Agentic AI Governance Accelerator

microfin
enables
digital trust.

Wissensaufbau, Standortbestimmung und Verprobung für beschleunigte Agentic AI Use Cases

KI-Agenten übernehmen Aufgaben, greifen auf Daten und Systeme zu und führen eigenständig Aktionen aus. Finanzunternehmen müssen im regulatorischen Kontext festlegen, welche Aufgaben und Entscheidungen sie delegieren, wo menschliche Freigaben erforderlich sind und wie sich das Handeln der Agenten nachvollziehen und kontrollieren lässt. Das betrifft gleichermaßen Architekten, Entwickler und Funktionen der IT-Steuerung.

Der microfin Agentic AI Governance Accelerator verbindet Wissensvermittlung, ein begleitetes Self-Assessment und die praktische Verprobung. Auf Basis unseres praxisnahen Agentic AI Governance Frameworks konkretisieren wir organisatorische, regulatorische und technische Anforderungen für euren Anwendungsfall. Eure bestehende IT- bzw. KI-Governance bildet dabei den Ausgangspunkt.

1



Enablement: Wissen auf- & ausbauen

Wir zeigen, wie bestehende KI-Governance gezielt um die Steuerung und Kontrolle von KI-Agenten erweitert werden kann – **ohne ihre Innovationskraft und Handlungsspielräume auszubremsen**.

Ihr lernt organisatorische, regulatorische und technische Grundlagen kennen: von Automatisierung, Berechtigungen und Delegation über Verantwortlichkeiten und die Einordnung nach **AI Act und DORA** bis hin zu Architektur, Entwicklung und wirksamen technischen Kontrollen. Eigene Use Cases machen die Inhalte greifbar und unterstützen den Transfer in die Praxis.

Dabei könnt ihr die Lerninhalte gezielt um eure **individuellen Interessen und Anforderungen** erweitern – zum Beispiel mit Schwerpunkten auf Agentic Coding, Regulatorik oder New Work.

2



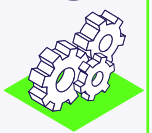
Self-Assessment: Status bestimmen

Aufbauend auf dem vermittelten Spezialwissen zeigt ein kompaktes, begleitetes Self-Assessment, welche Vorgaben, Rollen und Prozesse sowie technischen Fähigkeiten eure **bestehende KI-Governance** bereits abbildet – immer mit dem Blick, ob sie auch für agentische KI trägt.

Grundlage ist das **Agentic AI Governance Framework** von microfin, das praxisbewährte Lösungen aus dem Umfeld von Finanzunternehmen berücksichtigt.

Gemeinsam machen wir möglichen Lücken sichtbar, priorisieren die **wichtigsten Handlungsfelder** und legen fest, worauf wir in der anschließenden praktischen Verprobung den Fokus richten, damit euer Use Case den organisatorischen, regulatorischen und technischen Vorgaben Stand hält.

3



Hackathon: Use Case verproben

Anschließend verbinden wir das neue Wissen mit den Erkenntnissen aus dem Self-Assessment und euren bestehenden KI-Governance-Artefakten. In einem oder mehreren **klar begrenzten Zeitfenstern** entwickelt ihr einen konkreten Anwendungsfall für agentische KI weiter – mit dem Ziel, die relevanten Anforderungen an eine **belastbare Agentic-AI-Governance** für euer Unternehmen möglichst umfassend zu berücksichtigen.

Idealerweise arbeiten dafür **Fachbereich, Architektur, Entwicklung sowie Funktionsträger der IT- bzw. KI-Governance** zusammen. Gemeinsam schärft ihr bestehende Vorgaben oder entwickelt ergänzende Regeln und Kontrollen. Ausgewählte technische Kontrollen setzt ihr prototypisch um und prüft, wie geeignet und wirksam sie sind.

Bestimmt Inhalte & Umfang

Im Vorgespräch stimmen wir gemeinsam ab, welche Grundlagen und Vertiefungen relevant sind, wie tief das Assessment gehen soll und welche organisatorisch-technischen Kontrollen wir im Hackathon praktisch bearbeiten.

Euer Ergebnis:

Ein erprobter Prototyp für Agentic AI Governance

Für euren ausgewählten Use Case führen wir die Arbeitsergebnisse in einem **Minimum Viable Product** für Agentic AI Governance zusammen: einem schlanken, anwendungsbezogenen Prototyp, der anschließend erweitert werden kann.

Was der Prototyp umfasst



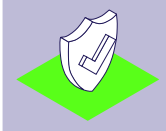
Verantwortlichkeiten und Entscheidungswege

Zuordnung der Aufgaben zwischen Fachbereich, IT und Kontrollfunktionen sowie Festlegung von Freigabe-, Eingriffs- und Eskalationswegen.



Regeln für Autonomie und Delegation

Festlegung erlaubter Aktionen, erforderlicher Berechtigungen und der Grenzen, innerhalb derer der KI-Agent selbstständig handeln darf.



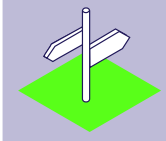
Ausgewählte, praktisch erprobte Kontrollen

Prototypische Umsetzung, Überprüfung von Maßnahmen, begrenzte Zugriffsrechte, Audit-Logs, Wiederholungsgrenzen oder menschliche Freigaben.



Nachvollziehbare Dokumentation

Verknüpfung relevanter organisatorischer, regulatorischer und technischer Anforderungen mit den bearbeiteten Maßnahmen und den Ergebnissen der Verprobung.



Priorisierte nächste Schritte

Priorisierte Empfehlungen für die weitere Umsetzung auf Basis der Verprobung. Benennung noch erforderlicher Prüfungen der Wirksamkeit einzelner Kontrollen sowie notwendiger Nachbesserungen. Die Erkenntnisse unterstützen auch den Aufbau oder die Weiterentwicklung eurer Sollschutzvorgaben für KI-Agenten.

Fachliche Vertiefungen

Grundlagen zu KI-Agenten

Automation vs. KI-Assistenten vs. KI-Agenten präzise unterscheiden, Funktionsweise und Autonomiegrade verstehen sowie Einsatzmöglichkeiten und Grenzen anhand konkreter Beispiele einordnen.

AI Act, DORA und CRA

Agentische Anwendungsfälle mit den einschlägigen Anforderungen abgleichen: Wir zeigen, was eure IT-Governance bereits abdeckt und wo Verantwortlichkeiten, Freigabeprozesse, Kontrollen oder Nachweise ergänzt werden müssen.

Agentic Coding

Aufgaben sinnvoll zerlegen, Kontext bereitstellen, Agenten präzise beauftragen und bei Fehlversuchen nachsteuern. Praktische Tipps zu typischen Stolperfallen, zur Prüfung generierten Codes und zur Einbindung in eure Entwicklungsabläufe – auch in On-Premises-Umgebungen.

Vorbereitung, Verprobung und Transfer

Vorab stimmen wir euren Anwendungsfall für agentische KI, vorhandene Unterlagen, technische Umgebung und erforderliche Zugänge ab.
Bei einer geplanten Plattformauswahl beziehen wir die Governance-Anforderungen frühzeitig in die Betrachtung von Architektur, Hosting und Berechtigungen ein.

Die praktische Arbeit gliedert sich in den Aufbau des Governance-Prototyps und dessen anschließende Umsetzung und Verprobung. Ein abschließendes Debriefing bündelt Erkenntnisse und Handlungsempfehlungen. Weitere Agentic AI Use Cases zur Verprobung oder eine anschließende Umsetzungsbegleitung können gesondert vereinbart werden.

Besprecht euren Bedarf mit uns

Gemeinsam klären wir euren Bedarf und erstellen darauf aufbauend euer **individuelles Festpreisangebot.**



Dr. Paul Tscheuschner
p.tscheuschner@microfin.de



Stefan Wendt
s.wendt@microfin.de