

Leading AI Transformation

Strategy, Governance, and
Security Considerations

Foreword by

David Weston

Corporate Vice President, AI Security, Microsoft

Yuri Diogenes

FREE SAMPLE CHAPTER |



Leading AI Transformation: Strategy, Governance, and Security Considerations

by Yuri Diogenes

Leading AI Transformation: Strategy, Governance, and Security Considerations

Published with the authorization of Microsoft Corporation by: Pearson Education, Inc.

Copyright © 2027 by Pearson Education, Inc.

Hoboken, New Jersey

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/global-permission-granting.html.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

ISBN-13: 978-0-13-594135-5

ISBN-10: 0-13-594135-0

Library of Congress Control Number: 2026948738

\$PrintCode

Trademarks

Microsoft and the trademarks listed at <http://www.microsoft.com> on the "Trademarks" webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

Credits

The visual elements in this publication were created using ChatGPT by OpenAI, with prompts and creative direction provided by the author.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author, the publisher, and Microsoft Corporation shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the programs accompanying it.

EDITOR-IN-CHIEF

Julie Phifer

EXECUTIVE EDITOR

Loretta Yates

ACQUISITIONS EDITOR

Shourav Bose

DEVELOPMENT EDITOR

Rick Kughen

MANAGING EDITOR

Sandra Schroeder

SENIOR PROJECT EDITOR

Tracey Croom

COPY EDITOR

Rick Kughen

INDEXER

Timothy Wright

PROOFREADER

Donna E. Mulder

TECHNICAL EDITOR

Dominik Hoeftling

COVER ILLUSTRATION

putilov_denis/stock.adobe.com

COVER DESIGNER

Twist Creative, Seattle

COMPOSITOR

codeMantra

GRAPHICS

ChatGPT

Dedication

I dedicate this book to my mother, Maria Salete Mascarenhas Diogenes, who passed away in September 2025. Thank you for your unconditional love, your guidance, and the countless lessons you taught me throughout my life. I miss you every day, Mom.

Contents at a Glance

	Acknowledgments	ix
	About the author	xi
	Introduction	xiii
	Foreword	xvii
CHAPTER 1	Identify the business value of generative AI solutions	1
CHAPTER 2	Identify benefits, capabilities, and opportunities for Microsoft's AI apps and services	23
CHAPTER 3	Identify an implementation and adoption strategy for Microsoft's AI apps and services	49
CHAPTER 4	Design identity, data, and cloud security for AI solutions	71
APPENDIX A	Preparing for AI Transformation Leader Exam (AB-731)	97
	Index	105

Contents

<i>Acknowledgments</i>	<i>ix</i>
<i>About the author</i>	<i>xi</i>
<i>Introduction</i>	<i>xiii</i>
<i>Foreword</i>	<i>xvii</i>

Chapter 1 Identify the business value of generative AI solutions 1

Identify the foundational concepts of generative AI	1
Describe the differences between generative AI and other types of AI ...	2
Select a generative AI solution to meet business needs	4
Describe the differences between AI models, including fine-tuned and pretrained models	6
Explain the cost drivers in Gen AI usage, including tokens and return on investment (ROI) considerations	7
Identify the challenges of using generative AI solutions, including fabrications, reliability, and bias	9
Identify when generative AI solutions can provide business value, including scalability and automation	11
Identify the benefits and capabilities of generative AI solutions	13
Describe the impact of prompt engineering	13
Identify business requirements for grounding solutions	15
Understand how retrieval-augmented generation (RAG) is used for AI solutions	16
Understand the impact of data on AI solutions, including data type, data quality, and representative datasets	17
Identify scenarios when machine learning adds value.	19
Next steps	20

Chapter 2 Identify benefits, capabilities, and opportunities for Microsoft's AI apps and services 23

Identify the benefits and capabilities of Microsoft 365 Copilot and Microsoft Copilot	23
Map business processes and use-cases to Copilot	24

Understand differences in capabilities between versions of Copilot	26
Understand the capabilities of Microsoft 365 Copilot Chat web and mobile experiences	27
Understand capabilities of the Copilot experience in various Microsoft 365 apps	28
Understand the capabilities of Microsoft Copilot Studio	30
Understand the capabilities of Microsoft Graph	32
Identify the benefits and capabilities of an integrated Microsoft AI solution, including risk mitigation and safety benefits	33
Map business processes and use-cases to Microsoft's AI apps and services	35
Identify when to use Researcher or Analyst in Copilot	36
Identify when to build, buy, or extend, including the Microsoft 365 Copilot extensibility framework	38
Identify the benefits and capabilities of Microsoft Foundry services	39
Map business processes and use-cases to Microsoft Foundry services . .	40
Identify capabilities of Microsoft Foundry services, including Azure Vision in Foundry services, Azure AI Search, and Microsoft Foundry . .	41
Match an AI model to a business need	43
Identify the benefits of Microsoft Foundry services for generative AI, including scalability and security	44
Next steps	46

Chapter 3 Identify an implementation and adoption strategy for Microsoft's AI apps and services **49**

Align an AI strategy with Microsoft's responsible AI policies	49
The importance of responsible AI	50
Establish governance principles for AI use	53
Establish an AI council to guide strategy, oversight, and cross- functional alignment	54
Plan for AI adoption across the organization	56
Establish an adoption team	56
Identify common barriers to adoption	58
Establish an AI Champions program	60

Understand Copilot license types, including pay-as-you-go, monthly, and included with a Microsoft 365 subscription	63
Understand Microsoft Foundry services subscription models, including pay-as-you-go and provisioned throughput unit (PTU) ...	66
Next steps	68
Chapter 4 Design identity, data, and cloud security for AI solutions	71
Designing considerations for Microsoft Entra as your identity security solution for AI	71
Everything starts with an identity.	72
Identity signals as a foundation for Zero Trust and AI security	74
AI-powered identity protection and risk detection	75
Behavior-based user and sign-in risk scoring	77
Adaptive access with conditional access	77
Designing considerations for Microsoft Purview as your data protection solution for AI	79
Data security posture management (DSPM) for AI	79
Data classification and sensitive data detection in AI	81
Information protection for AI apps and agents	82
Data governance for AI	85
Designing considerations for Microsoft Defender for Cloud as your cloud security solution for AI	87
Risk prioritization and contextual security recommendations	88
Threat protection for AI workloads	90
Next steps	94
Appendix A Preparing for AI Transformation Leader Exam (AB-731)	97
<i>Index</i>	105

This page intentionally left blank

Acknowledgments

I would like to thank Pearson/Microsoft Press for the almost two decades of partnership, and a special thanks to Shourav Bose and Loretta Yates. I would also like to thank my great friend and technical reviewer of this book, Dominik Hoefling, for the amazing work and constant feedback.

As you might have seen in the Foreword, the book started with a great contribution from David Weston. Thank you so much for your time, David.

Thank you to all my students, mentees, and everyone who attended my AI Security talks across the globe. Your feedback and insights helped me to shape this book!

—Yuri Diogenes

This page intentionally left blank

About the author

Yuri Diogenes has a PhD in cybersecurity leadership and a Master of Science in cybersecurity intelligence and forensics investigation. Yuri has been working at Microsoft since 2006, and currently, he is a principal PM manager at Microsoft CxE, where he manages the Defender for Cloud and Azure Network Security Teams. Yuri is also a Professor at the University of Texas at Dallas and EC-Council University. Yuri has published more than 30 books, mostly about information security and Microsoft technologies. Yuri also holds an MBA and many IT/Security industry certifications, such as CISSP, E|CND, E|CEH, E|CSA, E|CHFI, E|CTI, CompTIA Security+, CySA+, CASP, and MITRE ATT&CK Cyber Threat Intelligence. You can follow Yuri on X at @yuridiogenes and watch his Defender for Cloud in the Field show at aka.ms/MDCInTheField.

This page intentionally left blank

Introduction

AI is changing the way organizations think about work, leadership, security, and business transformation. But if you are like many leaders I talk to, you are probably not asking whether AI matters anymore. You are asking where to start, how to prioritize, how to avoid unnecessary risk, and how to turn all this innovation into measurable business value. That is the practical conversation this book is meant to have with you.

I wrote this book because AI adoption has moved beyond experimentation. Organizations are now expected to make real decisions about Microsoft 365 Copilot, Copilot Studio, Azure AI services, responsible AI, identity security, data protection, and cloud security. Those decisions are not only technical. They affect budgets, governance, productivity, trust, compliance, and culture. The goal of this book is to help you connect those pieces and build an AI strategy that is useful, secure, responsible, and aligned to the way your organization actually works.

Throughout the chapters, I will guide you through the concepts and decisions that matter most for AI transformation. We will start with the business value of generative AI, then look at Microsoft's AI apps and services, adoption strategy, responsible AI, and the security foundations required to protect identities, data, and cloud workloads. My intent is not to overwhelm you with theory, but to give you a clear way to think about AI in real business scenarios, including where it adds value, where it introduces risk, and where leadership must be intentional.

As you read this book, I encourage you to think about your own organization, your own users, and your own adoption journey. AI is not successful simply because it is deployed; it becomes successful when people trust it, use it effectively, and apply it to the right problems. My hope is that this book helps you move from AI curiosity to AI confidence, giving you the language, structure, and practical guidance needed to lead meaningful AI transformation with Microsoft technologies.

Who this book is for

This book is for decision-makers, architects, security leaders, and business stakeholders who are trying to make sense of AI beyond the hype. If you are responsible for shaping strategy, choosing the right Microsoft AI capabilities, securing data and identities, or helping your organization adopt AI in a practical way, this book was written with you in

mind. You do not need to be a data scientist to benefit from it. Still, you should be willing to think about AI as both a business opportunity and a leadership responsibility.

Assumptions

This book assumes that you already have a working understanding of AI in a business context. You should be familiar with core AI concepts, the role of Microsoft 365 services in the modern workplace, and the kinds of capabilities Azure AI can bring to business solutions. I also assume you have some experience leading change, influencing technology adoption, or helping an organization move from strategy to execution.

How this book is organized

This book is organized as a practical journey through AI transformation, starting with the business value of generative AI and then moving into the Microsoft technologies, adoption practices, and security foundations that make AI successful in the real world. The chapters were written in a way that they build on one another, but I also want you to feel comfortable jumping into the section that matches the decision or challenge in front of you. If you are new to AI strategy, I recommend reading the chapters in order. If you are already working on a specific initiative, such as Copilot adoption, Azure AI solution design, or AI security, you can go directly to the chapter that helps you move that work forward.

The book is organized as described here:

- Chapter 1 introduces the business value of generative AI and explains the foundational concepts leaders need to understand before making investment decisions. It covers how generative AI differs from traditional AI, how to select the right type of AI solution for a business need, how models such as pretrained and fine-tuned models differ, and why cost, tokens, ROI, reliability, bias, hallucinations, prompt engineering, grounding, RAG, data quality, and machine learning all matter.
- Chapter 2 focuses on Microsoft's AI apps and services, including Microsoft 365 Copilot, Microsoft Copilot, Copilot Chat, Copilot Studio, Microsoft Graph, Azure AI services, Azure AI Search, Azure AI Vision, Azure AI Foundry, and the build, buy, or extend decisions leaders must make when mapping business processes to AI capabilities.
- Chapter 3 shifts from technology to adoption and governance. It explains how to align AI strategy with Microsoft Responsible AI principles, establish governance, create an AI council, build an adoption team, identify adoption barriers, launch

an AI Champions program, and make licensing and subscription decisions that support real usage and measurable value.

- Chapter 4 brings everything together through the lens of security, with practical design considerations for identity, data, and cloud protection in AI solutions. It covers Microsoft Entra for identity and agent security, Microsoft Purview for data protection, classification, governance, and DSPM for AI, and Microsoft Defender for Cloud for securing AI workloads across cloud and multicloud environments. My recommendation is to read this book as both a guide and a reference: follow it chapter by chapter if you want the full end-to-end story or return to specific chapters when you need help making a decision, explaining a concept, or designing a safer and more effective AI strategy.
- The appendix is included to assist you in preparing for the AI Transformation Leader Exam (AB-731).

While the goal of the book is broader than exam preparation, the structure intentionally follows many of the decisions and concepts an AI transformation leader must understand to identify business value, choose the right Microsoft AI capability, plan adoption, apply responsible AI principles, and design security controls for identity, data, and cloud environments.

If you are preparing for AB-731, use the chapters to build your understanding and use the appendix as a review guide to test whether you can explain the concepts in your own words. That is the real goal: not just passing an exam but also becoming confident enough to lead AI transformation responsibly.

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

MicrosoftPressStore.com/AB731leadingAI/errata

If you discover an error that is not already listed, please submit it to us on the same page.

For additional book support and information, please visit *MicrosoftPressStore.com/Support*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *support.microsoft.com*.

This page intentionally left blank

Foreword

When Yuri asked me to write the foreword for his book on AI transformation, I thought long and hard about what my message should be. This is an important subject, and the stakes feel especially high right now.

Regardless of where you sit in the AI debate, one thing is clear: we are at an inflection point in technology. I've spent the last 20 years in cybersecurity, and today, I lead an AI security organization. From where I sit, this moment is both an opportunity and a risk. The good news is that we as leaders get to choose what we make of it.

AI is disrupting a wide range of industries, and security most of all. Attackers, as usual, are moving asymmetrically. They are quicker to put AI to work in their day-to-day operations. This doesn't mean some magic has been sprinkled over them and they've become unstoppable. Like the rest of us, they are simply raising their productivity. They augment skills they didn't have before, and they get more output from the skills they already have.

One reason attackers can do this faster than defenders is that they don't play by the rules. They have no governance. They don't have to lead an organization through change. They can focus on one thing: the outcome. I'm not suggesting we copy that minimalist approach, because it carries real risk. But it explains the gap, and it should worry us.

This book is for the people closing that gap, the ones leading through transformation across strategy, governance, and security. My message to you is simple: weigh the opportunity cost of not doing AI. Healthcare, manufacturing, agriculture, whatever your organization touches, the productivity gains on the table are enormous if we move fast enough to capture them.

The same holds for security. Every time we slow down in the name of caution, we pay an opportunity cost. When we refuse to lean into protecting our data and our identities, where AI can help so much, we pay again. Attackers are not waiting for us to get comfortable.

So, my ask is this: Put the skills in these pages to work—for your organization and for the broader good. Treat slowing down AI as the cost it really is. Yuri has laid out, clearly and practically, how to make this transformation, and I'd urge you to lean into it.

Use this book as your guidelines, and you'll be ready to drive the change. You'll be ready to build governance that sets real guardrails, the kind that lets you adopt AI quickly and in an agile way while keeping that opportunity cost low. And for the security professionals reading this, taking Yuri's advice to heart is how you keep attackers from getting ahead of you. Staying symmetric with them is better for all of us.

David Weston
Corporate Vice President, AI Security
Microsoft

Identify benefits, capabilities, and opportunities for Microsoft's AI apps and services

"AI will create new industries and transform existing ones."

Jensen Huang, NVIDIA CEO

IN THIS CHAPTER, YOU WILL:

- Identify the benefits and capabilities of Microsoft 365 Copilot and Microsoft Copilot
- Identify the benefits and capabilities of Azure AI services

Identify the benefits and capabilities of Microsoft 365 Copilot and Microsoft Copilot

If you take a step back and look across your organization at how some of the work gets done today, you can clearly identify areas that AI can help. Not only from the perspective of automating manual tasks, but also intelligently consuming insights that will help you make faster decisions. Microsoft 365 Copilot and Microsoft Copilot are not trying to change what your organization does; instead, they are changing how your organization does it and how effective your decisions can be as an AI Leader. The intent is not to hand over to your employees another tool for them to learn, but to embed AI directly into the application that they already use in their everyday work. In this case, the scope of applications is Word, Excel, Outlook, PowerPoint, and Teams. The goal is to remove friction and speed up adoption, which can help you as an AI Leader to start seeing value almost immediately, without having to rethink your organization's entire way of working.

Microsoft 365 Copilot understands your employee's work and provides tailored answers based on the context of the user, which means that when they ask Copilot for help, it's not responding in a vacuum. The answers will be grounded on emails, files, meetings, and chats, and they will be bounded since they will focus only on the ones the user is allowed to see. That context comes from Microsoft Graph,¹ and it's what makes Copilot feel far more relevant than a generic AI chatbot. As a result, your

¹ For more information about Microsoft Graph, visit <https://learn.microsoft.com/en-us/graph/overview>.

users will get an AI that's tailored to their response based on their profile, aligned to their role, and respectful of your organization's security and compliance boundaries.

Microsoft Copilot chat, on the other hand, builds on that idea by making AI available wherever your users are. The goal is to empower every user with an intelligent assistant in their workflow, whether they are preparing for a meeting, catching up after time away, or trying to get a quick answer without digging through documents. For organizations, that means AI becomes something people use naturally, not something reserved for power users or specialized teams.

From a leadership perspective, the key is not just understanding what Copilot can do, but also recognizing how it reshapes productivity, decision-making, and even organizational culture. Copilot acts as an augmentation layer, enhancing human capability rather than replacing it. This distinction is important, especially when communicating AI strategy at the executive level.

Map business processes and use cases to Copilot

To start mapping business processes and use cases to Copilot, you can start by asking a simple question: *Where are people spending time on repetitive, cognitive-heavy tasks?* Leadership will need to have this reflection exercise with their leadership team (LT) and managers to understand the business processes that can be improved with Copilot. Let's use as an example the scenario from the Finance department of an organization. Copilot can assist with summarizing financial reports, generating forecasts, and answering natural language questions over structured data. In another scenario, now with Human Resources (HR), Microsoft Copilot can help draft job descriptions, summarize candidate interviews, and generate onboarding materials. What becomes clear very quickly is that Copilot is not a single-use case tool; it is a horizontal capability that spans multiple functions.

Leadership must understand that when they are mapping business processes to Copilot, the goal isn't to sprinkle AI everywhere (which, unfortunately, many leaders are doing during this new wave of AI adoption). Instead, leaders must be intentional about where AI can remove friction in everyday work. As your leadership team reviews the organization's business processes, they may conclude that most business processes aren't broken; they are just weighed down by repetitive and time-consuming steps. That's where Copilot adds value by fitting naturally into how work already happens. Instead of redesigning processes from scratch, you're augmenting them, so people spend less time on busywork and more time on decision-making and outcomes.

Another important part of this mapping exercise is recognizing scale. In Chapter 1, you learned that *automation + scalability = cost reduction at scale*, while *scalability + augmentation = productivity and decision quality at scale*, and if you have all three, then you have transformational ROI (which is the classic Copilot scenario). Copilot delivers the most impact when a task is performed frequently by many people. If a process involves hundreds or thousands of employees writing emails, producing reports, analyzing spreadsheets, or attending meetings, even small-time savings compound quickly. That's why Copilot is often the right fit for organization-wide processes like communications, reporting, planning, and collaboration. When mapping use cases, leaders should always ask: *How often does this task occur, and how many people do it?*

Lastly, mapping business processes to Copilot helps avoid one of the most common AI pitfalls: over-engineering. You must realize that not every use case requires a custom AI solution or a new application. In many cases, Copilot already provides the capability out of the box, securely, compliantly, and within familiar tools. A practical approach is to map business processes into three categories, as shown in Figure 2-1.

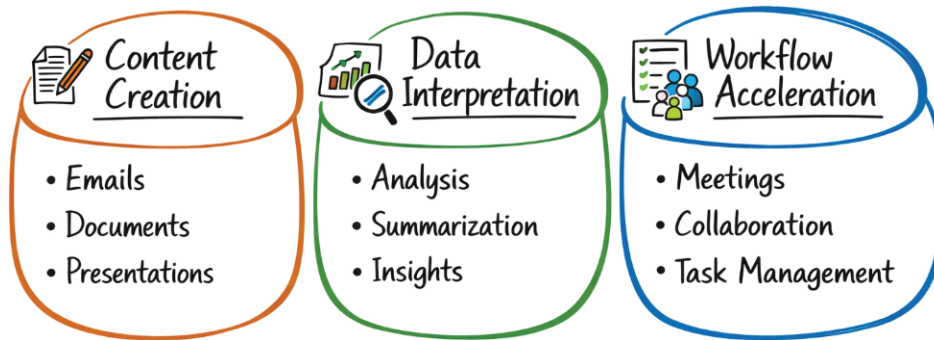


FIGURE 2-1 Mapping business processes

While Figure 2-1 offers some examples for each category, you should use this opportunity to revisit your business process and see which additional elements can be mapped to each category. Once mapped, leaders can prioritize use cases based on impact and ease of adoption. High-frequency, low-risk tasks are usually the best starting point.



Important From the leadership perspective, keep in mind that you don't need to solve everything on day one. Start with common, low-risk use cases, prove value through daily usage, and then expand as people get comfortable.

A good mental shift here is to stop thinking in terms of “process automation” and start thinking in terms of “work support.” Copilot isn't trying to take over full processes from end-to-end. Instead, the goal is to help with messy, manual parts inside those processes, the parts that slow your team down or break their focus. This leads to more productivity and more time to focus on more strategic projects.

As the AI transformational leader, you should think about change management and workforce enablement. The key question is not “*Will people use Copilot?*” but “*Will they use it effectively?*” At the same time, expectations must be set clearly. Copilot is a co-pilot, not an autopilot. Organizations that invest in skills, governance, and feedback loops will not only drive adoption but also ensure that the technology delivers meaningful, sustained business value.

Understand differences in capabilities between versions of Copilot

You have probably heard the word “Copilot” many times and wondered if this is a single product. In reality, Microsoft offers multiple Copilot experiences, each designed for a different scope and level of integration. Copilot is a family of experiences; each is designed for a different context and audience. Microsoft did this on purpose. Not every scenario needs deep access to organizational data, and not every user needs AI embedded inside enterprise workflows. Understanding these differences helps you avoid over-engineering and pick the version that delivers value with the least friction.

At a high level, the biggest distinction comes down to what data Copilot is grounded in. This is a fundamental point because some Copilot experiences work primarily with public web data, while others are deeply connected to Microsoft 365 data through Microsoft Graph. This difference directly affects relevance, trust, and compliance. When you are mapping business processes to Copilot use cases, this is also something you need to take into consideration. In other words, if the scenario requires AI responses that understand internal documents, meetings, and emails while honoring existing permissions, then Microsoft 365 Copilot is the right fit. On the other hand, if the scenario is more about general knowledge or light assistance, a simpler Copilot experience may be enough.

Another important difference lies in where (user experience) Copilot shows up. Some Copilot versions are embedded in apps like Word, Excel, Outlook, and Teams, while others show up as standalone chat experiences on the web or mobile. From an adoption perspective, this matters because when Copilot is embedded directly into the flow of work, it feels like a natural extension of what people already do. But when it’s separate, it feels more exploratory or ad-hoc rather than deeply work-flow-driven. There is value in both; it really depends on which experience you need to provide for the specific scenario to which you are mapping.

Leaders who are helping in the AI transformation also have a budget to honor, which in this case is important since there are different licensing aspects when adopting Copilot. Microsoft 365 Copilot is licensed as an add-on because it unlocks organization-wide productivity value tied to enterprise data and governance. Other Copilot experiences are included or freely accessible because they’re meant to lower the barrier to entry and encourage experimentation. Table 2-1 has a comparison of Copilot versions:

TABLE 2-1 Practice mapping business scenarios with an AI approach

Copilot Version	Common Use Case Scenario	Main Features	How It’s Licensed*
Microsoft Copilot (consumer/web)	General questions, learning, brainstorming, and everyday AI assistance	Web-grounded AI chat, image generation, and general Q&A, with no organizational context	Free or consumer subscription (not tied to Microsoft 365 tenant)
Microsoft 365 Copilot Chat (web and mobile)	Secure AI chat for work scenarios without deep in-app integration	Web-grounded chat, enterprise data protection, file upload, Copilot Pages, and IT controls	Included with Microsoft 365 subscription (no add-on license)

Copilot Version	Common Use Case Scenario	Main Features	How It's Licensed*
Microsoft 365 Copilot	Productivity and knowledge work inside Microsoft 365 apps	In-app Copilot for Word, Excel, Outlook, Teams, Loop, Whiteboard, OneNote, Forms, and PowerPoint; Graph grounding; meeting summaries; document drafting	Paid add-on license for Microsoft 365 users
Microsoft Copilot Studio	Custom conversational agents and workflow extensions	Build and customize Copilot agents, connect to data sources, and enable low/no-code extensibility	Licensed separately; consumed as an extensibility platform
Microsoft Security Copilot	Security operations and incident response	Security-specific AI grounded in Microsoft Security ecosystems, and security data	Separate, role-specific (not Microsoft 365 Copilot)

* The license column has information from March 2026. Make sure to visit <https://www.microsoft.com/en-us/microsoft-365-copilot/pricing-new>.

Based on Table 2-1, it is possible to conclude that the key difference lies in context awareness. The more integrated Copilot is with organizational data and workflows, the more relevant and actionable its output becomes. So, as you choose the most appropriate Copilot for your scenario, take this deep integration into consideration when selecting the appropriate version.

Ultimately, the value of Microsoft 365 Copilot and Microsoft Copilot lies not just in what they can do today, but also in the foundation that they create for continuous innovation. By integrating AI into everyday work, aligning it with enterprise data and security, Copilot enables organizations to gradually unlock new capabilities and improve outcomes.

Understand the capabilities of Microsoft 365 Copilot Chat web and mobile experiences

Microsoft 365 Copilot Chat introduces a unified conversational interface that works across web and mobile platforms. This experience is particularly important because it becomes the “entry point” for many users interacting with AI. You can think of Microsoft 365 Copilot Chat as a secure, enterprise-ready AI assistant that helps you quickly gather information, summarize content, and draft ideas. You can upload files, ask follow-up questions, and save conversations into Copilot Pages.

It is important to emphasize that without a Microsoft 365 Copilot license, Copilot Chat is grounded mainly in web data, but still benefits from enterprise protections like identity, data boundaries, and IT controls. With a Copilot license, that same chat experience can be enriched with your work context (emails, files, and Teams meetings) based on your permission level. Figure 2-2 shows an example of the web interface that appears when you access Microsoft 365 Copilot Chat Web using the URL <https://m365.cloud.microsoft/chat>.

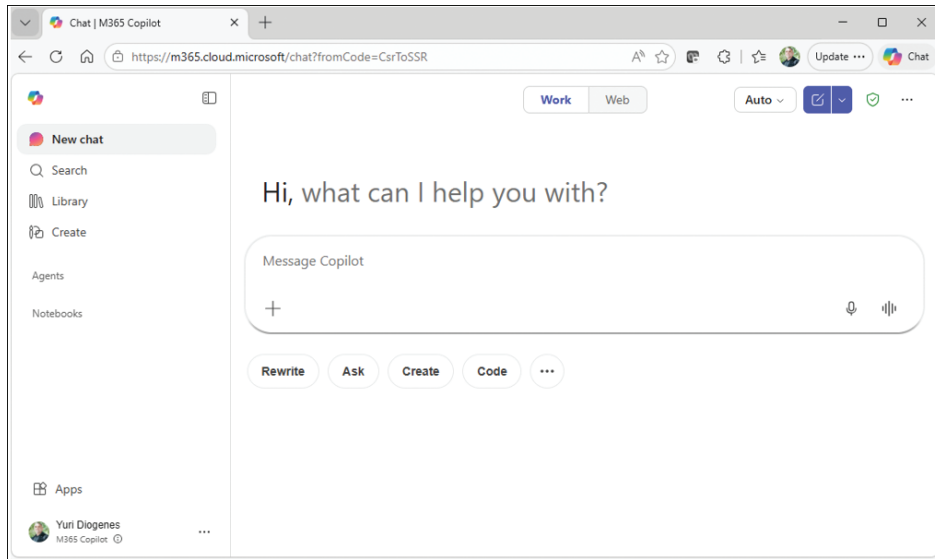


FIGURE 2-2 Microsoft 365 Copilot Chat Web

On this page, users can interact and ask questions such as: “Summarize the last three meetings I had with the security team and highlight action items.” Microsoft 365 Copilot Chat doesn’t just retrieve data; it synthesizes it. From a leadership standpoint, this reduces friction in knowledge access. Employees spend less time searching and more time acting.



Important While Microsoft 365 Copilot Chat for work is an enterprise-safe AI experience, the consumer Copilot accessible via URL copilot.microsoft.com is designed for personal use. It relies on public web data and runs outside your organization’s Microsoft 365 tenant.

Understand capabilities of the Copilot experience in various Microsoft 365 apps

One of the easiest ways to understand Copilot is to stop thinking of it as “one AI” and start thinking of it as many small helpers, each tailored to the application that you are already using to perform your daily tasks. These helpers will have peculiar behavior; in other words, Copilot behaves differently in Word than it does in Excel, and differently again in Outlook or Teams. This is intentional, and it is a good thing! Microsoft designed Copilot to adapt to the context of each application, so it helps with that specific kind of work instead of forcing a one-size-fits-all experience. Figure 2-3 shows a basic architecture² diagram of how this integration works:

² For a more in-depth explanation on the architecture and security boundaries, visit <https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture>.

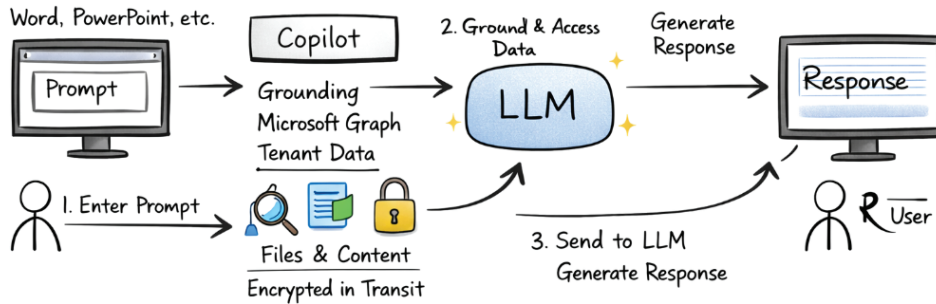


FIGURE 2-3 Microsoft 365 Copilot Chat Web

When a user, utilizing a Microsoft 365 application like Word or PowerPoint, enters a prompt in Copilot (1), Copilot preprocesses the input prompt by using grounding and accesses Microsoft Graph in the user's tenant (2). Based on this tailored request using grounding data, Copilot sends the grounded prompt to the LLM, which uses the prompt to generate a contextualized response for the user. That's when Copilot returns the response through the user interface (UI) of the application to the user (3).



Important Microsoft 365 Copilot uses Microsoft Graph to ground prompts in user-permitted organizational data and sends that context to Microsoft-hosted Azure OpenAI models, all within the Microsoft 365 tenant boundary and existing security controls.

In applications like Word and PowerPoint, Copilot is focused on creation and refinement. It helps you get past the blank page by generating first drafts, restructuring content, adjusting tone, or turning long documents into concise summaries. This is especially useful when you know what you want to say but don't want to spend time figuring out how to say it. In Excel, Copilot helps explain what your data is telling you, spot trends, create visualizations, and even suggest formulas. This enables information workers to be less occupied in wrestling with spreadsheets, quickly ask questions in plain language, and focus on making decisions based on the insights that come back.

In Outlook and Teams, Copilot helps to save time by summarizing long email threads, drafting responses, pulling out action items, and in the case of Teams, helps you to catch up on meetings you missed. Also in Teams, Copilot helps you stay oriented by recapping discussions, highlighting decisions, and outlining next steps. Leadership must understand that the value here is not only speed but also reducing cognitive load. Your team will spend less time catching up and more time contributing where it matters. Below is a quick summary of the main capabilities per application:

- **Word:** Helps draft, rewrite, and summarize documents
- **Excel:** Assists with data analysis, trend identification, and formula generation
- **PowerPoint:** Helps generate entire presentations from prompts or documents
- **Outlook:** Helps draft emails and summarizes threads

- **Teams:** Captures meeting notes, decisions, and action items in real time
- **Loop:** Helps with collaborative content creation
- **Whiteboard:** Helps draft natural language ideas into themes
- **OneNote:** Helps draft plans and generate ideas
- **Forms:** Helps draft questionnaires, surveys, and other form-based ideas

Bearing in mind those capabilities and use case scenarios are important, but as the AI transformational leader, you need to plan Microsoft 365 Copilot adoption by first establishing clarity of purpose. This should not be seen as just a technology rollout; it's a productivity transformation. As a Leader, you should ask: *Where do we lose the most time today? Which roles are overloaded with repetitive work? What outcomes do we want to accelerate? Decision-making, content creation, or data analysis?* The organizations that see the most value are the ones that tie Copilot usage directly to business scenarios, not generic enablement, for example, reducing executive reporting cycles, accelerating proposal creation, or improving meeting follow-ups. Without this alignment, Copilot risks becoming an interesting tool rather than a measurable driver of impact.

Understand the capabilities of Microsoft Copilot Studio

In Table 2-1, you learned that Microsoft Copilot Studio³ has a different use case scenario when compared with Microsoft Copilot. If Microsoft 365 Copilot is the AI that helps you work better, Microsoft Copilot Studio is the tool that lets your organization teach AI how your business works. Microsoft Copilot Studio is where you go when the built-in Copilot features aren't quite specific enough, and you want something more tailored. Think of Copilot Studio as the place where Copilot becomes customizable without forcing you into a heavy development lifecycle or complex AI engineering.

You can also think about Copilot Studio's main mission to build AI Agents,⁴ which are AI assistants that can answer questions, guide users, and take actions based on your instructions and data. The good news is that you don't need to be a developer or data scientist to do this. The experience is low-code and visual, which means business teams can design how these agents behave, what information they use, and how they interact with users. That's a huge shift from the old days of chatbots that required weeks of scripting and testing. For example, a company can use Copilot Studio to build an Agent that interacts with internal ticketing systems, retrieves policy documents, or automates approval workflows. Agents created in Copilot Studio can use enterprise data sources, including SharePoint, OneDrive, and approved websites. This ensures that responses are grounded in trusted content rather than generic web results. You can also extend these agents with Power Platform connectors and custom APIs, as shown in Figure 2-4.

³ For more information about Microsoft Copilot Studio pricing, visit <https://www.microsoft.com/en-us/microsoft-365-copilot/pricing/copilot-studio>.

⁴ For more information about AI Agents, read <https://news.microsoft.com/source/features/ai/ai-agents-what-they-are-and-how-theyll-change-the-way-we-work/>.

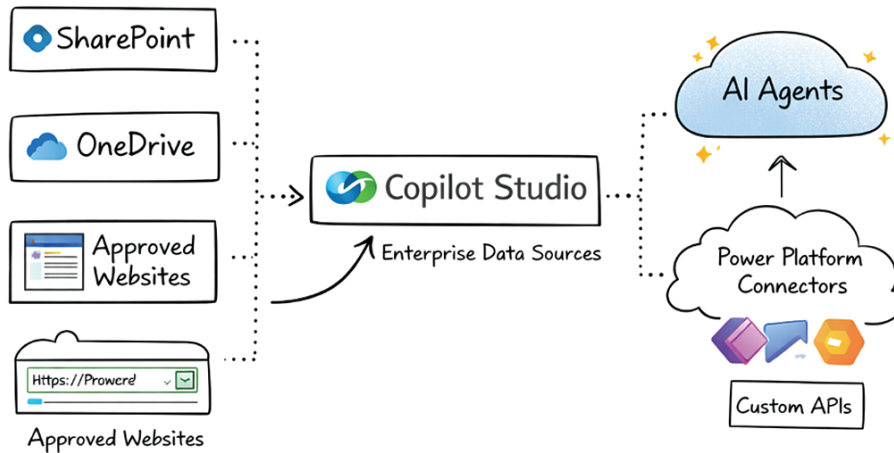


FIGURE 2-4 Agents created in Copilot Studio

It is also valid to say that Leaders usually don't start their AI journey by encouraging teams to build agents using Microsoft Copilot Studio. First, they learn how people use Microsoft 365 Copilot and Copilot Chat, where friction exists, and where generic AI stops being enough. Copilot Studio comes into play once you've identified repeatable patterns, questions people keep asking, tasks that keep getting handed off, or processes that always require manual intervention. In other words, you don't adopt Copilot Studio because it's powerful; you adopt it because you've already seen where power is needed. Having said that, each business has different needs according to its maturity level, and in some cases, some businesses may need to start their journey by creating custom agents based on pre-determined scenarios that they feel cannot be solved only by using Microsoft 365 Copilot.

Leaders should think about use cases that tend to sit at the intersection of high repetition, clear boundaries, and measurable impact. For example, the Human Resources (HR) department needs to automate the onboarding guidance or internal request workflows. You can create a Copilot Studio agent that can reduce burden across the organization by becoming a trusted first stop, answering questions accurately, and escalating or automating only when needed. Scenarios like this work well because they're contained, auditable, and easy to improve over time. Trying to solve ambiguous, judgment-heavy work with custom agents too early can lead to over-engineering and a level of complexity that your organization may not be mature enough at this point in the AI journey to deal with.

Copilot Studio should also be viewed as a governed extension layer, not an innovation free platform. Microsoft designed it to operate with enterprise controls, analytics, and governance so organizations can scale safely. That means success isn't measured by how many agents you build; instead, success should be measured by evaluating:

- How intentionally do you deploy them
- How well they're grounded in real business needs
- How clearly they improve outcomes

In practice, the strongest Copilot Studio deployments look boring on the surface, simple agents solving real problems consistently, but transformational underneath because they quietly change how work flows across your organization. Understanding the business value of Copilot Studio is critical because it aligns directly with the “extend versus build versus buy” decision model. Use Table 2-2 to understand some important questions that should be asked when thinking about building agents:

TABLE 2-2 Decision matrix

Question to Ask the Team	Considerations	Observations
Are you solving a knowledge or workflow gap?	Consider building an agent when the problem is not informational or conversational, but transactional, event-driven, or deeply system-integrated in ways that exceed what Copilot Studio connectors and flows can handle.	If the problem is that people can't find the right information, don't understand policies, or keep asking the same questions, you should not be thinking about building custom AI.
How often does this scenario happen and for how many people?	High-frequency, repeatable scenarios are ideal for extending Copilot with Copilot Studio agents.	If the use case doesn't justify a dedicated product, it probably shouldn't be built.
Does the AI need to take actions, and how complex are those actions?	You should move toward building only when actions require custom orchestration logic, advanced AI planning, multiple autonomous agents, or non-Microsoft AI stacks.	This is beyond just task automation.
Who owns this, and can it be governed safely?	When you build custom AI solutions, ownership shifts squarely to engineering and platform teams.	Leaders should treat “build” decisions the same way they treat building a new internal system: product road-map, support model, lifecycle plan, and risk acceptance.

Understand the capabilities of Microsoft Graph

You may think about Microsoft Graph⁵ as just a set of APIs, which technically is accurate. However, from an AI and business transformation point of view, Microsoft Graph is really the connective tissue of Microsoft 365. Think about Microsoft Graph as the layer that understands all about you, such as

- Who you are
- What you work on
- Who you collaborate with

Not only that, but it also understands where information lives across emails, files, chats, meetings, devices, and security signals, as shown in Figure 2-5. All these insights are exposed through a single, consistent endpoint and permission model.

If you think about AI at scale, this approach is very important. Microsoft 365 Copilot doesn't magically “know” your organization; it relies on Microsoft Graph to ground every response in real, permission-aware data. When you ask Copilot a question like “What's the latest document for this project?”

⁵ For more information about Microsoft Graph, visit <https://learn.microsoft.com/en-us/graph/overview>.

Index

Numerics

70–20-10 development philosophy, 57

A

AB-731, 97–98, 103–104

pillar questions, 101

preparation, 100–101

sample questions, 101–102

topics, 98–99

accountability, 51

Agentic AI. *See also* AI agents; Microsoft Copilot Studio

autonomy, 2

delegated trust, 92–93

AI adoption, 68–69. *See also* AI strategy

barriers, 58–59

adoption gap from pilot to scale, 60

cost and ROI uncertainty, 60

data quality, 60

human resistance, 59

lack of expertise, 59

leadership perception versus employee's reality, 59

organizational silos and lack of strategy, 60

security, 79

build-buy-extend framework, 38–39

establish an adoption team, 56–58

plan for adoption across the organization, 56

planning, 56

AI agents

attack vectors, 92

behavior-based user and sign-in risk scoring, 77

conditional access, 77–78

DSPM (data security posture management), 79–81

identity, 71, 72

information protection, 82–85

risky, 76

security risks, 71

trust boundaries, 84

AI council, 54–56, 68

AI strategy, 58–59

establish an adoption team, 56–58

establish an AI Champions program, 60–61

align champions with real business outcomes, 62–63

create a feedback loop, 62

define the role clearly, 61–62

establish the right mindset, 61

provide structured enablement, 62

recognition and awards, 62

scale the program thoughtfully, 63

establish an AI council to guide oversight and cross-functional alignment, 54–56

governance, 53–54

plan for AI adoption across the organization, 56

Responsible AI alignment, 49–50

trust, 49

AI transformation, 1

AI Transformation Leader Exam. *See* AB-731

AI-driven hiring discrimination, 49

algorithms, 3

Analyst, use cases, 37–38

augmentation, Gen AI, 11–12

automation, Gen AI, 11–12

autonomy, AI agents, 2

Azure AI Search, 42

Azure Machine Learning, 12

Azure OpenAI, 12

Azure Vision, 42

B

barriers to AI adoption

adoption gap from pilot to scale, 60

cost and ROI uncertainty, 60

data quality, 60

human resistance, 59

lack of expertise, 59

leadership perception versus employee's reality, 59

organizational silos and lack of strategy, 60

behavior-based risk scoring, 77

bias, AI models, 10

business processes

mapping to Copilot, 24–25

mapping to Microsoft AI Solutions, 35–36

mapping to Microsoft Foundry services, 40–41

C

capabilities

Microsoft 365 Copilot, 28–30

Microsoft 365 Copilot Chat, 27–28

Microsoft Copilot Studio, 30–32

Microsoft Foundry, 39–40

Microsoft Graph, 32–33

case law

Equal Employment Opportunity Commission (EEOC) v. iTutorGroup (2023), 49

Mata v. Avianca, 9

chain-of-thought prompting, 14

cloud security

risk prioritization and contextual security recommendations, 88–90

threat protection for AI workloads, 90–94

compliance, regulatory, 50

conditional access, AI agents, 77–78

consumption-based model, 7, 8

contextual grounding within the prompt, 13

Copilot, 26–27. *See also* Microsoft 365 Copilot; Microsoft Copilot

context awareness, 27

differences in capabilities between versions, 26–27

licensing, 63–64, 65–66

layered approach, 64

monthly model, 64, 65

pay-as-you-go models, 64, 65

map business process and use-cases, 24–25

Researcher, 36–37

Copilot Studio, 5, 12

copilots, 1

cost models, Gen AI, 7

D

data exposure, 34

data governance for AI, 85–87

data protection, 79

data quality, 17–18

deep learning, 2, 3

documentation, AI governance policies, 54

DSPM (data security posture management), 79–81

E-F

ethics, AI-driven hiring discrimination, 49. *See also* Responsible AI

fabricated content, 9–10

facial recognition, bias, 10

fairness, 51

few-shot prompting, 13–14

fine-tuned models, 6, 7

G

Gen AI, 2, 3

adoption, 1

augmentation, 11–12

automation, 11–12

benefits of Microsoft Foundry services, 44–46

bias, 10

choosing a solution, 4

direct costs, 7–8

infrastructure and integration costs, 8–9

ROI, 8–9

security and compliance, 5

use cases, 5

consumption-based model, 7–8

cost models, 7

data integration, 4

data quality, 17–18

differences with traditional AI, 3–4

discriminatory practices, 49

fabricated content, 9–10

fine-tuned models, 6, 7

fully customized models, 4

grounding, 15–16

overreliance, 10

platform-based approaches, 4

prebuilt solutions, 4

pretrained models, 6, 7

prompt engineering, 13

chain-of-thought prompting, 14

constraints, 14

contextual grounding within the prompt, 13

few-shot prompting, 13–14

output structuring, 14

role prompting, 13

RAG (retrieval-augmented generation), 16–17

reliability, 10

unstructured data, 17

value, 11–12

governance, 1, 2
 AI, 53–54, 68
 data, 85–87
 integrated Microsoft AI solution, 34–35
 grounding, 15–16, 27–28

H-I

hallucination, 9–10

identity. *See also* Microsoft Entra

AI agents, 71, 72
 signals, 74–75

inclusiveness, 51

information protection, 82–83

governance integration, 84–85
 operating philosophy, 84
 protection granularity, 84
 protection of AI-generated content, 84
 trust boundaries for AI agents, 84
 use cases, 83

integrated Microsoft AI solution, 33–34

data exposure, 34
 governance, 34–35
 operational visibility, 35
 prompt and response safety, 34
 trust, 35

J-K-L

licensing

Copilot, 26–27, 63–64, 65–66
 layered approach, 64
 monthly model, 64, 65
 pay-as-you-go models, 64, 65
 Microsoft 365 Copilot, 27
 Microsoft Foundry, 66
 pay-as-you-go models, 67
 PTUs, 67, 68

LLMs (large language models), 2–3

M

machine learning

deep learning, 3
 solution lifecycle, 19–20
 use cases, 19

Microsoft 365 Copilot, 5, 9, 12

contextual responses, 23–24

licensing, 27, 65

Outlook and Teams, 29–30

use cases, 27

Word and PowerPoint, 29

Microsoft 365 Copilot Chat, 12, 27–28

Microsoft AI Solutions

build-buy-extend framework, 38–39
 business process mapping, 35–36

Microsoft Copilot, 5

integrated AI, 24
 use cases, 26

Microsoft Copilot Studio

building AI agents, decision matrix, 32
 capabilities, 30–32
 use cases, 27

Microsoft Defender for Cloud, 87

AI-SPM (AI Security Posture Management), 87–88,
 89–90

DCSPM (Defender Cloud Security Posture
 Management), 88

Defender for AI Services, 92

risk prioritization and contextual security
 recommendations, 88–90

threat protection for AI workloads, 90–94

Microsoft Entra, 71

adaptive access with conditional access,
 77–78

Agent ID, 72–74

Agent ID dashboard, 73–74

behavior-based user and sign-in risk scoring, 77

ID Protection, 75–76, 77

identity signals, 74–75

Microsoft Foundry, 4, 5, 12

Azure AI Search, 42

Azure AI Search + Azure OpenAI, 12

Azure Vision, 42

business process mapping, 40–41

capabilities, 39–40

licensing, 66

pay-as-you-go models, 67

PTUs, 67, 68

RAG architecture, 12

Responsible AI support, 45

scalability, 44, 45–46

security, 44, 45–46

Microsoft Graph, 24, 32–33

Microsoft Purview

data classification and sensitive data detection,
 81–82

data governance for AI, 85–87

- data protection, 79
- DSPM (data security posture management), 79–81
- information protection
 - governance integration, 84–85
 - operating philosophy, 84
 - protection granularity, 84
 - protection of AI-generated content, 84
 - trust boundaries for AI agents, 84
- information protection for AI apps and agents, 82–85
- machine learning classifiers, 82
- SITs (Sensitive Information Types), 82
- Microsoft Responsible AI, 10–11
- Microsoft Security Copilot, 12, 27
- models
 - comparison, 7
 - fine-tuned, 6
 - matching to a business need, 43–44
 - pretrained, 6
- monthly subscriptions, Copilot, 64, 65

N-O

- neural networks, 2, 3
- NLP (natural language processing), 3
- operational visibility, integrated Microsoft AI solution, 35
- output structuring, 14
- overreliance, 10
- oversight, AI council, 54–56

P

- pay-as-you-go models
 - Copilot, 64, 65
 - Microsoft Foundry, 67
- policies
 - AI governance, 54
 - conditional access, 77–78
- predictive forecasting, 5
- pretrained models, 6, 7
- principles
 - governance, 53
 - Responsible AI, 51–52
- privacy, Rep, 51
- prompt engineering, 8, 13
 - chain-of-thought prompting, 14
 - constraints, 14
 - contextual grounding within the prompt, 13

- few-shot prompting, 13–14
- output structuring, 14
- role prompting, 13
- PTUs (provisioned throughput units), 67, 68

Q-R

- RAG (retrieval-augmented generation), 4, 5, 8, 12, 16–17
- regulatory compliance, 50
- reliability
 - Gen AI, 10
 - Responsible AI, 51
- Researcher, use cases, 36–38
- Responsible AI, 5, 10–11, 45–46, 68
 - accountability, 51
 - aligning with AI strategy, 49–50
 - fairness, 51
 - goals, 52
 - inclusiveness, 51
 - layered approach, 52
 - Microsoft Foundry, 45
 - privacy and security, 51
 - regulatory compliance, 50
 - reliability and safety, 51
 - risk assessment and mitigation, 50
 - transparency, 51
- risk scoring, 77
- risky sign-in, 76
- ROI (return on investment), Gen AI, 8–9
- role prompting, 13
- roles and responsibilities
 - AI adoption team, 57–58
 - AI Champions, 61–62
 - AI council, 55–56

S

- scalability, Microsoft Foundry, 44, 45–46
- security
 - cloud, risk prioritization and contextual security recommendations, 88–90
 - data classification and sensitive data detection in AI, 81–82
 - data protection, 79
 - DSPM (data security posture management), 79–81
 - identity
 - AI agents, 71, 72
 - signals, 74–75

- information protection
 - governance integration, 84–85
 - operating philosophy, 84
 - protection granularity, 84
 - protection of AI-generated content, 84
 - trust boundaries for AI agents, 84
 - use cases, 83
- information protection for AI apps and agents, 82–83
- Microsoft Foundry, 44, 45–46
- Responsible AI, 51
- risk scoring, 76
- Zero Trust, 72, 74
- signals, identity, 74–75
- sign-in, behavior-based risk scoring, 77

T

- tokens, 8
- traditional AI, differences with Gen AI, 3–4
- training, 70–20-10 approach, 57
- transparency, 51
- trust, 35, 49

U-V

- unstructured data, 17
- use cases. *See also* business processes; capabilities
 - Analyst, 37–38
 - Copilot, 24–25
 - Gen AI, 5
 - information protection, 83
 - machine learning, 19
 - Microsoft 365 Copilot, 27
 - Microsoft Copilot, 26
 - Microsoft Copilot Studio, 27
 - Microsoft Foundry, 40–41
 - Microsoft Security Copilot, 27
 - Researcher, 36–38
- users, behavior-based risk scoring, 77

- value, Gen AI, 11–12

W-X-Y-Z

- Zero Trust, 72, 74. *See also* trust