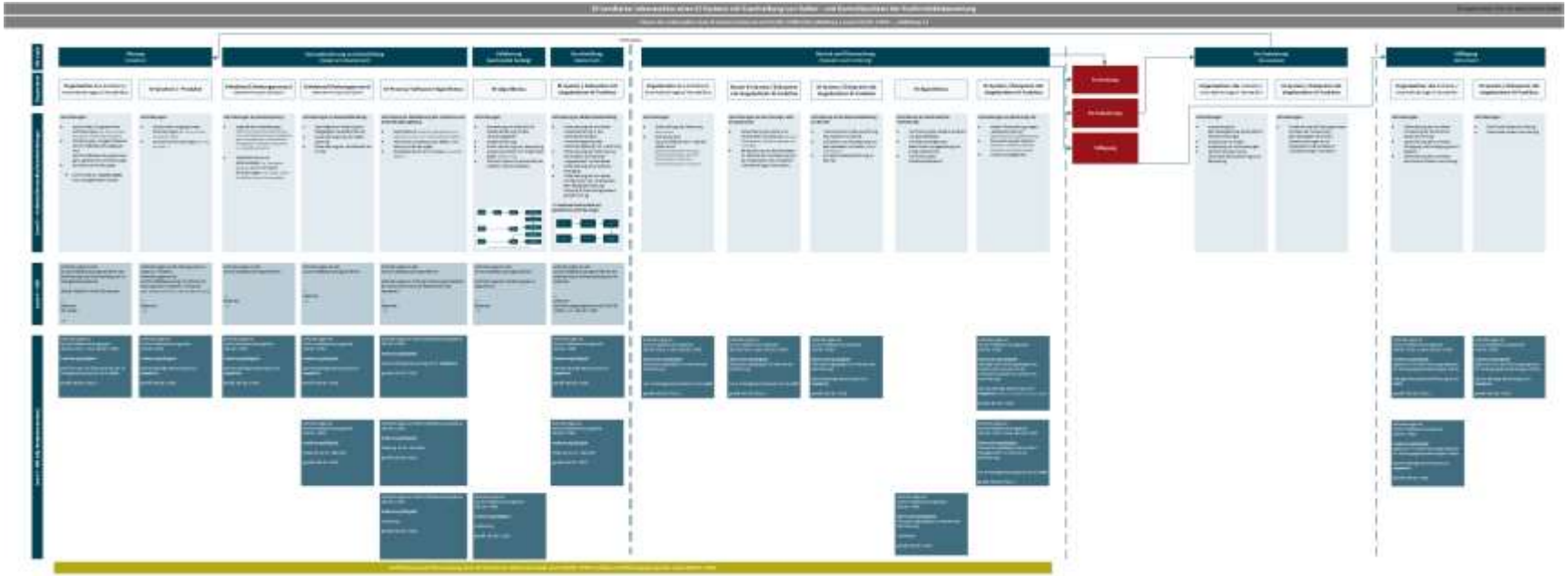
Funktionaler Ansatz für Konformitätsbewertung



Quelle: Eigene Darstellung nach ISO/IEC 17000:2020, Annex A

Arbeitsstand (09/22) einer KI-Landkarte als Strukturkarte für Konformitätsbewertung und Akkreditierung im Bereich Künstliche Intelligenz

KI-Landkarte - Übersicht



KI-Landkarte – Planungs- und Entwicklungsphase

Life Cycle

Planung
(Inception)

Konzeptionierung und Entwicklung
(Design and development)

Gegenstand

Organisation des Anbieters/ Inverkehrbringers/ Herstellers

KI-Systeme / -Produkte

Rohdaten/Erhebungsprozess/
Datensammlung als DB/Quelle

Rohdaten/Erhebungsprozess/
Datensammlung als DB/Quelle

KI-Prozess/-Software/-Algorithmus

Level 5 – Anbieter/Hersteller/Inverkehrbringer

Anforderungen:

- Konformität mit gesetzlichen Anforderungen (z.B. EU AI Act oder Kanadischer AI and Data Act (AIDA))
- Einhaltung der vorgeschriebenen Konformitätsbewertungstypen und Konformitätsbewertungsmodule gem. gesetzlicher Anforderungen
- Normative Anforderungen

→ Konformität zur **ISO/IEC 42001** muss nachgewiesen werden

Anforderungen:

- Konformität mit gesetzlichen Anforderungen (z.B. EU AI Act oder Kanadischer AIDA)
- Normative Anforderungen (z.B. ISO/IEC 5338 ff.)

Anforderungen an Datensammlung:

- Legalität des Datenbezugs (Zweck der Datensammlung, Fairness i.S.d. Anti-Diskriminierung, Löschbarkeit, Nicht-Verkettbarkeit, Vertraulichkeit, Verfügbarkeit, Integrität, Transparenz i.S.v. Betroffenenrechte)
- Qualitätskriterien an Referenzdaten (für Training des Modells), durch normative Anforderungen (z.B. ISO/IEC 5259 ff.; ISO 8000er Reihe zu Datenqualität)

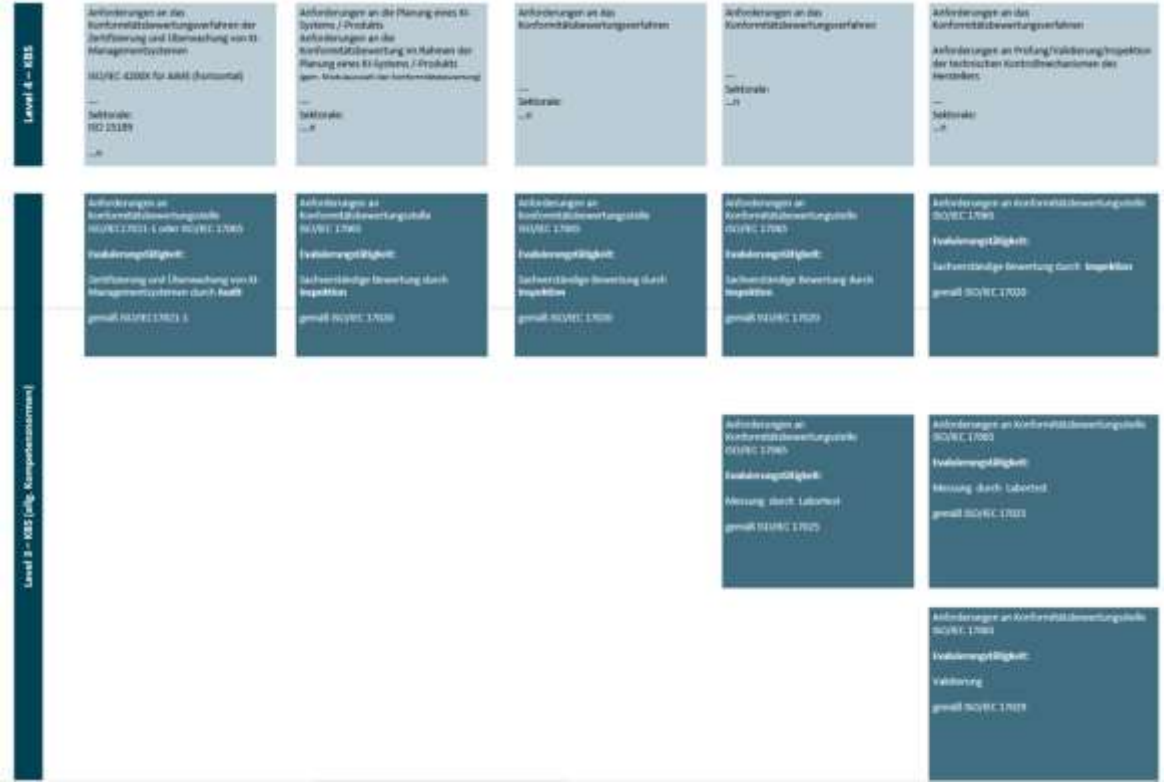
Anforderungen an Datenaufbereitung:

- Nachträgliche Herstellung der festgelegten Qualitätskriterien
- Sicherstellung eines korrekten Labeling
- Sicherstellung der Löschbarkeit als Prinzip

Anforderung an Modellierung des KI-Systems und Entwicklungsumgebung:

- Explainable AI (Grad der Erklärbarkeit des KI-Algorithmus und seiner Funktionalität herstellen)
- Technische Umsetzung von Safety- und Security Anforderungen
- Qualitätskriterien an KI-Modell (z.B. ISO/IEC 25059 ff.)

KI-Landkarte – Planungs- und Entwicklungsphase



DAkkS

KI-Landkarte – Validierungs- und Bereitstellungsphase

Marktzugang

Life Cycle

Validierung (und model testing)

Bereitstellung (Deployment)

Gegenstand

KI-Algorithmus

KI-System / Zielsystem mit eingebetteter KI-Funktion

Level 5 – Anbieter/Hersteller/Inverkehrbringer

Anforderungen:

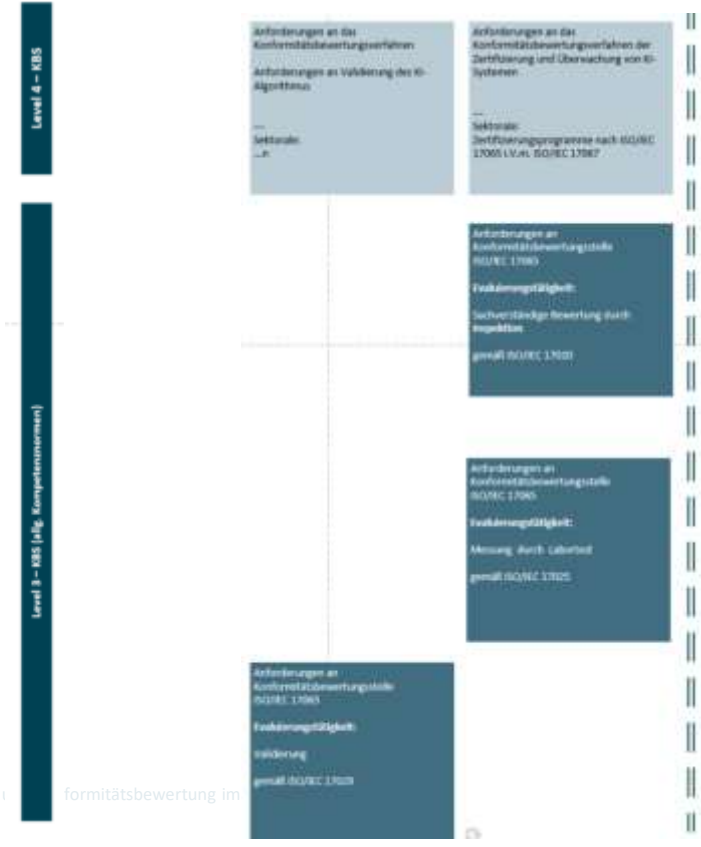
- Anwendung von Metriken für Modellvalidierung mittels Validierungsdaten
- Modellvalidierung
- Risiko Monitoring und -bewertung
- Anpassung Modell mit zusätzlichen Daten (Optimierung)
- Test der finalen Funktionalität des Modells mittels Testdaten

Anforderung an Modell-Bereitstellung:

- Sicherstellung der korrekten Implementierung in die vereinbarte Einsatz/ Umweltumgebung oder Laufzeitumgebung und -verteilung
- Sicherstellung der Optimierung des Modells auf Basis der vorgesehenen Umweltdaten
- Sicherstellung eines sicheren Packaging
- Sicherstellung der korrekten Konfiguration der vereinbarten Betriebsdatenerfassung/ Fernzugriff/Monitoringsysteme gemäß Vertrag

→ Nachweis Konformität mit gesetzlichen Anforderungen

KI-Landkarte – Validierungs- und Bereitstellungsphase



KI-Landkarte – Betriebs- und Überwachungsphase

Life Cycle

Betrieb und Überwachung
(Operation and monitoring)

Gegenstand

Organisation des Anbieters/ Inverkehrbringers/ Herstellers	Nutzer KI-System / Zielsystem mit eingebetteter KI-Funktion	KI-System / Zielsystem mit eingebetteter KI-Funktion	KI-Algorithmus	KI-System / Zielsystem mit eingebetteter KI-Funktion

Level 5 – Anbieter/Hersteller/Inverkehrbringer

Anforderungen:

- Sicherstellung der Steuerung (Governance)
- Einhaltung aller Kontrollmaßnahmen in ISO/IEC 42001-AIMS (Dokumentationsanforderungen, Rollenzuschreibungen, korrekte Steuerung der technischen Kontrollwerkzeuge im KI-System)

Anforderungen an den Nutzungs- oder Einsatzprozess:

- Sicherstellung korrekter und vereinbarter Anwendung (Einsatz in Zielumgebung / Laufzeitumgebung und -verteilung)
- Bereitstellung von Betriebsdaten im Rahmen der Vereinbarung mit der Organisation des Anbieters/ Inverkehrbringers/Herstellers

Anforderung an die Datenverarbeitung im Betrieb:

- Vereinbarte korrekte Ausführung des Systems im Betrieb
- Aufnahme und Verarbeitung von Betriebsdaten ins Modell (Initiale Labeling, etc.)
- Korrekte Modellausführung im Betrieb

Anforderung an kontinuierliche Verifizierung:

- Verifizierung des Modells auf Basis von Betriebsdaten
- Verifikationsergebnisse beeinflussen Ausgestaltung der Risikomaßnahmen
- Verifizierung der Erklärbarkeitsmetrik

Anforderungen an Monitoring von:

- Modell-Überwachung wegen „Selbstoptimierung" (Selbstevaluierung) (Monitoring)
- Überwachung des Systems (Definierte Verhaltensumfänge/ Interaktion mit Systemumwelt)
- Incident Management

Fortsetzung

Re-Evaluierung

Stillegung

KI-Landkarte – Betriebs- und Überwachungsphase

Zertifizierung und Überwachung eines KI-Systems als Softwareprodukt nach ISO/IEC 17065 auf Basis Zertifizierungsprogramm nach ISO/IEC 17067

Level 4 – KBS

Level 3 – KBS (allg. Kompetenznormen)

Anforderungen an Konformitätsbewertungsstelle ISO/IEC 17021-1 oder ISO/IEC 17065

Überwachungstätigkeit: Überwachungstätigkeit im Rahmen der Zertifizierung

von KI-Managementsystemen durch **Audit**

gemäß ISO/IEC 17021-1

Anforderungen an Konformitätsbewertungsstelle ISO/IEC 17021-1 oder ISO/IEC 17065

Überwachungstätigkeit: Überwachungstätigkeit im Rahmen der Zertifizierung

von KI-Managementsystemen durch **Audit**

gemäß ISO/IEC 17021-1

Anforderungen an Konformitätsbewertungsstelle ISO/IEC 17065

Überwachungstätigkeit: Überwachungstätigkeit im Rahmen der Zertifizierung

Sachverständige Bewertung durch **Inspektion**

gemäß ISO/IEC 17020

Anforderungen an Konformitätsbewertungsstelle ISO/IEC 17065

Überwachungstätigkeit: Ständige Überwachungstätigkeit der Modell-Optimierung und der Verhaltensstabilität im Rahmen der Zertifizierung

Sachverständige Bewertung durch **Inspektion** (Annex-versiertes Inspektor-agent)

gemäß ISO/IEC 17020

Anforderungen an Konformitätsbewertungsstelle ISO/IEC 17021-1 oder ISO/IEC 17065

Überwachungstätigkeit: Überwachungstätigkeit des Incident Managements im Rahmen der Zertifizierung

von KI-Managementsystemen durch **Audit**

gemäß ISO/IEC 17021-1

Anforderungen an Konformitätsbewertungsstelle ISO/IEC 17065

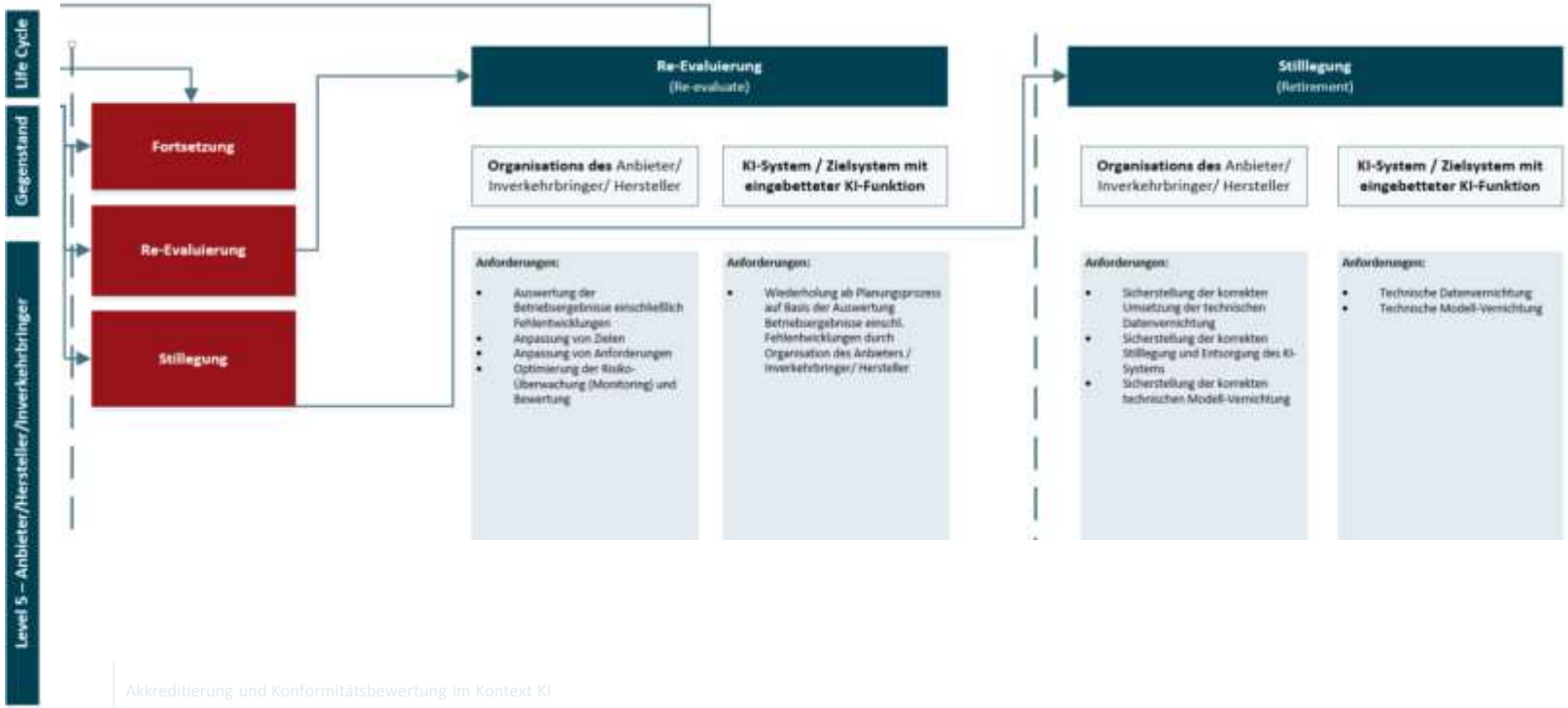
Überwachungstätigkeit: Überwachungstätigkeit im Rahmen der Zertifizierung

Verifikation

gemäß ISO/IEC 17029

DAkkS

KI-Landkarte – Phase: Re-Evaluierung oder Stilllegung



KI-Landkarte – Phase: Re-Evaluierung oder Stilllegung

Level 4 – KBS

Level 3 – KBS (alg. Kompetenzzentrum)

Anforderungen an Konformitätsbewertungsstelle
ISO/IEC 17021-1 oder ISO/IEC 17065

Evaluierungstätigkeit:
Eigene Art von Zertifizierungsprogrammen für Entsorgungsdienstleistungen nötig

Managementsystemzertifizierung durch
Audit

gemäß ISO/IEC 17021-1

Anforderungen an Konformitätsbewertungsstelle
ISO/IEC 17065

Evaluierungstätigkeit:
Eigene Art von Zertifizierungsprogrammen für Entsorgungsdienstleistungen nötig

Sachverständige Bewertung durch
Inspektion

gemäß ISO/IEC 17020

Anforderungen an Konformitätsbewertungsstelle
ISO/IEC 17065

Evaluierungstätigkeit:
Eigene Art von Zertifizierungsprogrammen für Entsorgungsdienstleistungen nötig

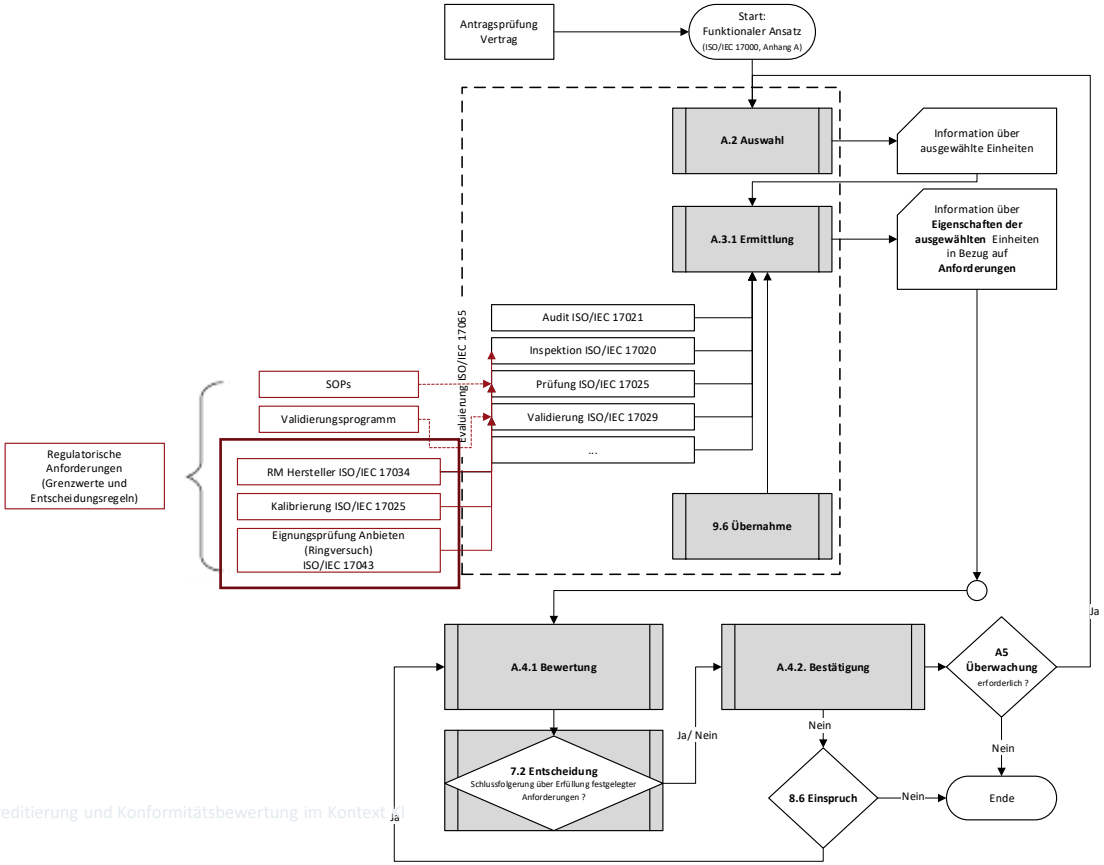
Sachverständige Bewertung durch
Inspektion

gemäß ISO/IEC 17020

Identifizierte Lücken:

Level 4 Normen/ Konformitätsprogramme/ SOP Grundlagen der Konformitätsbewertung

Funktionaler Ansatz für Konformitätsbewertung bei KI



Quelle: Eigene Darstellung nach ISO/IEC 17000:2020, Annex A

Zusammenfassung:

- QI-Konformitätsbewertungssysteme können mit KI-Produkten und Systemen umgehen
- NLF-Systeme (Module) der EU sind grundsätzlich geeignet auch zur Problemlösung im Bereich KI
- **Sektoral besteht Bedarf für Prüfspezifikationen und Konformitätsbewertungsprogramme im Sinne der ISO/IEC 17067 (Level 4)**
- **<u>Kein</u> Bedarf für neue Level 3 Normen!**
- **<u>Großer Nachholbedarf</u>** beseht bei den Grundlagensystemen:

  Eignungsprüfung (Ringversuche)
  Kalibrierung für bestimmte Messungen in Kontext KI
  Referenzmaterialen

www.dakks.de

Kompetenz bestätigen,
Qualität sichern,
Vertrauen schaffen.

DAkkS
Deutsche
Akkreditierungsstelle

Bildnachweis

- Abbildungen zu KI-Lebenszyklus aus ISO/IEC 22989:2022
- Abbildung zu funktionalem Ansatz aus ISO/IEC 17000:2020
- Beispiele akkreditierter Konformitätsbewertung: fotolia / WavebreakMediaMicro
- Beispiele akkreditierter Konformitätsbewertung: fotolia / Kzenon
- Beispiele akkreditierter Konformitätsbewertung: fotolia / Maksim Kabakou
- Beispiele akkreditierter Konformitätsbewertung: iStockphoto
- Beispiele akkreditierter Konformitätsbewertung: Adobe Stock / florinoprea
- Beispiele akkreditierter Konformitätsbewertung: fotolia / bomboman