VISCHER

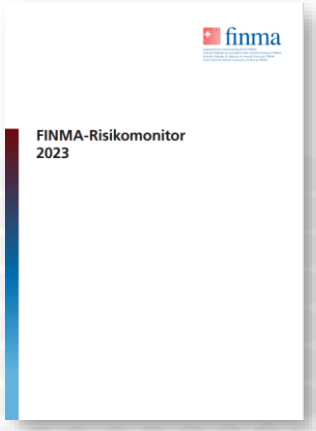
FINMA Aufsichtsmitteilung 08/2024.

Erkenntnisse und praktische Lösungen

David Rosenthal, VISCHER AG
18. Februar 2025

Bisherige Erwartungen der FINMA

1. Es müssen klare Rollen und Verantwortlichkeiten sowie Risikomanagementprozesse definiert und implementiert werden. Die Verantwortung für Entscheidungen kann nicht an KI oder Drittparteien delegiert werden. Alle Beteiligten müssen über genügend Know-how im Bereich KI verfügen.
2. Bei der Entwicklung, der Anpassung und in der Anwendung von KI ist sicherzustellen, dass die Ergebnisse hinreichend genau, robust und zuverlässig sind. Dabei sind sowohl die Daten als auch die Modelle und die Resultate kritisch zu hinterfragen.
3. Die Erklärbarkeit der Resultate einer Anwendung sowie die Transparenz über deren Einsatz sind je nach Empfänger, Relevanz und Prozessintegration sicherzustellen.
4. Nicht begründbare Ungleichbehandlung ist zu vermeiden.



Worum es der FINMA dabei geht:

https://vischerlnk.com/3MRHurk

Aufsichtsmitteilung 08/2024: Kernpunkte

- Nötig ist ein **risikobasierter Ansatz**, was aber heisst, dass die Institute die mit ihrer KI verbundenen Risiken kennen müssen
  - Primär Modell-, IT/Cyber- und Abhängigkeits-Risiken
  - Was ist überhaupt KI? Wo kommt sie zum Einsatz? Welche KI-Anwendungen sind aufgrund ihrer Risiken "wesentlich"?
- Es muss immer jemand intern insgesamt **verantwortlich** sein
  - Kann diese Person die Entscheide der KI begründen? Sind die treibenden Faktoren bekannt? Sind die Ergebnisse pausibel?
  - Bei Providern gilt was auch sonst beim Outsourcing gilt
- KI und Datenbasis vorab **testen** und danach **überwachen**
  - Passende Datenbasis oft wichtiger als konkretes Modell
  - Erwartungen und Methoden definieren, alles dokumentieren

https://vischerlnk.com/3EDw6yB

Erkenntnisse aus Gesprächen und Vor-Ort-Kontrollen

Schritt 1: Grundlagen und Überblick schaffen

- **Definieren**, was als KI gilt (z.B. Definition nach EU AI Act)
  - Aber: Systeme ohne KI können dieselben Risiken aufweisen
- Modell zur **Klassifizierung der KI-Risiken** festlegen
  - Inklusive "wesentliche" KI-Anwendungen
- **Weisung** erstellen
  - Prozesse, Massnahmen, AKV
  - Wahl- und Prüfkriterien, Dokumentation
  - Trennung der Rollen (Entwicklung, Prüfung)
- **Inventarisieren** von KI-Anwendungen
  - Eckwerte, Risikoklasse (inklusive Wesentlichkeit)
  - Interne Verantwortlichkeit (i.S.v. Accountability)

vischerlnk.com/gaira

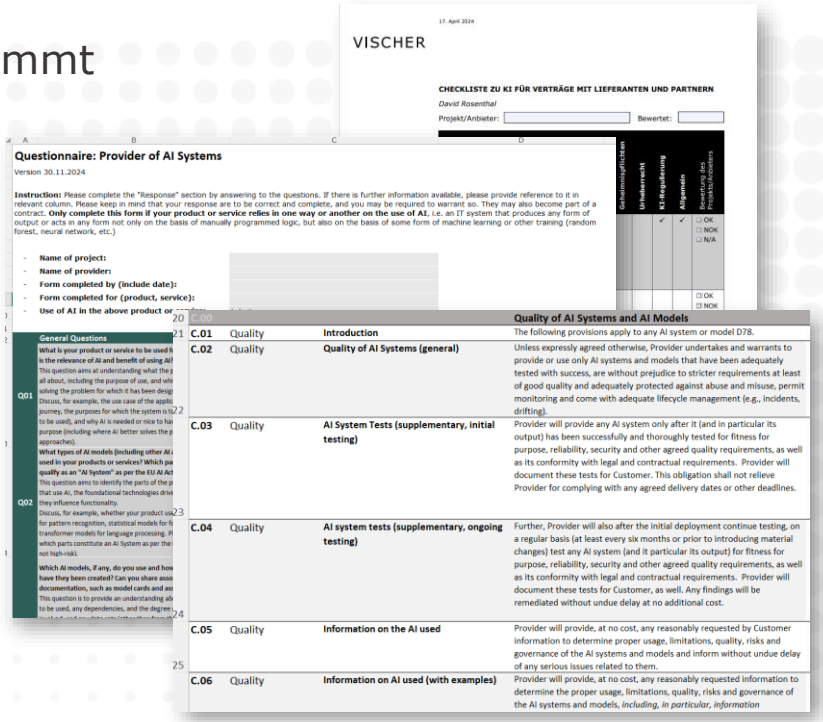
Schritt 2: Anwendungsspezifische Massnahmen

- Geregelte, dokumentierte **Auswahl** oder **Entwicklung** von KI
  - U.a. Anwendungszweck, Auswahl von Daten (Quellen, Qualität, Eignung, Integrität, Richtigkeit, Relevanz, Bias, Einheitlichkeit), und Modell (Robustheit, Korrektheit, Erklärbarkeit, Bias), KPIs
- **Beurteilung** von Qualität, Compliance und Risiken
  - Testen von Datenqualität, Modellverhalten, Funktionsfähigkeit
  - Compliance- und Risikobeurteilung, inkl. Massnahmen
- **Entscheid** über ihren Einsatz und etwaige Beschränkungen
- **Schulung** von Anwendern, Spezialisten und Management
- **Überwachung** des Einsatzes der KI-Anwendungen
  - Einhaltung der Vorgaben, Drifting, Manual Overrides, Incidents

Schritt 3: Lieferanten verpflichten

vischerlnk.com/ki-provider-check

- **Verstehen**, wo KI wie zum Einsatz kommt
- **Verträge** ergänzen
  - Einsatz von KI
  - Qualität von KI
  - KI-Compliance (z.B. EU AI Act)
- **Cloud**-Compliance- und Risiken wie bisher prüfen
- **Werkzeuge**
  - Fragebogen für Lieferanten
  - Standardklauseln/Klausel-Baukasten
  - CCRA-FI (https://vischerlnk.com/42ZgX4P)



VISCHER

17. April 2024

CHECKLISTE ZU KI FÜR VERTRÄGE MIT LIEFERANTEN UND PARTNERN

David Rosenthal

Projekt/Anbieter: Bewertet:

Questionnaire: Provider of AI Systems

Version 30.11.2024

Instruction: Please complete the "Response" section by answering to the questions. If there is further information available, please provide reference to it in relevant column. Please keep in mind that your response are to be correct and complete, and you may be required to warrant so. They may also become part of a contract. **Only complete this form if your product or service relies in one way or another on the use of AI**, i.e. an IT system that produces any form of output or acts in any form not only on the basis of manually programmed logic, but also on the basis of some form of machine learning or other training (random forest, neural network, etc.)

- **Name of project:**
- **Name of provider:**
- **Form completed by (include date):**
- **Form completed for (product, service):**
- **Use of AI in the above product or**

Gehirnmöglichkeiten | Urheberrecht | KI-Regulierung | Allgemein | Bemerkungen des Projektverantwortlichen

☐ OK ☐ NOK ☐ N/A

☐ OK ☐ NOK

General Questions

What is your product or service to be used f
is the relevance of AI and benefit of using AI
This question aims at understanding what the p
all about, including the purpose of use, and wh
Q01 solving the problem for which it has been desig
Discuss, for example, the use case of the applic
journey, the purposes for which the system is to
to be used), and why AI is needed or nice to ha
purpose (including where AI better solves the p
approaches).
What types of AI models (including other AI
used in your products or services? Which pa
qualify as an "AI System" as per the EU AI Act
This question aims to identify the parts of the p
that use AI, the foundational technologies drivi
Q02 they influence functionality.
Discuss, for example, whether your product use
for pattern recognition, statistical models for fi
transformer models for language processing. H
which parts constitute an AI System as per the
not high-risk).
Which AI models, if any, do you use and how
have they been created? Can you share asso
documentation, such as model cards and as
This question is to provide an understanding ab
to be used, any dependencies, and the degree

			Quality of AI Systems and AI Models	
C.01	Quality	**Introduction**	The following provisions apply to any AI system or model D78.
C.02	Quality	**Quality of AI Systems (general)**	Unless expressly agreed otherwise, Provider undertakes and warrants to provide or use only AI systems and models that have been adequately tested with success, are without prejudice to stricter requirements at least of good quality and adequately protected against abuse and misuse, permit monitoring and come with adequate lifecycle management (e.g., incidents, drifting).
C.03	Quality	**AI System Tests (supplementary, initial testing)**	Provider will provide any AI system only after it (and in particular its output) has been successfully and thoroughly tested for fitness for purpose, reliability, security and other agreed quality requirements, as well as its conformity with legal and contractual requirements. Provider will document these tests for Customer. This obligation shall not relieve Provider for complying with any agreed delivery dates or other deadlines.
C.04	Quality	**AI system tests (supplementary, ongoing testing)**	Further, Provider will also after the initial deployment continue testing, on a regular basis (at least every six months or prior to introducing material changes) test any AI system (and it particular its output) for fitness for purpose, reliability, security and other agreed quality requirements, as well as its conformity with legal and contractual requirements. Provider will document these tests for Customer, as well. Any findings will be remediated without undue delay at no additional cost.
C.05	Quality	**Information on the AI used**	Provider will provide, at no cost, any reasonably requested by Customer information to determine proper usage, limitations, quality, risks and governance of the AI systems and models and inform without undue delay of any serious issues related to them.
C.06	Quality	**Information on AI used (with examples)**	Provider will provide, at no cost, any reasonably requested information to determine the proper usage, limitations, quality, risks and governance of the AI systems and models, *including, in particular, information*

VISCHER

Danke für Ihre Aufmerksamkeit!

Fragen: david.rosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

www.vischer.com

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

Mehr zum Thema:
vischer.com/ki