

trail

Der AI-Governance-Copilot

20% der EU Firmen nutzen AI

(2025, Eurostat)



Bewerbungsroboter

Künstliche Intelligenz diskriminiert (noch)

Der Bewerbungsroboter von Amazon hat Frauen diskriminiert. Wie das passieren? Und wie können Algorithmen geeignete Kandidaten einen Job erkennen?

US-Justiz: Algorithmen benachteiligen systematisch Sc

Air Canada

In den USA wird seit Jahren Faktoren das Rückfallrisiko gar nicht so gut und bewertet

Chatbot verspricht Fluggast irrtümlich Rückerstattung – Airline muss zahlen

Er gewährte einen Rabatt, den es gar nicht gab: Weil ein Chatbot gegen die eigenen Richtlinien verstieß, wollte Air Canada einen Kunden auf dessen Kosten sitzen lassen. Nun entschied ein Gericht gegen das Unternehmen.

Kindergeldaffäre

Niederlande zahlen Millionenstrafe wegen Datendiskriminierung

Ein Skandal um rassistische Diskriminierung bei der Überprüfung von Kindergeldansprüchen erschüttert die Niederlande bis heute. Nun akzeptiert die Regierung ein Bußgeld in Millionenhöhe. Es ist der wohl erste Fall, bei dem eine Regierung für die automatisierte datenbasierte Diskriminierung von Bürger:innen zahlen muss.

Regulatorik muss **pragmatisch** umgesetzt werden

Regulatorik muss **pragmatisch** umgesetzt werden

KI **Compliance** muss **innovationsfreundlich** sein

Regulatorik muss **pragmatisch** umgesetzt werden

KI **Compliance** muss **innovationsfreundlich** sein

KI **Governance** muss **skalierbar** sein

Die Umsetzung ist komplex, zeitaufwändig und unbelastbar

Automatisches Speichern

compliance_checklist_for...

Start Einfügen Zeichnen Seitenlayout Formeln

Zwischenablage Schriftart Ausrichtung Zahlen Bedingte Formate Als Tabelle Zellenformat

G9

Control ID	Control Name	Description
C-001	Access Management	Ensure all user access is formally requested, approved, reviewed and removed from inactive accounts. This and removal of inactive accounts.
C-002	Data Encryption	Encrypt sensitive and regulated data at rest and in transit. Ensure alignment with industry best practices.
C-003	Incident Response Plan	Maintain, document, and test an incident response plan, responsibilities, and communication channels. Conduct tabletop exercises and updates based on lessons learned.
C-004	Audit Logging	Enable and protect audit logging for all critical systems, ensuring immutability where possible. Monitor logs for anomalies and investigate suspicious activities, ensuring immutability where possible.
C-005	Vulnerability Scanning	Perform vulnerability scans on systems and applications. Remediate findings and prioritize findings based on exposure to security threats.
C-006	Patch Management	Apply security patches to operating systems, applications, and hardware within defined timelines. Document exceptions and justify deviations from patch management policies.
C-007	Change Management	Implement a formal change management process for approvals, testing, and rollback procedures to prevent unauthorized or risky system modifications.
C-008	Network Segmentation	Segment networks by business function and sensitivity to reduce lateral movement risks. Enforce strict access controls between segmented zones and monitor traffic for anomalies.
C-009	Backup & Recovery	Ensure regular data and system backups are performed. Periodically test recovery procedures to confirm business-critical data can be restored within required recovery objectives.
C-010	Third-Party Risk	Conduct thorough due diligence and ongoing risk assessments of third-party vendors. Require security attestations, contracts, and monitoring of vendor compliance obligations.
C-011	User Awareness Training	Conduct periodic user security awareness and phishing simulation training. Track participation and measure improvements in employee security behavior over time.
C-012	Multi-Factor Authentication	Require multi-factor authentication for all access to sensitive systems and data. Periodically test MFA mechanisms to ensure reliability and user compliance.

Barrierefreiheit: Keine Probleme

AI Governance: Project #234

File Edit View Insert Format Tools Extensions Help

100% Normal text Proxi... 11

AI Governance: Project #234

Latest update: 01.09.23

OVERVIEW

ent outlines the comprehensive AI governance framework implemented organization's internal credit underwriting project. As artificial intelligence o play an integral role in our credit evaluation processes, ensuring and ethical AI usage is paramount. We aim to collect all important in this document to enable audits and knowledge transfer at a later point.

OLDER

omas Müller, Sanjay Kumar, Emre Avci, Sophia Bauer
s: Anna Rossi, Max Bleek
ia Rösner, Jack Blum

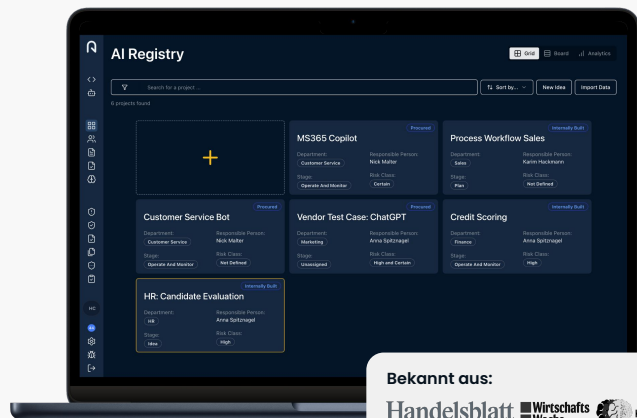
Has the model been tested for bias?

☒ Yes ☐ No

Describe the testing procedure

1. We identified the protected and non protected groups.
2. We defined the favourable outcome: getting hired
3. We calculated the rate of favourable outcome

Mit **trail** Compliance ins KI-Zeitalter bringen



Bekannt aus:

Handelsblatt WirtschaftsWoche KI BUNDESVERBAND



KI-basierte Compliance-Workflows



Effiziente Kollaboration



Audit-fähige Governance



Vertrauenswürdige KI "at Scale"

KI-Governance-Pioniere vertrauen auf trail



Effiziente und automatisierte KI Governance

1

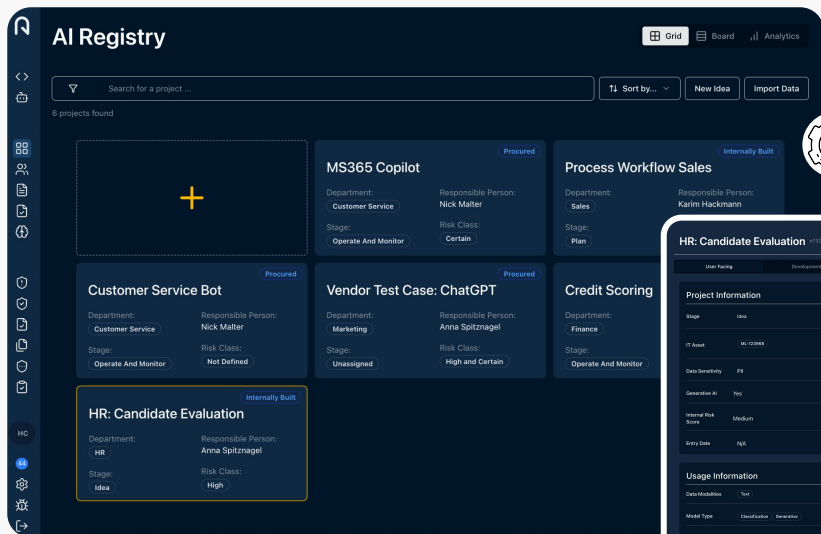
Aufnahme ins KI
Register

Einwertung des
KI Use Cases

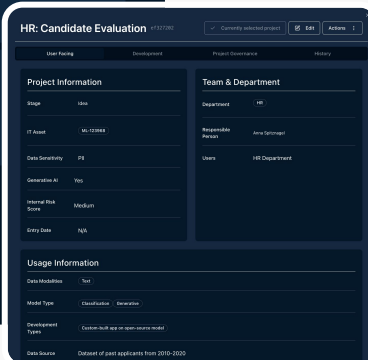
Zuordnung der
Anforderungen

Umsetzung der
Anforderungen

Dokumentation
und Kontrolle



Asset Management
& AI Platforms



- Selbstentwickelte & eingekaufte KI
- ML, GenAI, Agents

Effiziente und automatisierte KI Governance

2

Aufnahme ins KI
Register

Einwertung des
KI Use Cases

Zuordnung der
Anforderungen

Umsetzung der
Anforderungen

Dokumentation
und Kontrolle

The screenshot displays the trail AI Governance interface. At the top, a flowchart shows the process flow: Aufnahme ins KI Register (dark blue), Einwertung des KI Use Cases (dark blue), Zuordnung der Anforderungen (light grey), Umsetzung der Anforderungen (light grey), and Dokumentation und Kontrolle (light grey). The main content area is a questionnaire titled "Haben Sie das KI-System erheblich modifiziert oder seinen Zweck geändert?". It features a progress bar with five steps: 1. Rolle (highlighted), 2. Ausnahmen und Verbote, 3. GPAI-System, 4. Hochrisiko-KI-System, and 5. System mit begrenztem Risiko. The questionnaire text states: "Die Änderung eines KI-Systems (in seinem beabsichtigten Zweck), nachdem es bereits auf den Markt gebracht oder in Betrieb genommen wurde, kann Auswirkungen auf Ihre Verpflichtungen gemäß der KI Verordnung haben." Below the text are two buttons: "Ja, ich habe das System stark verändert oder seinen Zweck geändert" and "Nein, habe ich nicht". At the bottom left, a table titled "EU AI Act" shows the following data:

Role	Risk Class	GPAI Model Provider
Provider	High	No Gpai Model Provider

An "English" button is located at the bottom right of the interface.

Effiziente und automatisierte KI Governance

3

Aufnahme ins KI
Register

Einwertung des
KI Use Cases

Zuordnung der
Anforderungen

Umsetzung der
Anforderungen

Dokumentation
und Kontrolle

Stets aktuelle
Frameworks

Provider - High risk (Annex I A und Annex III)

2/28
2 of 28 fulfilled
Requirement Progress

Chapters

- Chapter IX - Post-market monitoring
information sharing and market surveillance
- Chapter III - High-Risk AI Systems
- Chapter VI - Measures in support of innovation

Active Controls

Linked controls for this requirement

Develop technical system documentation that includes modifications throughout the system lifecycle

Template: Develop technical system documentation that includes modifications throughout the system lifecycle

Description

This control involves developing technical system documentation that includes a detailed record of all modifications made to the AI system throughout its lifecycle. This encompasses changes to the model architecture, training data, algorithms, user interface, and system configurations. Tracking these modifications ensures traceability, supports compliance with regulatory requirements, facilitates post-deployment monitoring, and provides transparency for audits, maintenance, and incident investigations.

Control Response Use trail Documentation Feature

Owners Anna Spitzmuller

Linked Projects HR Candidate Evaluation

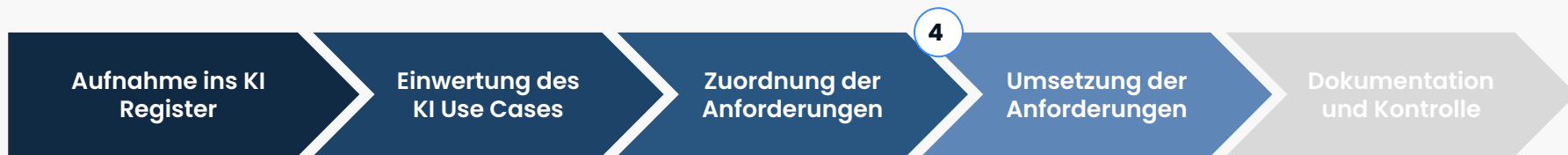
Status Satisfied

Review Period Review every: 365 days
Next review due: 05.10.2024

Chapter IX - Post-market monitoring information sharing and market surveillance

	Evidence	Controls
Post-market monitoring Providers of high-risk AI systems are to establish a post-market monitoring system. This system should collect and analyze data on the performance of these AI systems throughout their lifetime, ensure...	0	1
Owner	Karin Hackmann	Approval Nick Malter
Sharing information on serious incidents Companies who provide high-risk AI systems must report any serious incidents to the authorities in the country where the incident occurred. They must do this as soon as they know there's a link between...	0	0
Owner	Nikolaus Pinger	Approval Nick Malter

Effiziente und automatisierte KI Governance



KI-basierte

- Control-Analyse
- Dokumentation
- Workflows
- Vendor Management
- Risikomanagement
- Explainable AI

Große Control & Risiko-Library

```
from trail import Trail  
with Trail():  
    #your training code here
```

Components Generation

Preview

Data Retention & Deletion - Applicability

Data Retention & Deletion - Effectiveness

Generation Result

Experiment: 8f61ea21 Aug 13 2025 8:54PM Version: v2.0

Generate Document

Generated: Nov 14 2025 - 8:54PM

Control Applicability for Data Retention & Deletion

Applicability Already Applied

The provided source directly addresses the control's requirements concerning the ability to access, extract, and delete customer data. Specifically, customers will have the ability to access, extract, and delete Customer Data stored in each Online Service and Professional Services Data throughout the subscription term or Professional Services engagement ¹. This is further reinforced for EU Customers, who can access, export, and delete EDOA (Customer Data) at any time ². The source also details Microsoft's data deletion policies ³ and general provisions around data access ⁴ and data subject rights ⁵, all of which are relevant to the control.

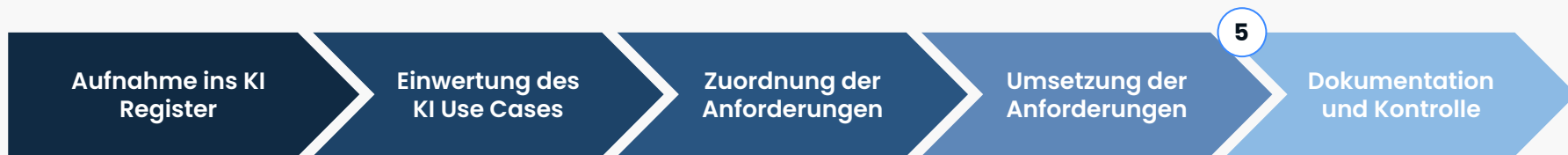
Sources (1)

Control Effectiveness for Data Retention & Deletion

Effectiveness Effective

At all times during the term of Customer's subscription or the applicable Professional Services engagement, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service and Professional Services Data ¹. Customers can extract data for 90 days post-termination ². Microsoft will delete data after this 90-day retention period for Online Services ² or earlier upon customer request for Personal Data in connection with software and Professional Services Data ³, demonstrating that the ability to access, extract, and delete customer data is provided to the customer by the vendor.

Effiziente und automatisierte KI Governance



Auto-Alerts:
Stets aktuelle
Ergebnisse



Effiziente Audit &
Zertifizierungsmöglichkeit

Custom Experiment

Version: Latest Save Save As New Version Export PDF Generate Evidence

Data Processing

The data processing steps are as follows: 1. The 'credit-g' dataset is loaded from OpenML. 1. 2. The target variable is converted from categorical ('good', 'bad') to a binary format (1 for good credit, 0 for bad credit). 2. 3. Categorical variables are handled using one-hot encoding, dropping the first category to avoid multicollinearity. 3. 4. Column names are sanitized to ensure compatibility with XGBoost by replacing non-alphanumeric characters with underscores. 4. 5. Features are scaled using `StandardScaler`. 5. 6. The processed data is split into training and testing sets. 6.

Data Split

The data was split into training and testing sets using an 80/20 ratio, meaning 80% of the data was used for training and 20% for testing. A `random_state` of 42 was employed to ensure reproducibility of the split.

Model

Comment: `Import: XGBoost as xgb` 1 and the model instantiation `model =`

cross-validation scores are calculated on the training data 1 using `cross_val_score` from gging of the scores, occurs within lines 156-161 3]

Markdown WYSIWYG

Change History

UPDATE	Control	Anna Spitznagel	Oct 5 2025 - 3:23PM
UPDATE	Control	Anna Spitznagel	Oct 5 2025 - 3:23PM
Linked	Comment	Nikolaus Pinger	Aug 26 2025 - 1:29PM

KI-Agenten mit Human-in-the-Loop für Compliance-Aufgaben



Unsere Kunden sparen Zeit, erhöhen Qualität und skalieren KI

Bis zu

80%

Reduktion
manueller
Aufwände

**“Automatisiert und pragmatisch - ohne
Bedarf an manueller Interpretation”**



Dr. Sina Wulfmeyer

Chief Data Officer **UNIQUE**

**“Technologiegetrieben und
effizient”**



Silke Schneider-Wild

Vorständin **Sparda-Bank**

**“Innovative Software für
effiziente Audits”**



Ali Behbahani

Global Product Line Manager
Cybersecurity and AI **TÜV SÜD**

Jetzt KI Governance als Wettbewerbsvorteil nutzen



Kundenerwartungen

Vertrauen stärken und Akzeptanz erhöhen



AI at Scale

Time-to-Market und ROI beschleunigen



Compliance

Effiziente Umsetzung des EU AI Act

Effiziente KI-Governance bei hoch regulierten Finanzdienstleister

Großer deutscher Finanzdienstleister

> 5000 Mitarbeitende

> 1,5 Mrd. Umsatz

Hoch Reguliert

Fokus: EU AI Act

Herausforderungen

- ⚠️ Verschiedenste KI-Projekte
- ⚠️ Manuelle Compliance-Prozesse
- ⚠️ Komplexe, proprietäre Systeme

Erfolgreiche Einführung einer Enterprise KI-Governance

Ziel: EU AI Act Readiness und vertrauenswürdige KI als Wettbewerbsvorteil

Erfolge mit trail:

- ✓ Zentrale KI Steuerung
- ✓ Effiziente Governance Umsetzung
- ✓ Unternehmensweite KI Skalierung
- ✓ Steigerung Kundenvertrauen

Kontakt

Jetzt mehr erfahren!

trail



Anna Spitznagel

anna@trail-ml.com

+49 177 7558380



www.trail-ml.com

Vielen Dank für die Aufmerksamkeit!

trail

www.trail-ml.com