



Responsible AI at Microsoft

November 2024

Martin Haas, Leiter Mittelstand und KMU, Microsoft Schweiz

The Promise of AI



We have made huge investments in AI because we're **optimistic about what it can do to help people, industry and society**, and because we're committed to **bringing technology and people together to realize the promises of AI responsibly**.



With help from next-generation AI, Indian villagers gain easier access to government services



Assisted by AI, a workforce of bees tracks pollution and boosts biodiversity



Generative AI tools are helping people with listening difficulties in Japan

We cannot realize the value of AI without **trust**

73%

of people feel concerned about
the potential risks of AI

75%

more willing to trust AI with
assurance mechanisms for
ethical and responsible use

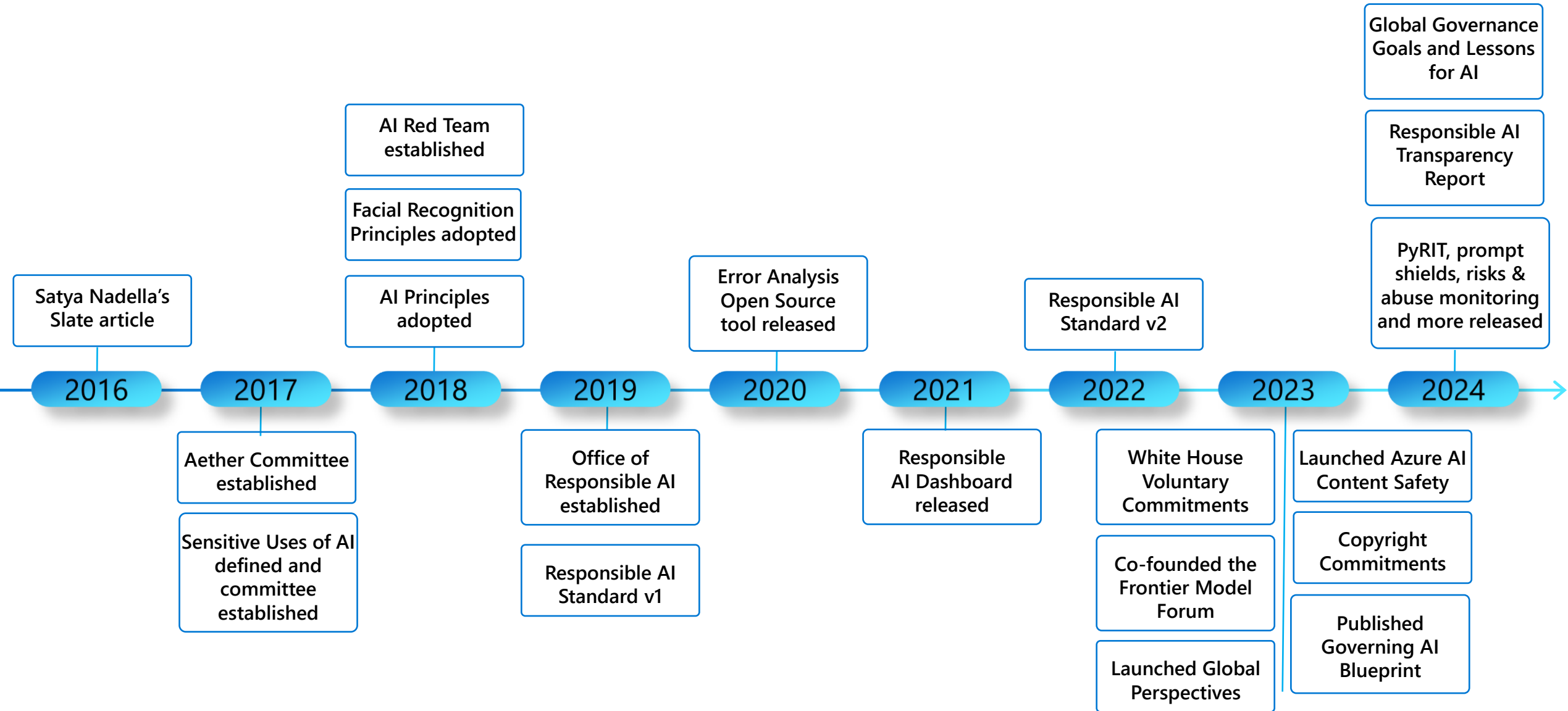
Source: [Trust in Artificial Intelligence: A Global Study.](#)

Microsoft's commitment is to build AI systems that are safe, secure, and trustworthy **by design**



Microsoft's Responsible AI Governance Framework

Our responsible AI journey



Microsoft's AI Principles



Fairness



Reliability
& Safety



Privacy &
Security



Inclusiveness

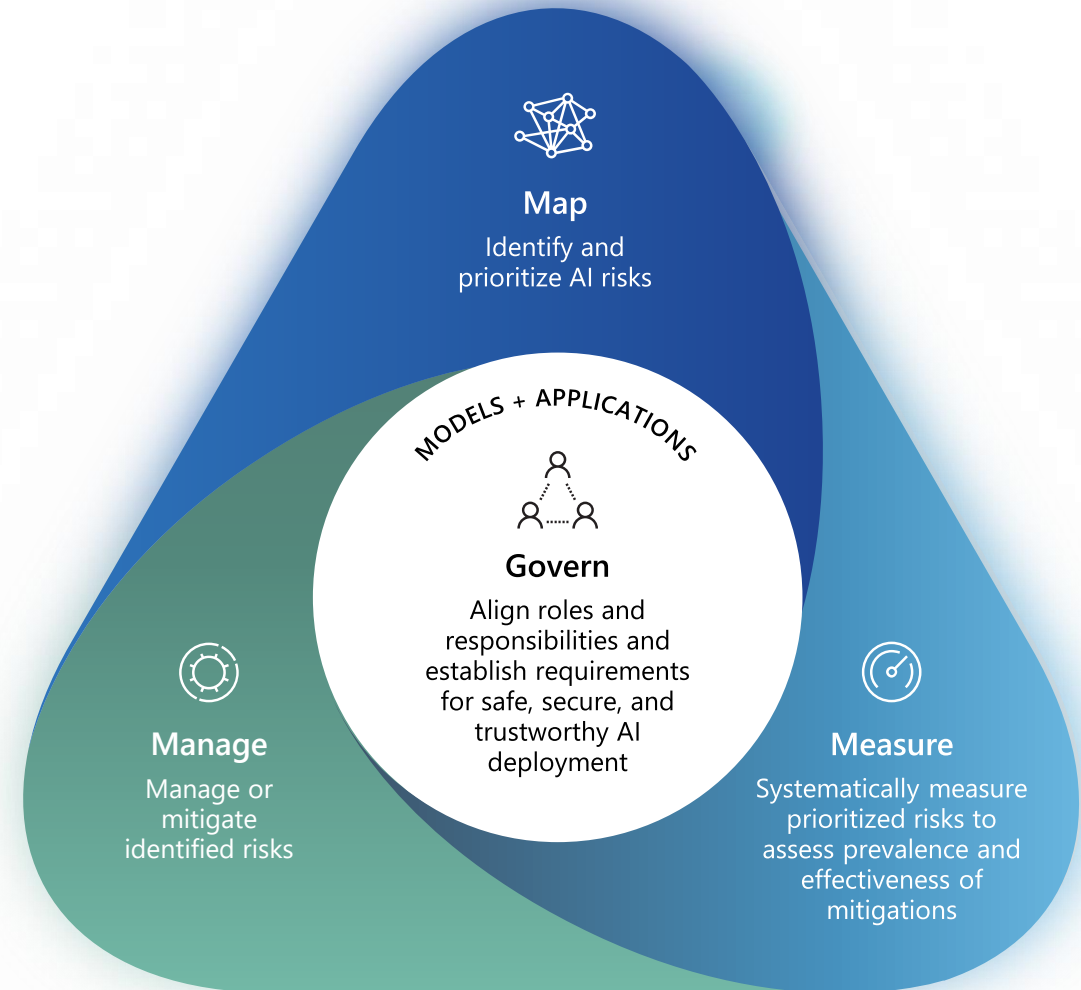


Transparency



Accountability

How we build generative AI systems responsibly



NIST AI Risk Management Framework

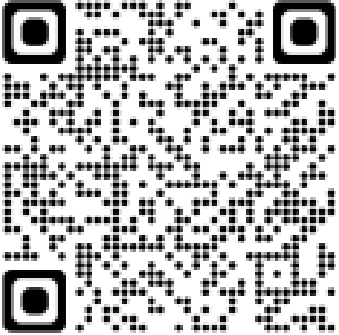
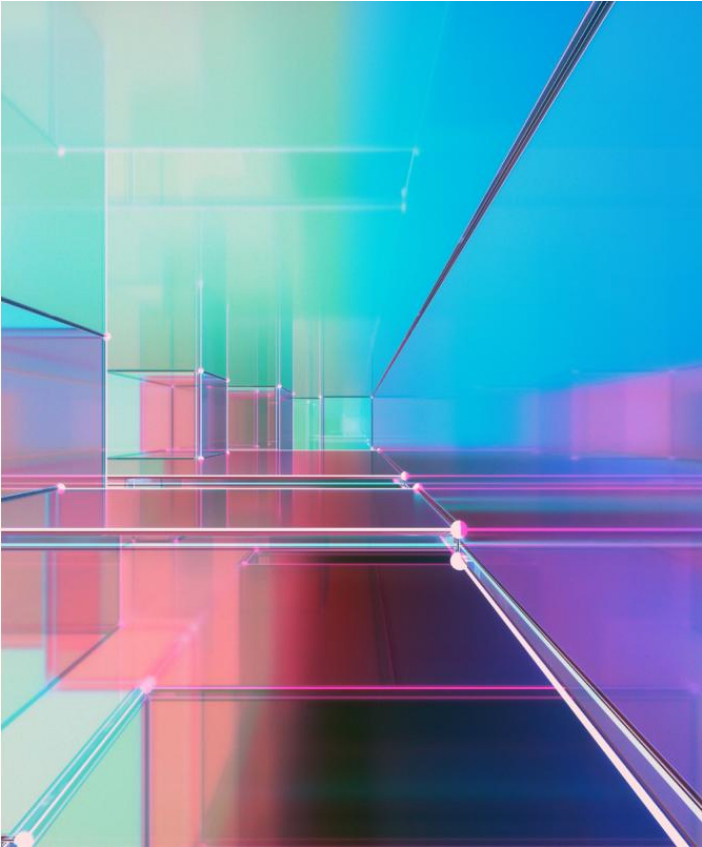
Responsible AI Transparency Report



Responsible AI Transparency Report

How we build, support
our customers, and grow

May 2024



Generative AI introduces new risks



Ungrounded outputs & errors



Jailbreaks & prompt injection attacks



Harmful content & code

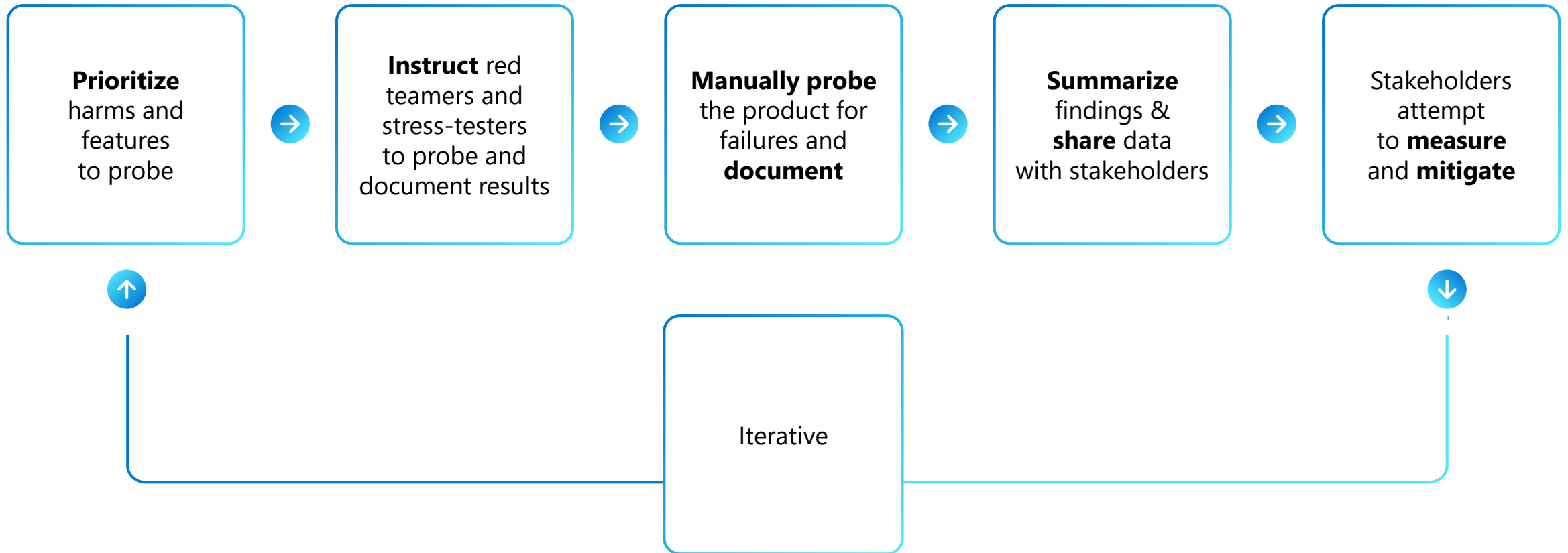


Infringement claims



Manipulation & human-like behavior

Red teaming with an iterative approach

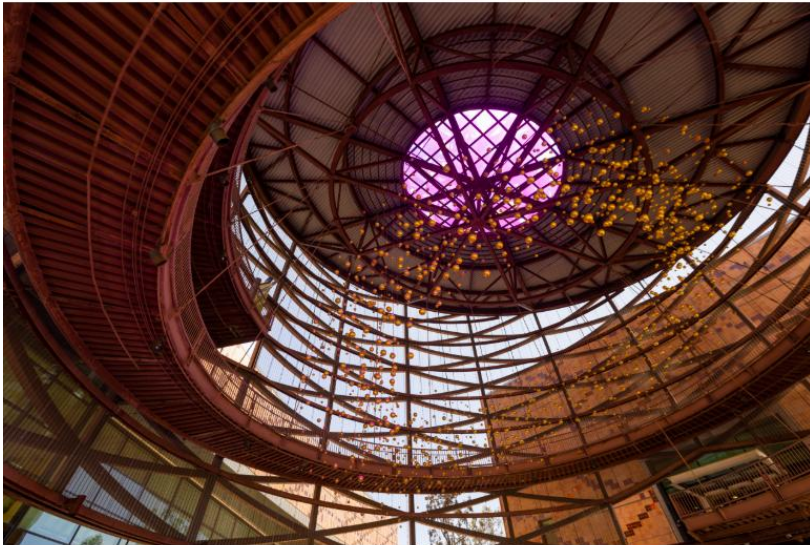


<https://aka.ms/CustomerRedTeamingGuide>

Microsoft's Customer Copyright Commitment

Microsoft announces new Copilot Copyright Commitment for customers

Sep 7, 2023 | Brad Smith, Vice Chair and President, Hossein Nowbar, CVP and Chief Legal Officer

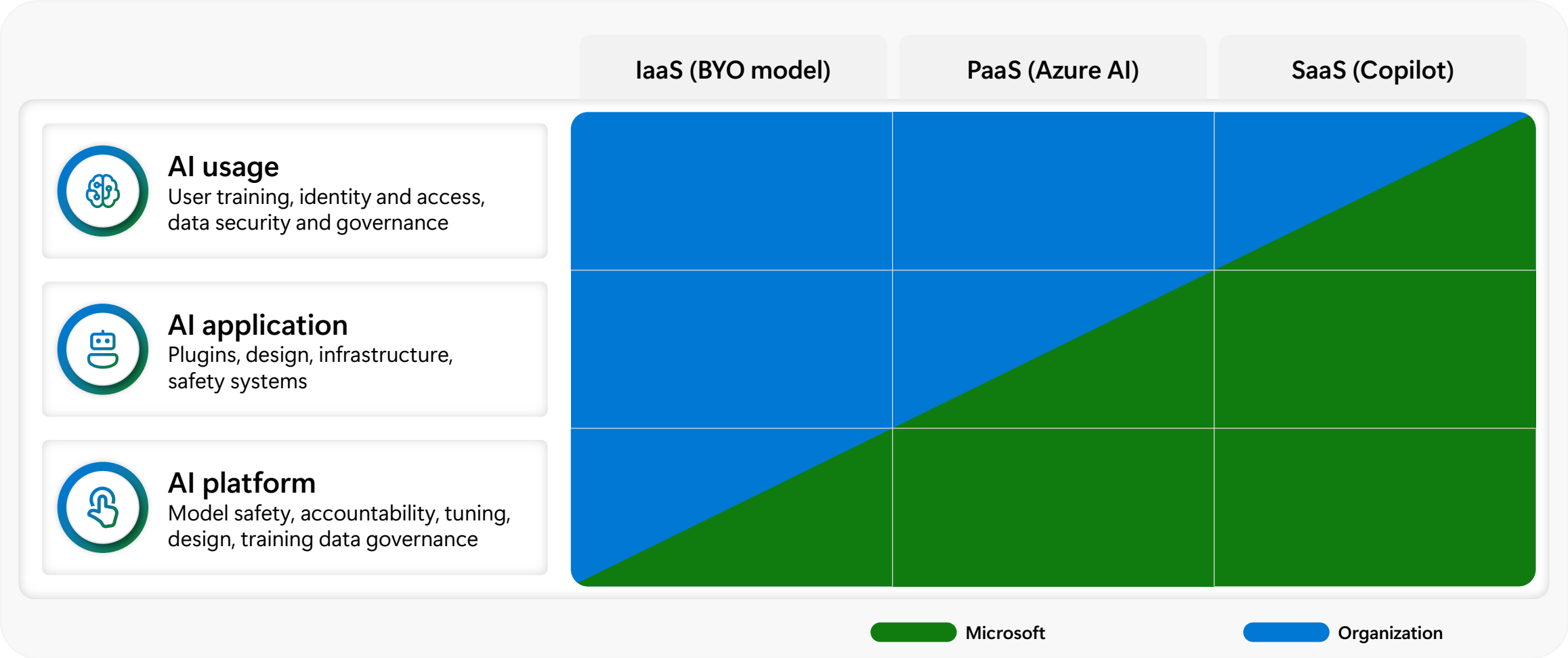


01.05.2024 Update: On November 15, 2023, Microsoft [announced](#) the expansion of the Copilot Copyright Commitment, now called the Customer Copyright Commitment, to include commercial customers using the Azure OpenAI Service. By extending the Commitment to cover the outputs from the Azure OpenAI Service, Microsoft is broadening our commitment to defend these customers and pay for any adverse judgments if they are sued for copyright infringement for the use of the Azure OpenAI Service outputs. This expansion of our copyright commitment is intended to further address customer concerns relating to potential IP infringement liability that could result from the use of the output of Microsoft's Copilots and Azure OpenAI Service. Our customers must have implemented the required [guardrails and mitigations](#) we have made available to be eligible for the benefits provided by the Customer Copyright Commitment. For our Azure OpenAI Service, we offer documentation and tooling that support the responsible use of AI and reduce risks of infringing copyrighted content.

You'll find more details below. Let me start with why we are offering this program:

- 1. We believe in standing behind our customers when they use our products.** We are charging our commercial customers for our Copilots, and if their use creates legal issues, we should make this our problem rather than our customers' problem. This philosophy is not new: For roughly two decades we've defended our customers against patent claims relating to our products, and we've steadily expanded this coverage over time. Expanding our defense obligations to cover copyright claims directed at our Copilots is another step along these lines.
- 2. We are sensitive to the concerns of authors, and we believe that Microsoft rather than our customers should assume the responsibility to address them.** Even where existing copyright law is clear, generative AI is raising new public policy issues and shining a light on multiple public goals. We believe the world needs AI to advance the spread of knowledge and help solve major societal challenges. Yet it is critical for authors to retain control of their rights under copyright law and earn a healthy return on their creations. And we should ensure that the content needed to train and ground AI models is not locked up in the hands of one or a few companies in ways that would stifle competition and innovation. We are committed to the hard and sustained efforts that will be needed to take creative and constructive steps to advance all these goals.
- 3. We have built important guardrails into our Copilots to help respect authors' copyrights.** We have incorporated filters and other technologies that are designed to reduce the likelihood that Copilots return infringing content. These build on and complement our work to protect digital safety, security, and privacy, based on a broad range of guardrails such as classifiers, metaprompts, content filtering, and operational monitoring and abuse detection, including that which potentially infringes third-party content. Our new Copilot Copyright Commitment requires that customers use these technologies, creating incentives for everyone to better respect copyright concerns.

Security for AI shared responsibility model



Lancierung eines
smarten Rucksackes



W AutoSave Off Document4 - Word General* Search

File Home Insert Draw Design Layout References Mailings Review View Help Acrobat

Clipboard Paste Font Paragraph Styles Editing Adobe Acrobat Dictate Sensitivity Add-ins Editor Copilot

 **Draft with Copilot** ✕

Schreibe ein Marketingkonzept für die Lancierung eines neuen smarten Rucksackes. Der Rucksack beinhaltet eine eingebaute Ladestationen für Handys, GPS-Tracker zur Verfolgung des Rucksackes und Bluetooth-Chips für den Kontakt mit einem Smartphone.

246/2000

Generate 📎 Reference a file

Marketingkonzept für die Lancierung des neuen smarten Rucksacks

Ein innovativer Ansatz für moderne Mobilität

1. Einführung

Mit der rasanten Entwicklung der Technologie und dem zunehmenden Bedürfnis nach Konnektivität wird der neue smarte Rucksack als must-have Accessoire für den modernen Lebensstil positioniert. Der Rucksack integriert fortschrittliche Funktionen wie eine Ladestation für Handys, einen GPS-Tracker zur Verfolgung und Bluetooth-Chips für die Verbindung mit einem Smartphone. Dieses Marketingkonzept zielt darauf ab, die Markteinführung des Produktes erfolgreich durchzuführen und es als unverzichtbares auf dem Markt zu etablieren.

2. Marktanalyse

2.1 Zielmarkt

Der Zielmarkt für den smarten Rucksack umfasst technologieaffine Konsumenten, die und privat viel unterwegs sind und dabei stets vernetzt bleiben möchten. Zu den Hauptzielgruppen gehören:

- Berufspendler
- Reisende und Abenteuerler
- Studenten und Schüler
- Technologie-Enthusiasten

2.2 Wettbewerbsanalyse

Der Markt für smarte Rucksäcke ist noch relativ neu, jedoch gibt es bereits einige Wettbewerber wie die Marken „Xiaomi“ und „Targus“, die ähnliche Produkte anbieten. Unser smarte Rucksack hebt sich durch zusätzliche Funktionen und ein innovatives Design von den bestehenden Produkten ab. Ein Vergleich der verschiedenen Produkte und ihrer Preise zeigt, dass der Markt für hochwertige, multifunktionale Rucksäcke gibt, der durch gezielte Marketingmaßnahmen erfolgreich erschlossen werden kann.

3. Produktmerkmale

3.1 Eingebaute Ladestation

Der smarte Rucksack verfügt über eine leistungsstarke, eingebaute Ladestation, die es ermöglicht, Handys und andere mobile Geräte unterwegs aufzuladen. Dies stellt sicher, dass die Nutzer jederzeit erreichbar bleiben und nicht auf externe Ladegeräte angewiesen sind.

3.2 GPS-Tracker

Ein GPS-Tracker ist im Rucksack integriert, um den Standort in Echtzeit verfolgen zu können. Dies ist besonders nützlich, um den Rucksack im Falle eines Verlustes oder Diebstahls schnell wiederzufinden.

3.3 Bluetooth-Chips

Die eingebauten Bluetooth-Chips ermöglichen eine nahtlose Verbindung mit dem Smartphone des Nutzers. Dies erleichtert die Steuerung der Rucksackfunktionen und sorgt für eine intuitive Bedienung.

3.4 Hochwertiges Design

Der Rucksack ist aus strapazierfähigen, wasserabweisenden Materialien gefertigt und in einer Vielzahl von Farben und Stilen erhältlich, um den individuellen Geschmack der Nutzer zu treffen.

4. Marketingstrategie

4.1 Positionierung

Der smarte Rucksack wird als unverzichtbarer Begleiter für den modernen, mobilen Lebensstil positioniert. Die Betonung liegt auf der Kombination von Funktionalität, Technologie und Stil.

4.2 Preisstrategie

Der Rucksack wird im Premiumsegment positioniert und zu einem Preis von etwa 150-200 EUR angeboten. Durch die hohe Qualität und die innovativen Funktionen wird dieser Preis gerechtfertigt.

4.3 Vertriebskanäle

Der Vertrieb erfolgt sowohl online (über die eigene Webseite und etablierte E-Commerce-Plattformen wie Amazon) als auch offline (in ausgewählten Elektronik- und Outdoor-Geschäften). Kooperationen mit Mobilfunkanbietern und Reiseagenturen werden ebenfalls angestrebt.

4.4 Kommunikationsstrategie

- Online-Marketing: Eine umfassende Online-Marketingkampagne wird über soziale Medien, Google Ads und Influencer-Marketing durchgeführt. Ziel ist es, eine hohe Reichweite und Aufmerksamkeit für das Produkt zu erzeugen.
- PR und Medienarbeit: Pressemitteilungen und Artikel in Technologie- und Lifestyle-Magazinen sollen die Bekanntheit des Produkts erhöhen. Zudem werden Produkttests und -bewertungen in Blogs und auf YouTube angestrebt.
- Events und Messen: Teilnahme an Technologie- und Outdoor-Messen, um das Produkt direkt dem Zielpublikum vorzustellen und Feedback zu sammeln.
- Kooperationen: Zusammenarbeit mit bekannten Technologie- und Outdoor-Marken sowie Influencern, um die Glaubwürdigkeit und Reichweite zu erhöhen.

5. Umsetzung und Zeitplan

Der Produktlaunch ist für das vierte Quartal des Jahres geplant. Ein detaillierter Zeitplan wird erstellt, um sicherzustellen, dass alle Marketingmaßnahmen rechtzeitig und koordiniert durchgeführt werden. Die wichtigsten Meilensteine umfassen:

- Q1-Q2: Produktentwicklung und Tests
- Q3: Produktion und Aufbau der Vertriebskanäle
- Q4: Markteinführung und Beginn der Marketingkampagne

6. Erfolgskontrolle

Die Erfolgskontrolle erfolgt durch die regelmäßige Analyse der Verkaufszahlen, der Reichweite und Interaktion in den sozialen Medien sowie des Feedbacks der Kunden. Anpassungen der Marketingstrategie werden basierend auf den Ergebnissen vorgenommen, um die Effizienz der Maßnahmen kontinuierlich zu verbessern.

7. Fazit

Der neue smarte Rucksack bietet eine innovative Lösung für die Bedürfnisse des modernen, mobilen Lebensstils. Durch eine gezielte Marketingstrategie und die Betonung der einzigartigen Produktmerkmale wird der Rucksack erfolgreich auf dem Markt eingeführt und sich als unverzichtbares Accessoire etablieren. Die Kombination aus Funktionalität, Technologie und Stil spricht eine breite Zielgruppe an und bietet ein enormes Wachstumspotenzial.

Clipboard Slides Font Paragraph Drawing Editing Adobe Acrobat Dictate Sensitivity Add-ins Designer Copilot



Click to add title

Click to add subtitle

Datensicherheit und Datenschutz

Secure and govern AI with Microsoft



Prepare

- Zero Trust strategy – **Microsoft Security**
- Data labeling, classification, metadata management, and data lineage – **Microsoft Purview**
- Identity and access governance – **Microsoft Entra**



Discover

- AI app usage, prompt, response, and grounding data risk analytics – **Microsoft Purview**
- Security posture management for AI assets (apps, models, orchestrators, SDKs) – **Microsoft Defender**



Protect

- Prompt & response data security – **Microsoft Purview**
- Endpoint and access controls on AI app usage – **Microsoft Entra & Intune**
- SaaS app security – **Microsoft Defender**
- Threat protection for AI workloads – **Microsoft Defender**
- AI safety system – **Azure AI Content Safety Prompt Shield**



Govern

- Compliance assessments against AI regulations and standards – **Microsoft Purview**
- Prompt & response lifecycle management, eDiscovery, audits, communication compliance – **Microsoft Purview**
- Mitigation for harmful content, hallucination, and protected materials – **Azure AI Content Safety**

Microsoft's privacy commitments apply to AI



We will keep your organization's data private.



Your organization's data is not shared.



You are in control of your organization's data.



Your organization's data security and privacy are protected by design.



Your access control and enterprise policies are maintained.



Your organization's data is not used to train foundation models.



Our products and solutions comply with global data protection regulations.

Verträge

Volume
Licensing

Microsoft Products and Services Data Protection Addendum

Last updated January 2, 2024

Published in English on January 2, 2024. Translations will be published by Microsoft when available.
These commitments are binding on Microsoft as of January 2, 2024.



GDPR & Generative AI

A Guide for the Public Sector

April 2024



Thank you



Martin Haas

Leiter Mittelstand und KMU,
Mitglied der Geschäftsleitung Mi...



Connect