



K2's AI Workshop: Implementing What We've Learned



What About Randy?



- 40+ years of technology experience, top-rated speaker for almost 40 years
- Top 25 Thought Leaders in Accounting 2011-2026
- 2004-2025 Accounting Today 100 Most Influential in Accounting for twenty-two years
- Inducted Accounting Hall of Fame, Feb 2011
- Monthly columns on technology in CPA Practice Advisor, weekly podcasts on technology
- Published author of six books, from Hutchinson, KS
- randy@k2e.com or randyj@nmgi.com
- 620-664-6000 x 112



Learning Objectives



Identify the steps for querying data from tools such as Gemini and ChatGPT

List three capabilities of Microsoft's Copilot service

Differentiate between the capabilities of free and paid AI tools

Name some of the risks associated with AI









What is Artificial Intelligence? What are the major capabilities?

GETTING STARTED WITH AI

Most Finance Teams Are Here. Today We Move Forward









The AI Experimenter

-  Uses ChatGPT or Claude occasionally — no repeatable workflow
-  Asks AI to write emails or summarize documents
-  Hasn't changed core finance processes
-  Skeptical of outputs; rarely acts on them without heavy review
-  Thinks of AI as a curiosity, not infrastructure
-  Still spending 3 days on close, 2 days on the board deck

TODAY



AI-Powered Finance Team

-  AI embedded in repeatable monthly workflows — not optional
-  Claude handles the first draft; humans handle judgment
-  Close commentary written in minutes, not days
-  Models flex in real time when CEO asks "what if" questions
-  Risk register is a living document, not an annual exercise
-  Board narrative reviewed — not written — by the CFO

What Is Artificial Intelligence?



- Stated simply, **artificial intelligence (AI) uses computers to perform tasks that humans would perform otherwise**
- Some examples of AI applications include **machine learning (ML), speech recognition, and analyzing data for trends**
- Notably, most who study the topic consider **ML to be a subset of AI...** further, almost every business professional uses ML, although many may not recognize that they use it
 - Adding rules to Outlook could be considered an example of ML



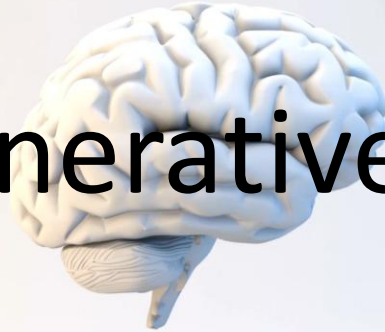
Gartner AI Hype Cycle



So, Why All The Recent Buzz About AI?



Generative AI!

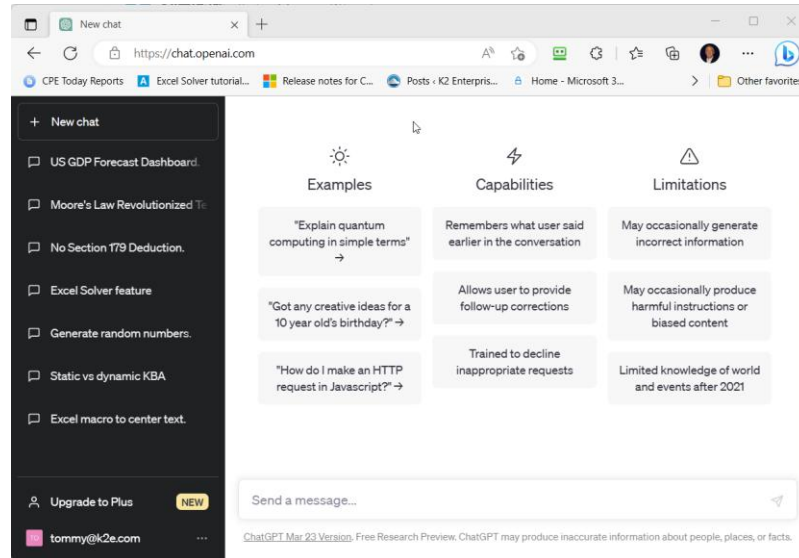


New Terminology



- **Tokens** – Units of resource for AI to work. A rough measure of a unit is a word or syllable of a word
- **Context Window** – The number of Tokens an AI can have in memory at a time. This includes all background processing. Current models: 1 Million.
- **MCP Server** – Tools for AI to connect to external applications. Established by Anthropic
- **Agents** – AI that can take actions or build tools
- **Retrieval Augment Generation** – Known as RAG. Method of giving a dataset for the AI to work with
- **Markdown** – structure for representing formatting (bold, italics, heading, etc.) in plain text.

And The Latest Star Of The Show...



What Is Generative AI?



- Conceptually, generative AI is quite simple...it is a form of AI **that allows technology to generate customized responses to your questions and prompts**
- Recent advancements in **Large Language Models (LLMs)** allow generative AI tools such as **ChatGPT** and **Gemini** to create responses to your questions
- It might be fair to **think of generative AI tools as turbo-charged search engines**

Today's Biggest Generative AI Tools



ChatGPT (Open AI)

- Launched in **November 2022**
- Microsoft has invested **\$11B**
- The free version (3.5) was last updated in January 2022
 - **v4.0 in Plus \$20/mo.**
 - **Teams \$30/mo., Enterprise plan**
 - **GPT-4o (omni) new on 5/13/24**
 - **Sora for AI Video 12/9/24**
- <https://chat.openai.com>

Gemini (was Bard by Google)

- Available in **March 2023**
- Like ChatGPT, you sign-up for a subscription
- Currently, **no charge** for Gemini Basic, but Gemini Advanced is \$19.99/mo. in Google One Premium subscription
- <https://gemini.google.com/app>

Today's Biggest Generative AI Tools



Copilot (Microsoft)

- Launched in **February 2023**
- Developed by **OpenAI**
- Microsoft has invested **\$10-20B**
- Initially launched as Bing Chat, now in Windows 11, M365
 - **M365 \$30/mo., Enterprise plan**
 - **Free in Windows 11, Edge**
 - **Phi-3 new on 4/23/24**
- <https://copilot.microsoft.com/>

Claude (Anthropic)

- Released in **March 2023**
- Amazon has invested **\$4B**
- Currently, **no charge** for Claude
 - **Claude Pro \$20/mo., Opus**
- <https://claude.ai/chats>

Today's Biggest Generative AI Tools



Perplexity AI

- Launched in **August 2022**
- In app citations, exceptional source referencing, real-time web access
 - **Pro Plan \$20/mo.**
 - **Can upload and analyze local files**
- <https://www.perplexity.ai/>

Llama (Meta)

- Released in **February 2023**
- Llama 3 in April 2024
- Currently, **no charge** for Llama, open-source
 - **Defense Llama from Scale AI**
 - **Lockheed Martin and Palantir**
- <https://www.meta.ai/>

Safest AI Tools Last Year Constitution/ Indemnification



Safety

- Claude
- Copilot
- Perplexity AI
- ChatGPT
- Gemini
- LLaMA (Meta)



Popularity

- ChatGPT – 60.2% (14% in India)
- Copilot – 12.8%
- Gemini – 15.3%
- Perplexity AI – 5.5%
- Claude – 4.9% (80% business)
- All others below 1%

What A Difference A Year Makes!



Engines & Purpose

- **Google (Gemini / Vertex AI / APIs)** - currently dominates inference volume and cost-sensitive workloads
- **OpenAI / Microsoft (GPT models via OpenAI API, Azure OpenAI, Copilot)** - Still the largest ecosystem by revenue and consumer reach, but pricing pressure + enterprise shifts away from GPT in coding and large-scale inference
- **Anthropic (Claude family)** - Enterprise leader by spend and production usage, especially in coding, agentic workflows, and regulated environments
- **Meta (LLaMA ecosystem)** - Dominates open-source model usage, on-prem and cost-contained deployments

Estimated Global Share

- Google (Gemini) 35–40%
- OpenAI / Microsoft (GPT) 25–30%
- Anthropic (Claude) 15–20%
- Meta (LLaMA) 8–10%
- Amazon (Bedrock / Titan) 5–7%
- China + Others 5–8% (combined)

Which AI Engines Fit Accounting



CPA / Accounting Use Case	Best-Fit AI Engines	Why
Tax research & memo drafting	OpenAI (GPT), Anthropic (Claude)	Long-form reasoning, citations, structured writing
Audit workpapers & risk assessment	Anthropic, OpenAI	Consistency, predictable, fewer hallucinations
Client email drafting & summaries	Microsoft Copilot (GPT)	Native M365 integration, governance
Bookkeeping transaction QA	Google (Gemini), Anthropic	High-volume pattern detection, low-cost inference
Financial statement review	Anthropic, OpenAI	Stable reasoning over large documents
Advisory forecasting & modeling	Google, OpenAI	Data transformation + scenario analysis
Coding (Excel, Power Query, Python)	Anthropic (Claude)	Best-in-class code generation and refactoring
Document classification & OCR assist	Google, OpenAI	Multimodal strength and scale
AI copilots embedded in firm apps	Microsoft, Google	Identity, security, admin controls
Private / on-prem AI workloads	Meta (LLaMA)	Control, cost containment, privacy

Evolution Of AI



- **AI 1.0.** Predictive or rules-based systems that classify, score, or detect
 - **AI 2.0.** Generative systems that create text, images, code, and summaries
 - **AI 3.0.** Agentic systems that work through steps and loops to pursue outcomes
- **Why “steps” matter.** Earlier AI use was often a one-shot interaction: ask a question, get an answer. AI 3.0 matters because many real business tasks are not one-shot tasks. They require several linked activities such as gathering information, applying rules, using software tools, checking for exceptions, and deciding what to do next. A step-based design lets AI move through that work in a more structured way.
 - **Why “loops” matter.** The “loop” is what makes the system adaptive. The AI does not just complete Step 1, Step 2, and Step 3 mechanically. It can review what happened, detect problems, revise the plan, call another tool, and continue until it reaches an acceptable result or needs human review. That iterative pattern is a core distinction between simple AI assistance and more agentic AI behavior.

AI 3.0 – Steps/Loops



Where is the puck going?

- AI 3.0 generally refers to the move from single-response AI to **multi-step, goal-driven** AI systems
- Instead of answering one prompt and stopping, the system works through a sequence: it plans, acts, checks results, and repeats as needed
- Often described as a reasoning-action loop or agentic loop.
- Recent overviews from Salesforce, IBM, and other enterprise sources describe agentic systems this way: they break work into steps, use tools, evaluate intermediate results, and iterate toward a goal

Agentic AI



Why This Still Matters

1. **Execution** - It shifts AI from answering to doing.
2. **Efficiency** - It can reduce workflow friction in high-volume, rules-based work.
3. **Capacity** - It creates leverage without requiring a full staffing increase.

Accounting-Oriented Projects

- **Close orchestration.** Monitor tasks, detect delays, and report close status.
- **Client document chase.** Request, track, and escalate missing tax or CAS items.
- **AP exception review.** Flag duplicates, unusual vendors, and policy violations.

MCP – Model Context Protocol



Why This Matters More

- **Standardized connectivity.** MCP creates a common way for AI tools to connect with data, applications, and services.
- **Better agent performance.** AI agents become more useful when they can securely reach the systems where work happens.
- **Less integration waste.** Firms can reduce one-off connectors and lower the risk of being locked into a single vendor ecosystem.
- ***The real value of AI increasingly depends on how well it connects to the firm's tools, data, and workflows.***

Vibe Coding



Finding your groove or brain fry fatigue?

- OpenAI co-founder Andrej Karpathy — [coiner](#) of the term "vibe coding" — told the No Priors podcast he's been in a "[state of AI psychosis](#)" since December. Y Combinator CEO Garry Tan, too.
- **Lower barrier.** More professionals can help build useful software with natural language.
- **Faster innovation.** Ideas can move from concept to prototype much more quickly.
- **Broader participation.** Domain experts can shape tools directly instead of waiting on developers.
- ***Vibe coding matters because it turns software creation into a faster, more accessible business capability—while also increasing the need for review and governance.***

The Benefits Of Being AI Agnostic



1. Reduces vendor lock-in
2. Supports better-fit solutions for different use cases
3. Improves negotiating leverage and cost control
4. Strengthens risk management
5. Makes innovation easier
6. Supports resilience and continuity

The Risk Of Being Too AI Agnostic



Flexibility Without Focus Creates Problems

- **Too much complexity.** Supporting too many AI tools can increase training, governance, and support burdens.
- **Fragmented workflows.** Users may duplicate work or move inconsistently across disconnected platforms.
- **Higher risk exposure.** More tools can mean greater demands for privacy, security, compliance, and contract review.
- ***The goal is not to use every AI tool. The goal is to preserve choice while standardizing where it matters.***

What Do Agent Tokens Cost?



- Microsoft Copilot / OpenAI (GPT family) Typical cost
 - Microsoft Copilot (M365): ~\$30 per user / per month
 - Azure OpenAI (custom apps, integrations)
 - Input tokens: ~\$2–\$5 per million
 - Output tokens: ~\$8–\$15 per million (model-dependent)
 - Anthropic (Claude) Typical cost (API only)
 - Input tokens: ~\$2–\$3 per million
 - Output tokens: ~\$8–\$15 per million
 - No per-user license
- Google Gemini / Vertex AI Typical cost structure
 - Gemini Flash (lightweight, high-volume)
 - Input: ~\$0.35–\$0.75 per million tokens
 - Output: <\$1.50 per million
 - Full Gemini Pro / Ultra
 - Input: ~\$1–\$3 per million
 - Output: ~\$4–\$10 per million
- Tools & Platform (n8n is free)

Token Cost For Projects



Rate Reference		Claude \$3/\$15 /MTok	OpenAI \$2.50/\$10 /MTok	Gemini \$1.25/\$10 /MTok	Copilot \$30/user/mo
Task	Tokens (In / Out)	Claude (\$)	OpenAI (\$)	Gemini (\$)	Copilot
Extract Invoice	1,200 in / 400 out	\$0.0096	\$0.0070	\$0.0055	Subscription
Draft an Email	500 in / 600 out	\$0.0105	\$0.0073	\$0.0066	Subscription
Analyze Fin. Stmt's	6,000 in / 2,500 out	\$0.0555	\$0.0400	\$0.0325	Subscription
Create a Budget	2,000 in / 3,500 out	\$0.0585	\$0.0400	\$0.0375	Subscription

What Do Licenses Cost?



- ChatGPT (OpenAI)
 - ChatGPT Go - \$8 / mo.
 - ChatGPT Plus - \$20 / mo.
 - ChatGPT Pro - \$200 / mo.
- Microsoft Copilot 365 - \$30 / mo.
- Anthropic (Claude)
 - Claude Pro \$20 / mo. (\$17/mo. annual)
 - Claude Max \$100–\$200 / mo.
- Google Gemini
 - Google AI Plus \$7.99 / mo.
 - Google AI Pro (Gemini Advanced) \$19.99 / mo.
 - Google AI Ultra \$249.99 / year (~\$20.83/mo.)
- Perplexity
 - Perplexity Pro \$20 / mo.
 - Perplexity Max \$200 / mo.

What is Claude for Finance?



Claude is not a search engine.

It is a large language model (LLM) trained to reason, write, analyze, and generate code. Think of it as a highly capable analyst who can hold an entire context — your data, your instructions, your company's situation — and produce work at the level of a skilled finance professional.

- **Reads and reasons over documents**
Upload a CIM, a GL export, a contract — Claude reads it
- **Generates and runs code**
Python, SQL, Excel formulas — writes and explains all of it
- **Writes in your voice**
Board memos, management commentary, investor narratives
- **Reasons through ambiguity**
"What does this pattern mean for our close?" — it thinks it through

Not the Same As...

Google Search

Finds links. Claude synthesizes.

ChatGPT

Different model, different strengths. Claude excels at long-form reasoning & code.

Copilot in Excel

A specific tool. Claude is a reasoning partner, use it across everything.

RPA / Macros

RPA executes rules. Claude understands context.

3 Tools. One Team. Different Jobs



Claude Chat

chat.claude.ai

"Your senior analyst who never sleeps"

Best for:

- ✓ Upload a document and interrogate it
- ✓ Generate board narratives & commentary
- ✓ Reason through a complex scenario
- ✓ Design a model architecture before building

Claude Cowork

Desktop Application

"Your automation layer — works on your actual desktop"

Best for:

- ✓ Open, read, and update Excel files
- ✓ Pull data across multiple open documents
- ✓ Populate templates from source files
- ✓ Draft and send email alerts automatically

Claude Code

claude.ai or Terminal

"Your quant on demand — writes and runs Python/SQL"

Best for:

- ✓ Financial models with full scenario logic
- ✓ Anomaly detection scripts from GL data
- ✓ LBO / DCF / driver-based model scaffolds
- ✓ Automated Excel output with charts & formats

AI in Accounting – Where Hours & Impact Are



Where accounting spends their time (typical month):

Reconciliations & variance hunting



AI: High

Journal entries & adjustments



AI: Medium

Narrative writing (memos, commentary)



AI: Very High

Data gathering & formatting



AI: High

Close checklist management



AI: Medium

Meetings & review cycles



AI: Low

62% of a controller's month is in activities where Claude delivers meaningful time savings. The math is obvious — the question is just whether you build the workflow.

Task	Claude Chat	Claude Cowork	Claude Code
Analyze a P&L or GL for anomalies	✓ Primary		✓ For recurring script
Write a board financial narrative	✓ Primary		
Populate an Excel template from PDF data		✓ Primary	
Build a 3-scenario financial model	✓ Design phase		✓ Build phase
Run monthly KRI refresh & email alert		✓ Primary	
Analyze a CIM / due diligence doc	✓ Primary		
Build an LBO / DCF model	✓ Architecture		✓ Build phase
Update board deck with new financials		✓ Primary	
Write a risk register from scratch	✓ Primary		
Automate anomaly detection monthly			✓ Primary



Differentiating Between The Leading AI Players

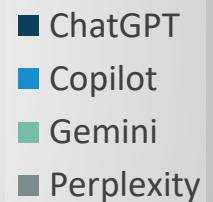
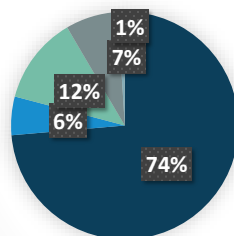


AI Market Share – Consumer Users

Claude has not been considered a consumer product

Consumer Market Share As Of February 2026

Source: Gemini





AI Market Share – Business Users

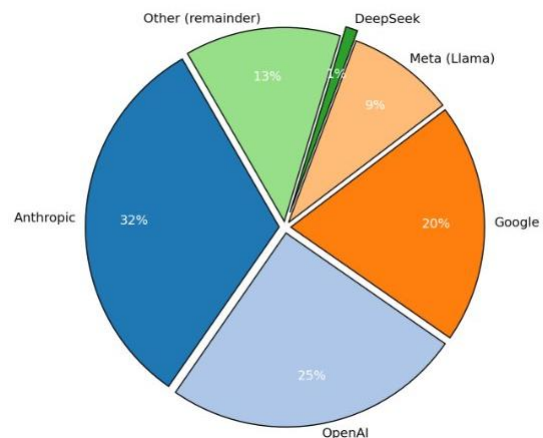
Business Market Share As Of February 2026

Source: Gemini



AI Market Share – Business Users

Just two months later...





With an understanding of the
previous

NOW, ONTO COPILOT, in depth



It's A Copilot, Not An Autopilot!

- Much like a PC, a calculator, spreadsheets, word processors, and other technologies, **Copilot is another tool** for you to use
- Copilot does what you tell it to do, helping you to work more **efficiently and effectively**
- However, you can use Copilot in conjunction with **agentic AI** tools to automate many business processes, improving efficiency and accuracy along the way
- You will learn more about agentic AI later in this session



Comparing The Copilot Offerings

Offering	Targeted User Base	Key Features
Copilot (free)	General use	Basic AI Chat, Limited Usage
Microsoft 365 Personal	Individuals	Copilot Integrated Into Office Apps
Microsoft 365 Family	Households	Shared Usage & AI Across Devices
Microsoft 365 Premium	Individual Power Users	Advanced AI, Office, And Security
Copilot Chat	Enterprise Users	Free AI Chat Grounded In Web
Microsoft 365 Copilot	Organizations	AI In Workflow And Admin Controls
Copilot Studio	Enterprise Developers	Custom AI Agent Creation



Before Going Into Demo Mode, Let's Learn About Enterprise Data Protection



Enterprise Data Protection (EDP)

EDP is a series of controls, commitments, policies, and procedures that collectively can work together to help maintain the privacy and security of your data, your prompts, and the responses that you receive

EDP is available for users of **Microsoft 365 Copilot** and **Microsoft 365 Copilot Chat**



Key EDP Features And Provisions

- EDP secures your data via **encryption**, both at rest and in transit
- Additionally, EDP uses **physical security controls and data isolation** to help minimize risks to your data
- Microsoft asserts that the company will **help to maintain the privacy of your data and supports GDPR, the EU Data Boundary, and ISO/IEC 27018**
- Additionally, Microsoft states that the company complies with its **Data Protection Addendum**, which you can view [here](#)



Key EDP Features And Provisions

- Data processed by Copilot stays within your M365 tenant
- **Role-based access control**
- M365 Copilot natively honors **Sensitivity Labels, Encryption, and Data Loss Prevention** policies established in **Microsoft Purview**
- All Copilot interactions are logged and can be reviewed in the **Microsoft 365 Compliance Center** **
- Subscribing companies retain complete control of their data

- *Requires Microsoft Purview service to be licensed and configured in your M365 tenant*



Key EDP Features And Provisions

- Some Copilot offerings support and honor any access and control policies that you establish, such as identity models, permissions, sensitivity labels, and retention policies
- Further, some Copilot offerings help to protect against security and copyright risks, including minimizing the risk associated with harmful content and prompt injections
- Additionally, some Copilot offerings do not use your data to train foundation models: ***“prompts, responses, and data accessed through Microsoft Graph aren’t used to train foundation models”***



Creating Effective Copilot Prompts



Writing Effective Copilot Prompts

As you likely know by now, issuing **prompts** is how you ask your generative AI platform to do something for you
For example, you could issue the following prompt to virtually any generative AI tool, including Copilot

What is the capital of Indiana, what is its population, and what is the median income in the state?



Tips For Effective Copilot Prompts

- Be specific and clear
- Define your desired output format
- Establish the desired tone and style
- Provide enough detail for the AI tool to understand your request
- Use keywords and industry phrases

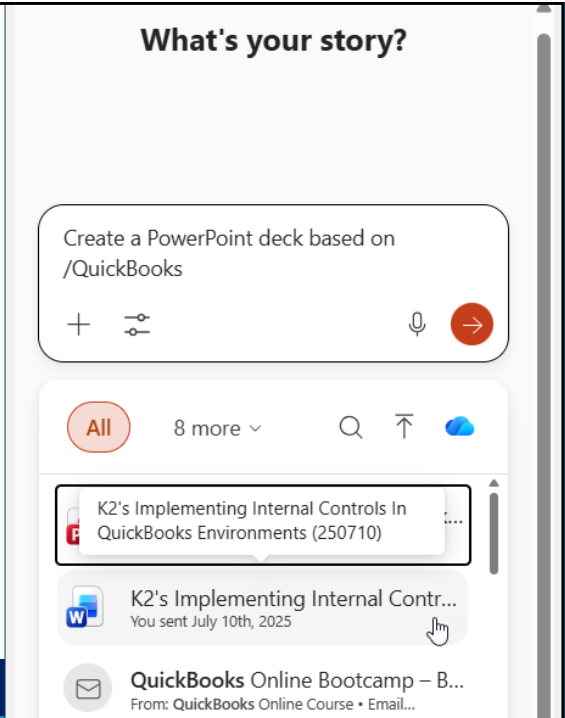


Tips For Effective Copilot Prompts

- Break complex tasks into segments
- Remember, this is an iterative process
- Don't be afraid to experiment
- Offer examples
- AI has limitations and may not understand elements, such as sarcasm or nuance

Also, The Slash Character Is An Ally

When you want to reference data from your OneDrive account, you can use the slash “/” character as a shortcut. This feature can be a tremendous time saver!



Types of prompts

Ask

Ask prompts encourage users to inquire or seek information about a specific topic or task.

Inform

Inform prompts provide users with detailed information or explanations regarding a particular subject.

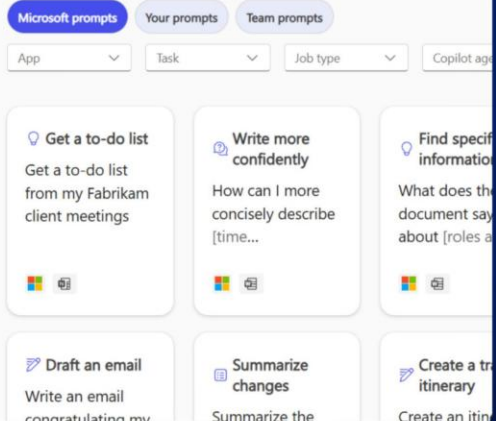
Direct

Direct prompts guide Copilot to perform specific actions or tasks with clarity and purpose.

Create

Create prompts inspire users to generate new ideas or content, fostering creativity and innovation.

Prompts to try

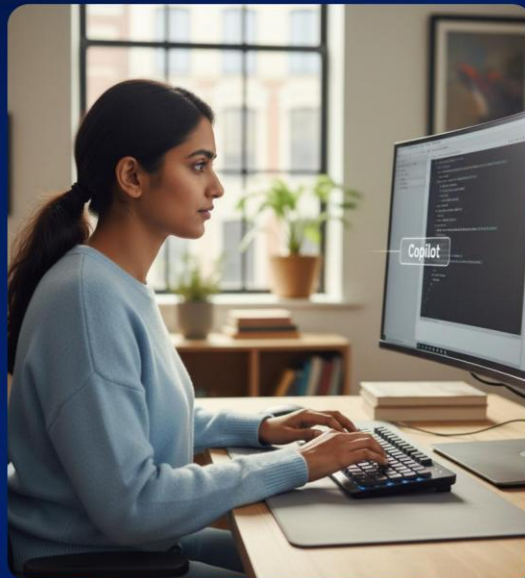


Untrain your brain!

“Write something”

VS.

“Write a two-paragraph email inviting prior volunteers to an upcoming program planning session, and include a reference to the impact of their previous involvement?”



Strategies to create prompts that get results



Be Specific About
the Task



Set the Tone



Ask for Structure



Provide Context



List Key Points or
Requirements



Review, Rewrite, Revise



Analyzing Business Data With Copilot



Analyzing Business Data With Copilot

You can use Copilot in several ways to help you analyze business-oriented data. Included are options for:

- Gathering data
- Data scrubbing/cleansing
- Generating descriptive analytics
- Forecasting and predicting
- Identifying risks
- Analyzing historical results and comparing them to expectations



Using Real-world Data...let's See Examples Of Copilot's Integration With Microsoft 365 Apps

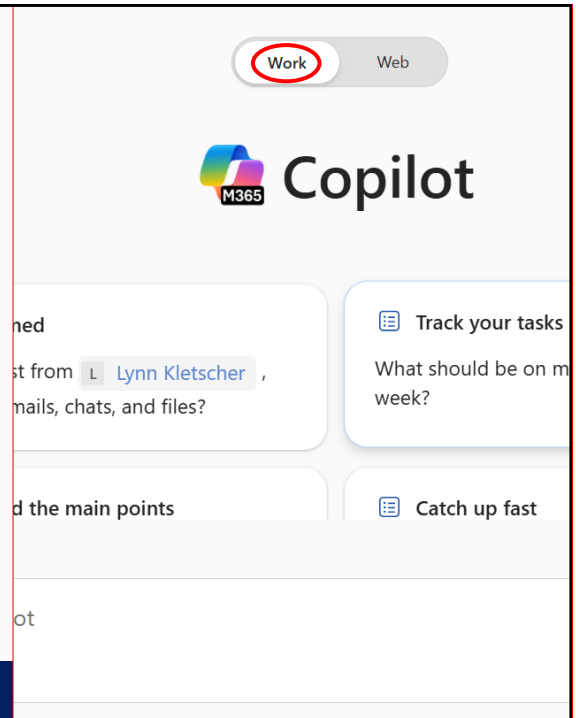


Copilot And Your Microsoft 365 Apps

With a qualifying Copilot subscription, you can integrate your Excel, Word, Outlook, PowerPoint, and Teams apps so that Copilot automates many of the rote, repetitive actions you would otherwise need to complete manually
Let's get into some examples...

Toggle Between Work and Web

Users can select **Work** and access internal data, in addition to web-based data
EDP is in force when using this feature



Comparing The Two Options



Work

- Can assist when responding to emails
- Creating PowerPoint presentations
- Creating meeting transcripts
- Analyze Excel data

Web

- Conducting market research
- Locating external resources
- Generating content
- Analyzing data available to the public



Copilot Use Cases With Word

Write a document

Proof a document

Rewrite existing content

Convert text into a table

Summarize a document

Ask questions about a document



1st Example - Integrating Copilot With Word

Perhaps the most direct form of integrating Copilot to Word is to have Copilot draft a document for you

To have Copilot automate the task:

- Open Word
- Locate the Copilot icon
- Issue a prompt for Copilot to draft a document for you...for example, "Create a 600-word report that describes possible cases for using artificial intelligence in business settings."
- With the report created, issue a prompt to "Modify the tone to make it more formal."

2nd Example - Integrating Copilot With Word



Have Copilot write a summary of a lengthy contract or other similar document
To have Copilot automate the task:

- Open Word
- Locate the Copilot icon
- Issue a prompt for Copilot to summarize the document for you...for example, “Create a 200-word summary of the document”

Copilot Use Cases With PowerPoint



- Create a slide show from an existing document
- Create a slide show from an outline
- Add a slide or image to an existing presentation
- Summarize a lengthy presentation
- Get insights and advice from an existing presentation

1st Example - Integrating Copilot With PowerPoint



You can use Copilot to create PowerPoint presentations from scratch, from Word documents, or from PDFs

To have Copilot automate this task:

1. *Open PowerPoint*
2. *Choose the **Create presentation about** option and enter a topic of interest for you*
3. *Explore using the Designer feature to modify the “look”*

2nd Example - Integrating Copilot With PowerPoint



In this example, use an existing Word or PDF document as the foundation of the PowerPoint presentation

To have Copilot automate this task:

1. *Open PowerPoint*
2. *Choose the **Create presentation from** option and choose a Word or PDF document to serve as the base for your newly-created PowerPoint presentation*
3. *Again, consider how you could modify the formatting to improve the presentation’s look*

3rd Example - Integrating Copilot With PowerPoint



In this example, we will use Copilot to summarize an existing presentation
To have Copilot automate this task:

1. *Open any existing PowerPoint presentation or use the one you created in the previous example*
2. *In the Copilot pane, issue the following prompt: "Summarize the key points of the presentation"*

Copilot Use Cases With Excel



- Assist with writing formulas
- Create charts from existing data
- Build a PivotTable from existing data
- Write macros and scripts
- Python code generation
- Ideas and Insights



Integrating Copilot With Excel

Many options exist to integrate Copilot with Excel, and some have been in Excel for several years, with no need to use Copilot to take advantage of Excel

- For example, Excel's Analyze Data feature will do exactly what its name indicates it will do...Analyze Data helps you to understand your data
- Analyze Data
- ...let's check that one out!

This prompt caused Copilot to generate a list of tasks to complete from an Outlook Inbox

Work Web

Today

please check my email and let me know if there are any tasks I need to complete

Copilot

Sure, Tommy! Here are some tasks that need your attention based on your recent emails:

- Feedback on Pricing Structure:** [redacted] has requested your feedback on the 1 and 2-hour pricing structure for societies in relation to the [redacted] structure (1).
- AI Unboxed Event:** [redacted] has proposed several dates for the [redacted] event in May and June. You need to confirm your availability and preferences for the event schedule (2).
- [redacted] has informed you about a payment from [redacted] and is awaiting your confirmation on the breakdown of the remaining balance (3).
- [redacted]: Casey Sims is looking for session titles and descriptions for the [redacted] event scheduled for [redacted].
- Year-End Engagement for [redacted]:** [redacted] has outlined several items needed to start the year-end process for [redacted] to ensure last year's adjusting entries are recorded, complete year-end bookkeeping, and upload necessary documents (5).
- 2025 Plans and Partnership Discussion:** [redacted] has summarized the discussion points for 2025 plans and partnership opportunities with [redacted]. You need to review and provide your thoughts on the proposed schedule, course content, and partnership strategies (6).
- [redacted]: [redacted] has created a folder for you to upload your video and handouts for the [redacted]. You need to confirm if you plan to record in some other way (7).
- Multi-State Events:** [redacted] to expand the event schedule and is available to discuss additional multi-state events (8).
- Speaking Rates and Availability:** [redacted] to respond to an inquiry about your speaking rates and availability for an event in May 2025 (9).
- [redacted] as provided details about the CPA Educators Conference and is looking forward to seeing you in San Diego. You need to review the draft agenda and shipping instructions (10).

Can you summarize the key points for the Year-End Engagement task? Can you draft a response for the [redacted] session details?

Can you provide more details on the [redacted] event dates? View prompts

Message Copilot

Add content

0 / 10000

Copilot

Agents

- Visual Creator
- Get agents
- Create an agent

Recent chats

- please check my email and let 6:12 PM
- how do i integrate copilot wit 4:37 PM
- provide a detailed set of inst 10:26 AM
- 2023-Disney-Annual-Report ... 9:48 AM
- What is the capital of Iowa, w 9:04 AM

See more

Integrating Copilot With Outlook

26, K2 Enterprises, LLC



Integrating Copilot With Outlook

Another example of Copilot integrating with Outlook to generate a response to a thread of email messages.

The screenshot shows an Outlook interface with a 'Re:' field and a 'Summarize' button. Below, a 'Summary by Copilot' box contains a numbered list of four points from an email thread. A red arrow points from the text box above to the 'Summary by Copilot' header. At the bottom of the summary box, it says 'AI-generated content may be incorrect'.

Summary by Copilot

- 1. invited to do a tech-related session at on April 24th.
- 2. but mentioned a scheduling conflict, being available from 1:30 p.m. to 4:15 p.m. Central.
- 3. scheduled for the 1:45 p.m. - 2:45 p.m. CT time slot and invited to discuss the topic either over a call or in San Diego.
- 4. provided a Google Drive link for to upload the course video and materials.

AI-generated content may be incorrect



Let's Analyze A Set Of Financial Statements Using Copilot

Work **Web**

Today

Prompt

2023-Disney-Annual-Report 1.pdf Analyze the attached financial statement of Disney, looking for trends and patterns in the data that would help describe Disney's financial performance

Result

Copilot

Sure, Tommy! I've analyzed the financial statement of Disney for the fiscal year 2023. Here are some key trends and patterns that describe Disney's financial performance:

Revenue Growth

Disney's total revenues for fiscal 2023 increased by 7% to \$88.9 billion compared to \$82.7 billion in fiscal 2022 [1]. This growth was driven by higher service revenues, which rose by 7% to \$79.6 billion, and product revenues, which increased by 10% to \$9.3 billion [1].

Segment Performance

- Entertainment:** Revenues increased by 3% to \$40.6 billion, with growth in Direct-to-Consumer (DTC) services and Content Sales/Licensing [1]. However, operating income decreased by 32% to \$1.4 billion due to higher programming and production costs [1].
- Sports:** Revenues slightly decreased by 1% to \$17.1 billion, primarily due to lower affiliate fees and advertising revenue [1]. Operating income decreased by 9% to \$2.5 billion [1].
- Experiences:** Revenues grew by 16% to \$32.5 billion, driven by higher theme park admissions, resorts and vacations, and merchandise sales [1]. Operating income increased by 23% to \$9.0 billion [1].

Cost Management

Total costs and expenses increased by 5% to \$79.9 billion [1]. The increase was primarily due to higher

Can you provide more details on the restructuring and impairment charges?

What are the main drivers behind the increase in theme park revenues? How did the Direct-to-Consumer services perform in detail?

View prompts

Copyright 2026, K2 Enterprises, LLC

Integrating Copilot With Teams

- You can **integrate Copilot with Teams** to automate many rote, repetitive tasks that most users do not want to perform or handle using manual procedures
- Examples include **summarizing threads of messages and providing recaps of meetings**
- To take advantage of this integration, your **Admin team will need to enable several options and configuration settings**

K2 Enterprises

Copyright 2026, K2 Enterprises, LLC



Integrating Copilot With Teams

Once your Copilot and Teams settings are established appropriately, you can use Copilot to

- **Generate a complete transcription of the meeting**
- In the transcript, Copilot can list
 - Key discussion points
 - Action items
 - Follow-up questions and issues
- Also, in-meeting support includes **answering questions, summarizing discussions, and helping late-arriving participants catch up** to the current topics of discussion



Copilot – Beyond The Basics

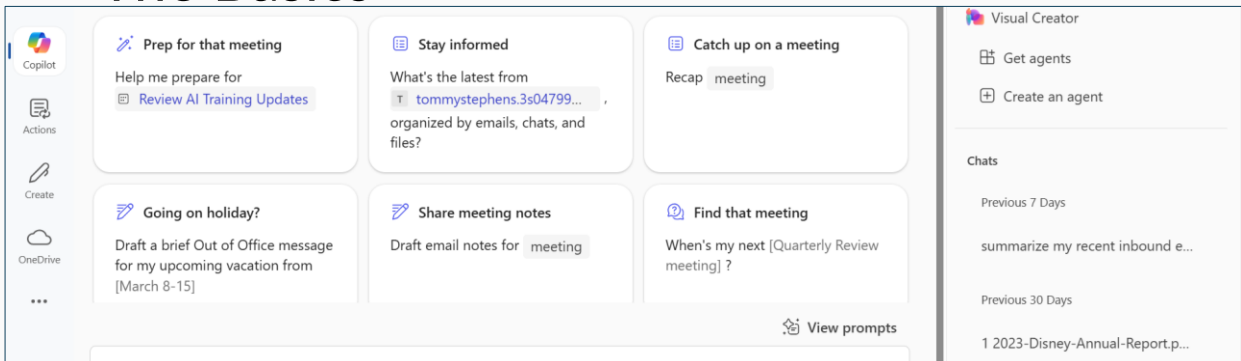


Copilot – Beyond The Basics

- Using Copilot to automate routine tasks offers tremendous options for improving efficiency, accuracy, and effectiveness
- But, **you can move beyond Copilot's basic functions to automate many rote, repetitive tasks**
- To take advantage of this capability, access Copilot from your browser at <https://m365.cloud.microsoft/chat/>
- Then, click the **Work** button near the top of the window



Copilot – Beyond The Basics



The screenshot displays the Microsoft Copilot interface. On the left is a navigation sidebar with icons for Copilot, Actions, Create, and OneDrive. The main area is a grid of task suggestions:

- Prep for that meeting**: Help me prepare for [Review AI Training Updates]
- Stay informed**: What's the latest from [tommystephens.3s04799...] organized by emails, chats, and files?
- Catch up on a meeting**: Recap [meeting]
- Going on holiday?**: Draft a brief Out of Office message for my upcoming vacation from [March 8-15]
- Share meeting notes**: Draft email notes for [meeting]
- Find that meeting**: When's my next [Quarterly Review meeting] ?

At the bottom right of the grid is a **View prompts** button. To the right of the grid is a **Visual Creator** section with options to **Get agents** and **Create an agent**. Below that is a **Chats** section with filters for **Previous 7 Days** and **Previous 30 Days**, and a list of chat items including **summarize my recent inbound e...** and **1 2023-Disney-Annual-Report.p...**



Copilot – Beyond The Basics

- Now, you can take advantage of many of the automations available in Copilot to make your “day in the life of” flow more smoothly and efficiently
- For example, Copilot offers some suggestions, such as **helping you to prepare for an upcoming meeting**
- Or, you can **ask Copilot to update you on the latest emails, chats, and files from a specified team member**



Managing Conversation History

By default, **Copilot saves all your conversations**

- You can view and access prior conversations, if desired
- To do so, **view the Conversation History in the Copilot app**

If you want to delete a conversation, **access the conversation in the left pane, click the ellipsis, and choose Delete**

Also, note the option to save a conversation to a **Notebook**

- A Notebook is a collection of content that you store to facilitate quick-and-easy retrieval and analysis



Copilot And Agentic AI



Agentic AI

- **Agentic AI** gives you the opportunity to customize Copilot so that it meets your specific needs
- Further, you can use Agents to run specific tasks on a fixed schedule, further elevating your productivity
- Note, however, you may need to ask your IT staff to enable custom agents for you
- Note the presence of an existing library of agents, such as **Researcher**, **Analyst**, **Microsoft 365 Admin**, **AI Meeting Notes**, **TeamsMaestro**, and others



Agentic AI Characteristics

Autonomous Decision-Making

Agentic AI systems can make **independent decisions** and act without constant human guidance or supervision

Goal Pursuit and Adaptation

These AI systems pursue **set objectives** and **adapt to new situations** or changing environments effectively

Planning and Self-Improvement

Agentic AI plans **actions**, **evaluates results**, and **learns from experience** to enhance future outcomes

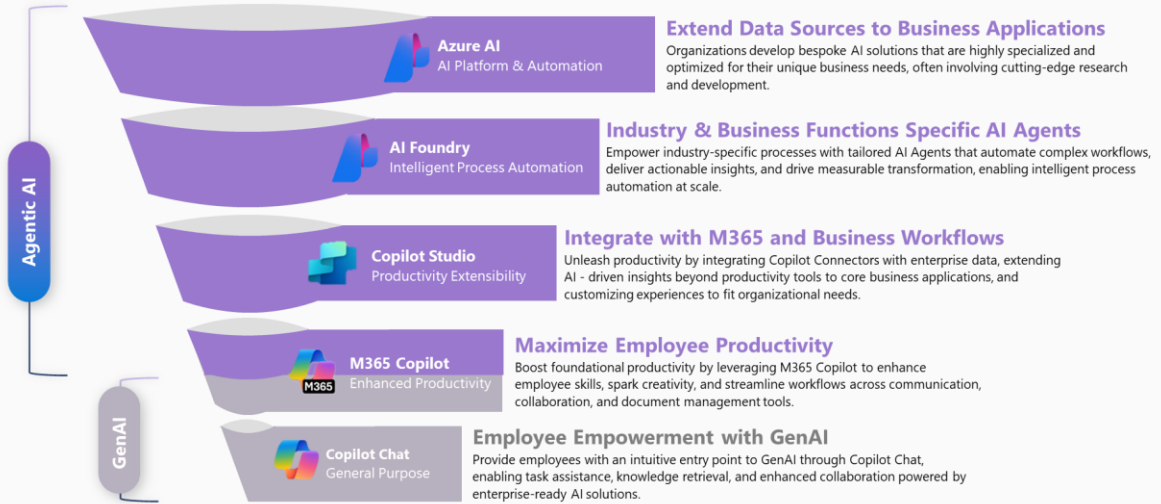


The Role Of “Agents” With Copilot

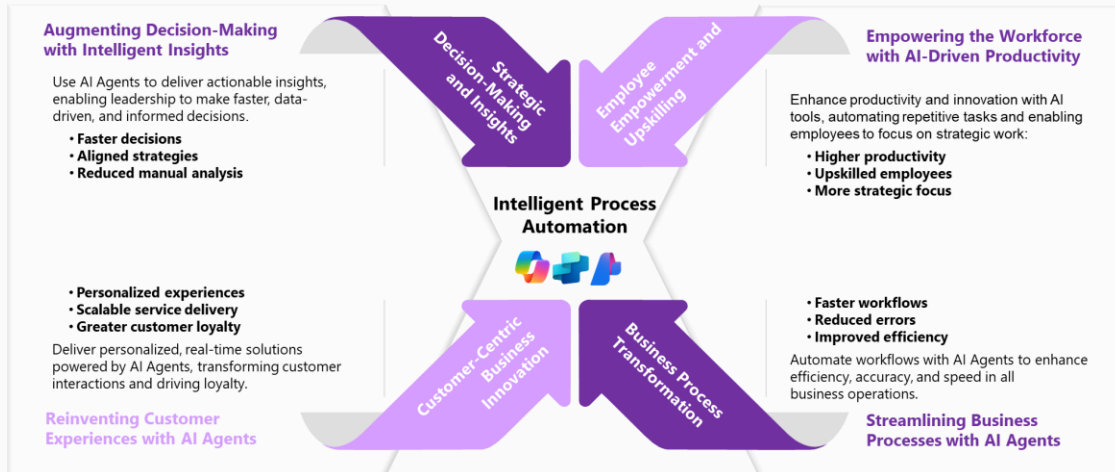
- If desired (and allowed), you can use “agents” to extend Copilot’s **functionality**
- An **agent is a digital assistant** you can use to provide real-time support and automation of tasks
- **Agents help by automating tasks**, with minimal input required by the end user
- For example, you can use agents to **summarize your calendar** and have the **summary delivered every morning at 6:00 a.m.**

AI Tool Levels

Detailed below are the various levels of GenAI tools, ranging from the more simplistic tools in terms of functionality i.e. Copilot for M365, to the more complex tools such as AzureOpen AI Service and custom-built AI solutions developed for a very specific purpose.



Driving Business Value with Intelligent Automation



Copilot's Agents Enable Higher Levels Of Productivity



- Clicking the **Agents** button on the left side of the Copilot window provides access to **numerous options to save time and delegate routine tasks to Copilot**
- You can also access and use third-party agents with Copilot for more sophisticated tasks

A Simple Agent Creation Example



Read all emails in my Inbox every morning at 6:00 a.m. and prepare a report of all the items I need to complete on the same day



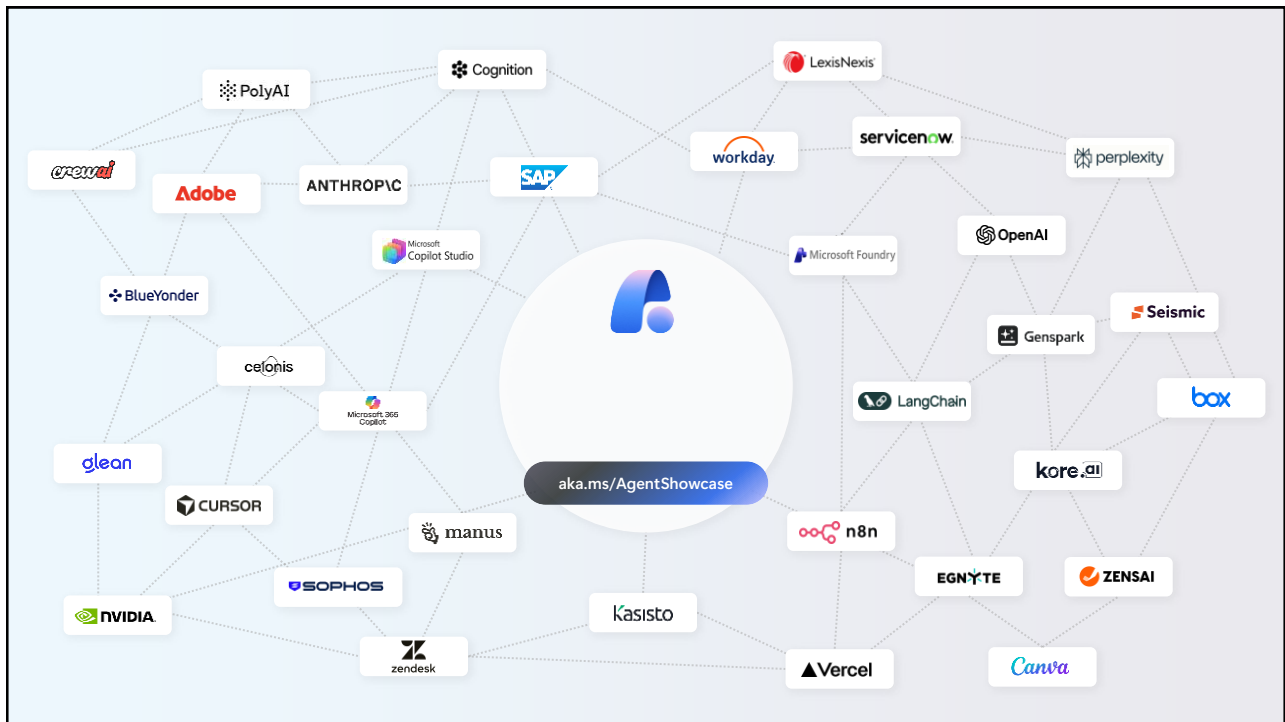
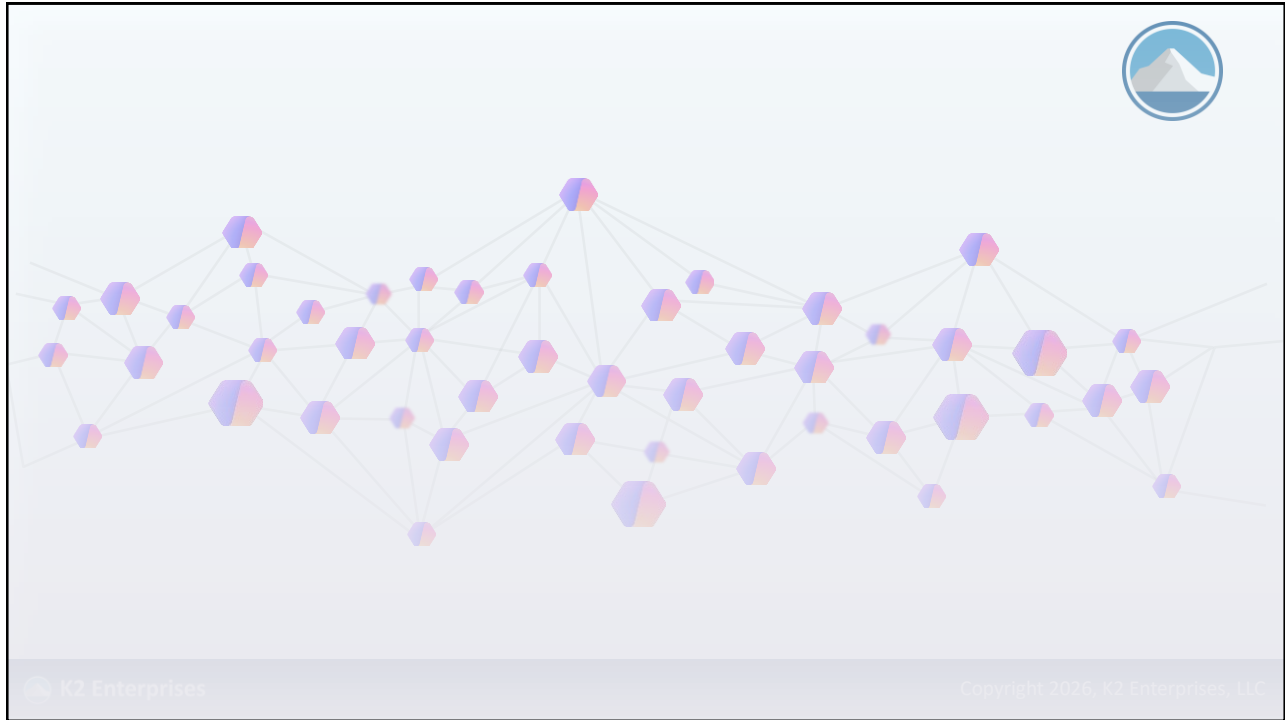
Microsoft Copilot Studio

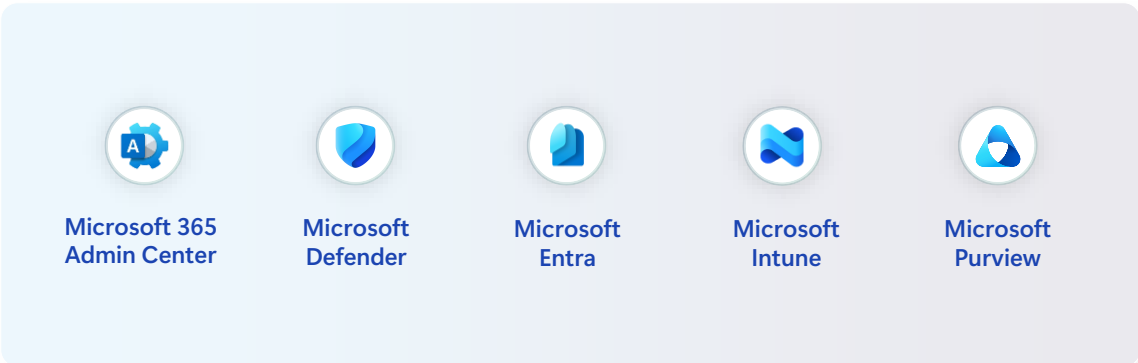

- **Microsoft Copilot Studio** is a graphical, low-code tool that allows users to build AI agents and agent flows
- You can create custom agents or enhance Microsoft 365 Copilot with generative AI, sophisticated dialog creation, knowledge, actions, and built-in analytics
- Copilot Studio connects to other data sources using prebuilt or custom plugins, enabling users to enhance logic
- You can deploy these agents across multiple channels, if desired

Agent 365


Materials courtesy of Ryan Rager & Microsoft


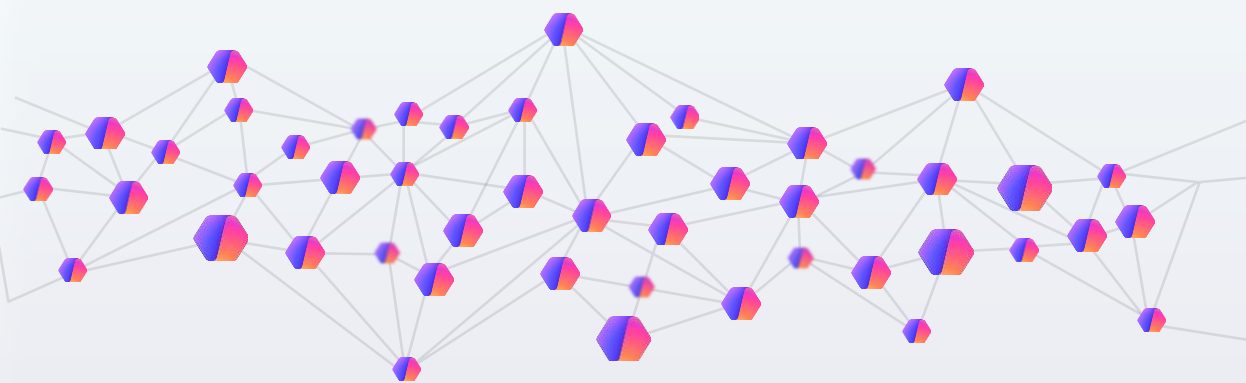






Microsoft 365 Admin Center Microsoft Defender Microsoft Entra Microsoft Intune Microsoft Purview


 K2 Enterprises Copyright 2026, K2 Enterprises, LLC



Can we track and monitor all agents?
Do we know what agents are doing?

Do we have proper guardrails for agents and people that interact with them?

Are agents protected? Do they have the right access? Can they leak sensitive data?

 K2 Enterprises Copyright 2026, K2 Enterprises, LLC



Now Available

Microsoft Agent 365

The control plane for agents



K2 Enterprises



The control plane for agents



Observe/Audit 
Monitor and manage all agents in real time from a single view

Govern 
Establish guardrails for agents and users

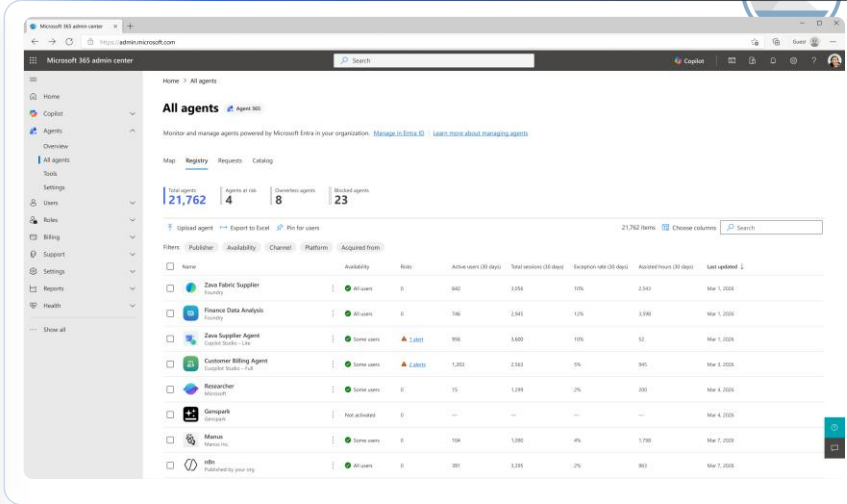
Secure 
Protect agents comprehensively



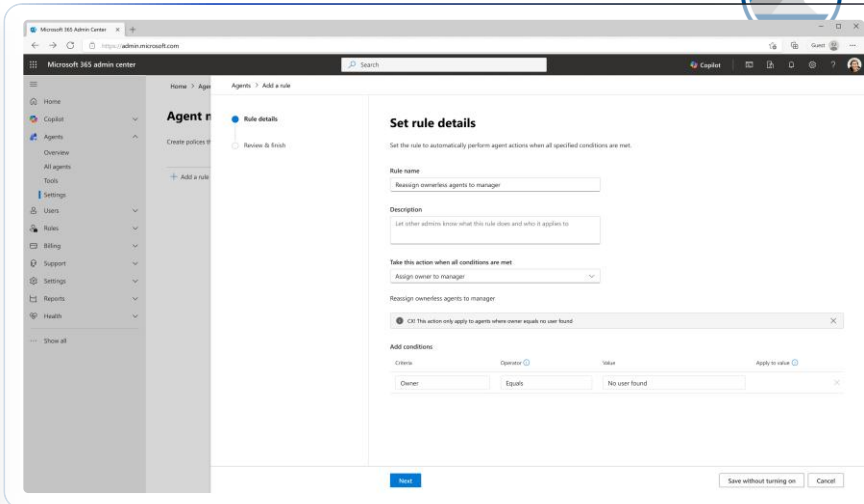
K2 Enterprises



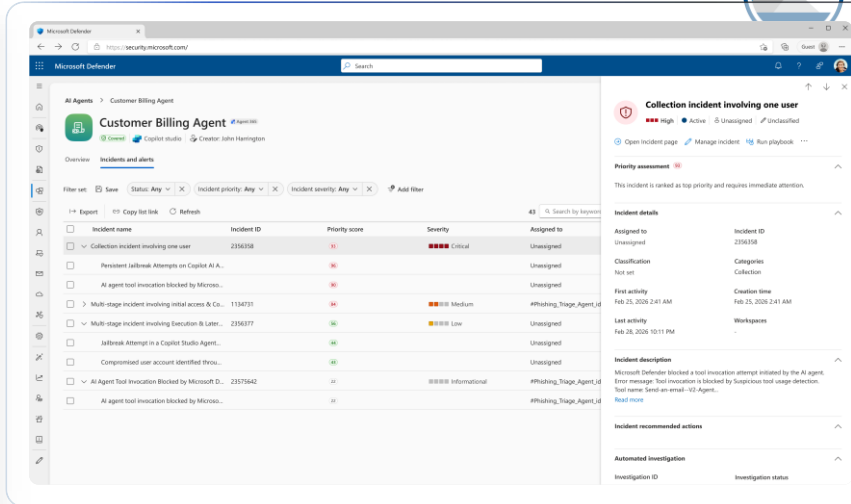
- Gain visibility into agents in your environment
- Understand how they're used
- Act quickly on performance behavior & risk signals before they impact the business.



- Establish guardrails for agents and people
- Onboard agents with IT oversight
- Govern agent access to resources and data
- Be audit ready with built-in compliance and data retention.



- Secure agent identities
- Control access to resources
- Prevent data oversharing and leaks
- Defend against threats & vulnerabilities with enterprise-grade security solutions.



Microsoft 365 E7

The Frontier Suite



Now available

Microsoft 365
Microsoft 365 E5
 +
 Entra Suite
 Secure productive work

Microsoft 365
Copilot
 AI built for work

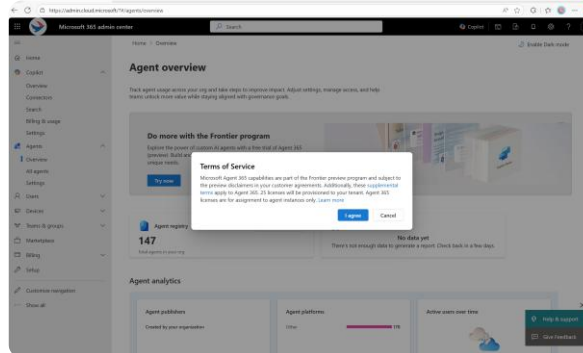
Microsoft
Agent 365
 Control plane for agents

Work IQ



Get started with Agent 365

- As an admin, go to admin.microsoft.com
- If you're already enrolled in the Frontier program, click "Try now" on the Agent overview page and accept terms.
- If not already in the Frontier program, Select Copilot > select Settings > under User access, select Copilot Frontier > choose the groups to grant access.



Learn more

[Agent 365 Overview](#)

[Agent 365 Documentation](#)

[Agent 365 Blog](#)



Let's Go Into Demo Mode And Create A New Agent



Copilot Studio And Agents

Create an agent that summarizes my day for me. Specifically, I need it to summarize all the emails in my inbox. I also need it to let me know of any outstanding items in my to-do list or tasks and, in particular, highlight any

Features labeled as 'preview' are subject to supplemental terms. [See terms](#)

Name	Type	Last modified	Last published	Owner	Protection status	Engaged sessions
Copilot in Power Apps	Agent	# Microsoft Copilot Studio 2 m...	2 months ago	SYSTEM	Protected	0

Explore agents

- Website Q&A**
Agent template
Instantly answer user questions using the content of your website or other knowledge.
- Voice**
Agent template
An agent with voice capabilities.
- Safe Travels**
Agent template
Provides answers to common travel questions and related health and safety guidelines.
- Financial Insights**
Agent template
Help financial services professionals get quick and concise info from their org's financial documents and other available resources.



Copilot Studio And Agents

Researcher

Daily Summary Assistant

All agents

Create agent

Conversations

- Preparing a Microsoft Copilot ...
- Understanding Notebooks in ...
- Target Market for Microsoft Co...
- Managing Conversation Histor...
- Difference Between Microsoft ...

All conversations

Pages

- Notebooks
- Create

- Summarize my day**
Give me a summary of today's emails and tasks.
- Highlight urgent tasks**
What tasks are due in the next 24 hours?
- Show important emails**
List emails from k2e.com and meeting invites.
- Outstanding items**
What items are still outstanding on my to-do list?
- Daily recap**
Provide a recap of today's key emails and tasks.
- Upcoming deadlines**
What deadlines are approaching soon?

Microsoft Copilot



- **Copilot** is an AI-based platform that works much like a personal assistant and is powered by **ChatGPT-4**
- Copilot is **available in Windows 11** and you can enable it by going to **Settings, Personalization, Taskbar, and toggling the Copilot toggle switch “ON”**
- You can also access Copilot in the Edge browser using a feature known as **Bing Chat**
 - Open the Edge browser and enter a search phrase
 - Edge populates a pane on the right side of the Window with the search response

Microsoft Copilot



- Once you enable Copilot, you can use it to access ChatGPT-4 by clicking the Copilot icon in the Taskbar and typing your topic of interest, such as “***compare the advantages and disadvantages of operating as an S corporation from an income tax perspective***”
- Beyond the free subscription, you can elect a **paid subscription (\$30 per month) to Copilot Pro**
- Pro adds **better performance, faster creation of images**, along with **some integration** with Word, Excel, PowerPoint, Outlook, and OneNote

Microsoft Copilot



Question

Compare the advantages and disadvantages of operating as an S corporation from an income tax perspective.

- ✓ Searching for: advantages and disadvantages of S corporation from an income tax perspective
- ✓ Generating answers for you...



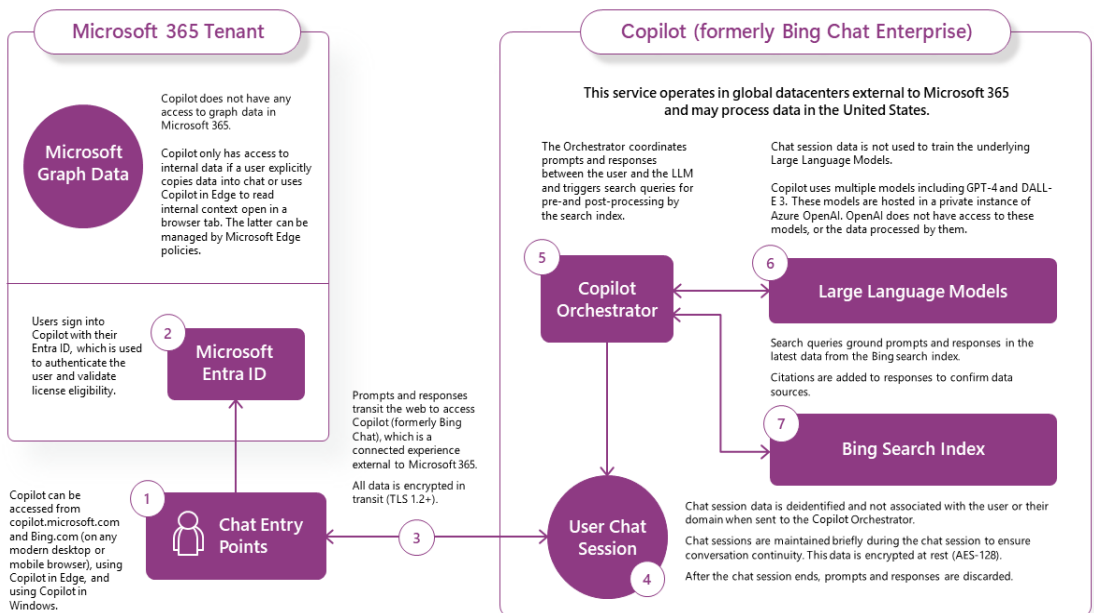
Response

Operating as an S corporation from an income tax perspective has both advantages and disadvantages. Here are some of the main points to consider:

Advantages:

- **Avoidance of double taxation.** The earnings of an S corporation are only taxed once, at the level of its shareholders. This is significantly better than for a C corporation, where the corporation is taxed and then again when any distributions to shareholders are taxed¹.

Copilots And Data Protection



Copilot For Microsoft 365



- A paid subscription to Copilot also integrates with Microsoft 365, where you can use it to do things such as:
 - Automatically respond to emails
 - Create PowerPoint presentations from Word documents
 - Summarize threads of email messages
 - Summarize Chat content from a thread of messages
 - Create transcripts of meetings
- Copilot became generally available as a subscription tool on 11/1/23 for companies with more than 300 Microsoft 365 users

Copilot Is Now Available For Most Business-Oriented 365 Subscribers



- **In January**, Microsoft announced the removal of the 300-license restriction!
- The cost of the paid subscription is **\$30 per month**, but you still **must have a qualifying Microsoft 365 subscription** (Microsoft 365 Business Standard, Business Premium, E3, E5, Office 365 E3, or E5)

Other AI Tools You Should Consider



- **Grammarly**, for improved writing
- **Originality**, to test for copyright infringement/plagiarism
- **Excel's Analyze Data and Insights in Power BI**, to identify "items of interest" in data sets
- **FORECAST.ETS** and **Forecast Sheets** in Excel
- **MindBridge** for fraud detection



LET'S GO INTO DEMO MODE...

Generative AI In Tax & Accounting



- So far, the examples presented have centered around “generic” searches, similar in some regards to those that could have been performed using search engines
- Now, let’s move forward into **using generative AI in tax and accounting scenarios**

Tax Return Engagement Letter



The engagement letter partially pictured to the right was created by prompting Gemini with the phrase “***Tax Return Engagement Letter for an S Corporation...***”

[Draft 1] [Draft 2] [Draft 3] [Clear]

Tax Return Engagement Letter Tax Return Engagement Letter for an S Corporation Tax Return Engagement Letter for an S Corporation

Client Name: [Address] [Client Name] [Date]

Tax Return Engagement Letter for an S Corporation

[Date]

[Client Name]
[Client Address]

Dear [Client Name],

This letter is to confirm and specify the terms of our engagement with you to prepare the federal and state income tax returns for [Year] for [S Corporation Name].

Services to be Provided

We will provide the following services:

- Prepare the federal and state income tax returns for [Year] for [S Corporation Name], based on the information and documentation you provide to us.
- Review the returns with you before you file them.
- Answer any questions you have about the returns or tax planning.

Working With ChatGPT



- In general, you will work in ChatGPT much like working with your favorite search engine
- That is, simply type in your request and ChatGPT will attempt to respond
- Once you type your request, you can modify or append it
 - For example, to include more details or to change the format from simple text to a bullet-point memo



Working With ChatGPT



- Should you decide to upgrade to **ChatGPT Plus**, the monthly subscription fee is \$20
- **With the Plus subscription, you will have access to GPT-4, priority access to new features, and faster response times**
- You can also browse, create, and use other GPTs
- **Further, you will have access to DALL-E, browsing, and Advanced Data Analysis**
- For \$5/user more (\$25 billed annually), Team lets you share your workspace, provides unlimited access, data is excluded from training, and has an admin console
- Finally, there is also an Enterprise version, known as **ChatGPT Enterprise**

Working With ChatGPT



- One very important option to configure in ChatGPT is **Custom instructions**
- To configure this option, **click the ellipses next to your name**
- Then **click Custom Instructions and tell ChatGPT a little about yourself**

Custom instructions ⓘ

What would you like ChatGPT to know about you to provide better responses?

I live in Woodstock, Georgia, a suburb of Atlanta.
I am a Certified Public Accountant.
I enjoy spectator sports, including Auburn University football. I also enjoy snow skiing, salt-water fishing, and spending time at the beach.

229/1500

How would you like ChatGPT to respond?

Call me Tommy.
ChatGPT should remain neutral in responses.
Responses should contain moderate degrees of detail and should be relatively formal.

144/1500

Enable for new chats

Cancel Save

ChatGPT And Custom Instructions



- Consider the response below received from ChatGPT after the Custom Instructions shown in the previous slide were entered into the system



data security issues and artificial intelligence

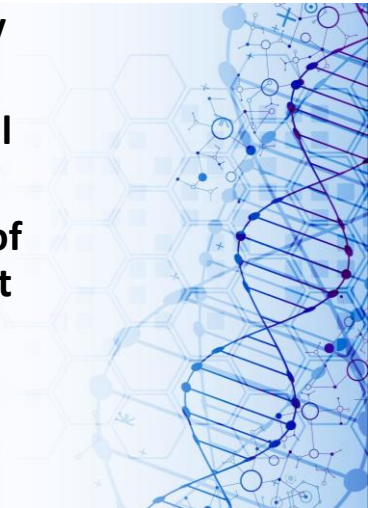


Certainly, **Tommy**. The intersection of data security and artificial intelligence (AI) is a topic of considerable importance. As a **Certified Public Accountant**, you likely appreciate the significance of safeguarding sensitive information, especially in the context of evolving technologies like AI.

Working With Gemini



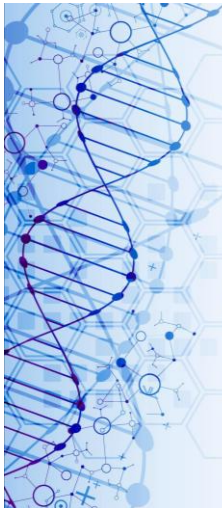
- In general, **working with Gemini will closely resemble working with ChatGPT**
- Again, **type in your request, and Gemini will respond** accordingly
- **Gemini uses an updated data set, capable of generating responses based on more recent data than ChatGPT 3.5**



Working With Gemini



- Remember, there is a free plan for Gemini and there is also a paid subscription available
- When working with Gemini, **pay attention to the icons near the upper, right corner of your browser's window**
 - There you can **view a history of your queries, integrate with Google apps, access help and FAQs, view update history, and manage settings**



Tax Return Engagement Letter

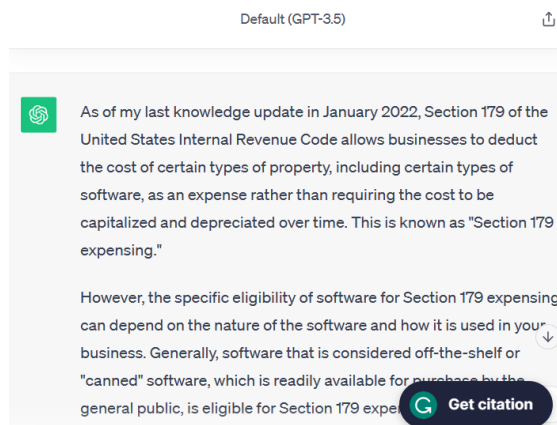


- Of course, you could simply **paste the text into your word processing application** and edit it to meet your specific needs
- Additionally, **note that Gemini provided three different versions of the engagement letter** and you could choose which version you want to use as your template

Tax Research



Like the previous example, you could enter the phrase “**does computer software qualify for Section 179 expensing**” into ChatGPT (3.5) and receive the response indicated to the right



Tax Research



- **What if you need more details** in the responses you receive from your query?
 - **Tell your AI tool to provide that level of detail to you!**
- For example, consider the following prompt entered into Gemini
 - ***I'm researching the impact the Secure Act 2.0 has on 401(k) plans. In a bullet point list, provide the most relevant verbatim excerpts from the document, with a citation at the end of each quote to the exact section to find the excerpt in the results***

Tax Research Results *(generated by Gemini)*

Impact of the Secure Act 2.0 on 401(k) plans:



- **Automatic enrollment for new plans:** Beginning in 2025, all new 401(k) and 403(b) plans will be required to automatically enroll eligible employees at a default contribution rate of between 3% and 10% of their compensation. The default rate will increase by 1% each year until it reaches at least 10%, but not more than 15% of compensation. Employees will have the option to opt out of automatic enrollment. (SECURE Act 2.0, Section 101)
- **Expanded participation for part-time workers:** Beginning in 2025, employers will be required to allow long-term, part-time workers to participate in their 401(k) plans. A long-term, part-time worker is defined as an employee who has worked at least 500 hours per year for three consecutive years. (SECURE Act 2.0, Section 102)
- **Increased age for required minimum distributions (RMDs):** The age at which participants must begin taking RMDs from their 401(k) plans has been increased from 72 to 73, effective for plan years beginning after December 31, 2022. The age will increase to 75 for plan years beginning after December 31, 2032. (SECURE Act 2.0, Section 103)
- **Reduced penalty for failing to take RMDs:** The penalty for failing to take an RMD has been reduced from 50% to 25% of the RMD amount. This penalty applies to RMDs that are not taken in a timely manner, but it does not apply to RMDs that are missed altogether. (SECURE Act 2.0, Section 104)

Responding To IRS Notices



- Another useful application of generative AI tools such as ChatGPT and Gemini is their capability to **create drafts of responses to tax notices and other correspondence**
- For example, consider an IRS CP-12 notice, indicating the taxpayer owes \$1,000 and you believe the IRS is in error
- You could enter the phrase ***“Respond to IRS CP-12 where John Jones owes \$1,000 and disagrees with the IRS”***

Creating Responses To IRS Notices *(generated by ChatGPT)*



accurately. Here are some general steps you may consider taking:

- 1. Review the Notice:**
Carefully go through the CP-12 notice to understand the specific details of the IRS's claim. Verify the tax period and the nature of the adjustment.
- 2. Gather Documentation:**
Collect all relevant documentation, including tax returns, receipts, and any supporting documents that can substantiate John Jones's position. This will be essential in building a case against the IRS's claim.
- 3. Contact the IRS:**
Reach out to the IRS using the contact information provided on the CP-12 notice. Explain the reasons for the disagreement and provide supporting documentation. It's advisable to remain calm and professional during any communication with the IRS.
- 4. Certified Mail:**
If you choose to send additional information or documentation, consider using certified mail with return receipt requested. This will provide proof of both the sending and receiving of your documents.
- 5. Request an Appeals Conference:**
If the disagreement persists, John Jones may have the option to request an appeals conference. This involves presenting the case to an independent IRS officer who will review the matter impartially.
- 6. Seek Professional Assistance:**
As a Certified Public Accountant, you might want to consider leveraging your expertise or

Creating Responses To IRS Notices



- Although the guidance provided in the previous slide might be helpful, particularly to less-experienced staff, you may have been hopeful of getting a draft of the **actual response letter** created by your AI tools
- Modifying your request to *“Create a response letter to IRS CP-12 where John Jones owes \$1,000 and disagrees with the IRS”* generates the draft response indicated on the next slide

Creating Responses To IRS Notices *(generated by ChatGPT)*



I hope this letter finds you well. I am writing in response to CP-12, which indicates that John Jones owes \$1,000, a claim he disputes.

Upon reviewing the notice, we respectfully disagree with the proposed adjustment. We have conducted a thorough examination of the relevant tax period and have gathered supporting documentation to substantiate our position.

Enclosed, please find copies of the tax returns, receipts, and any other pertinent documents that support our claim. We believe that these materials will provide clarity on the matters in question. We request that you review this information in reconsidering the proposed adjustment.

If necessary, I am open to further discussions or meetings to discuss this matter in detail. Additionally, I would appreciate guidance on any specific procedures or documentation required to facilitate a resolution.

Please be advised that we have also retained copies of this correspondence for our records.

Thank you for your prompt attention to this matter. We look forward to resolving this issue amicably.

Sincerely,

[Your Full Name]

Are There Dangers With AI? *Absolutely!*



Biased
Outputs

Copyright
infringement

Data privacy

Data security

Deepfakes

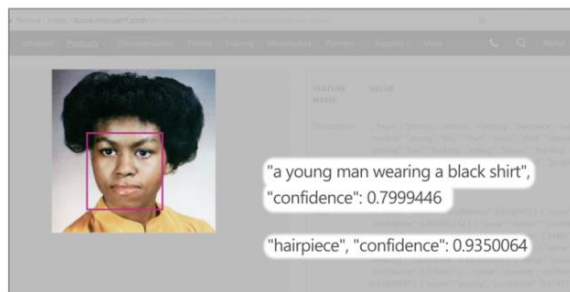
Hallucinations

Biased Outputs



- AI systems can be biased either **intentionally** or **unintentionally**
- Bias can exist around all factors, including personal ones such as race, gender, and age
- For example, consider the case of **Michelle Obama**

Michelle Obama



Copyright Infringement



Who owns the copyright to materials generated by AI?

Response, Per ChatGPT

Generally, the entity or individual that creates the AI-generated content is considered the copyright owner. However, this may vary based on jurisdiction and specific contractual agreements.

Response, Per Gemini

In the United States, the Copyright Office has stated that it will not register works that were created by an autonomous AI tool. This means that, under current US law, AI-generated works are either in the public domain or they are derivative works of the materials that the AI was trained on.

Copyright Infringement



New York Times Has Sued MSFT & OpenAI!

- In December, NYT sued Microsoft and ChatGPT's parent company, OpenAI
- The Times alleges *"mass copyright infringement"*
- The Times continues with *"These tools were built with and continue to use independent journalism and content that is only available because we and our peers reported, edited, and fact-checked it at high cost and with considerable expertise"*
- One example provided by the Times OpenAI's software producing almost identical text to a Times article about predatory lending practices in New York City's taxi industry

Data Privacy



- Consider the type of data you might “feed” into an AI tool or platform. How comfortable are you that sensitive data remains private and not identifiable back to an individual or an organization?
- Other issues include
 - Is there informed consent about collection and use
 - The threat of exposing sensitive data through a breach or attack
 - Lack of transparency regarding use of an individual’s or organization’s data

Data Security



- Like other large caches of data, the **data stored in AI tools and platforms can present an inviting target because of the private nature of the data**
- Additionally, a general lack of human oversight can increase the vulnerability of the data
- Moreover, **the complexity of AI systems presents challenges concerning storing and protecting sensitive data**
- In fact, as reported on 11/10/23, Microsoft temporarily blocked team members from using ChatGPT due to security concerns

Deepfakes



- **Deepfakes involve using AI to generate realistic images, audios, and videos so that they appear to represent an authentic person engaging** in some activity in which the person did not engage
- For example, a deepfake exists that appears to show Mark Zuckerberg bragging that he has control of data stolen from billions of people
- You can see some outstanding – and scary! – examples of deepfakes on YouTube at <https://k2e.fyi/deepfakes>

Hallucinations



- Like humans, **AI is not perfect!**
- Sometimes, AI “hallucinates” and generates a faulty response that seemingly does not represent the data
- Often, **these hallucinations are based on anomalies in the AI model or issues associated with training the model**
- As an example, **Gemini incorrectly asserted in February 2023 that the Webb Space Telescope took the first image of a planet outside the solar system...in fact, the pictures of an exoplanet were taken in 2004**

Risks and Security



Hallucinations



Hackers



Sycophant



Prompt Injection



Human



Disruption



Shadow

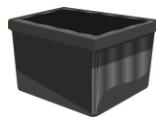


Scheming

Risks and Security



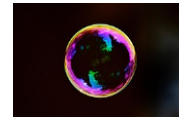
Deepfakes



Black Box



Environment



Bubble



Entry Level



Privacy



Lazy



Slop

Risks and Security



Leakage



Poisoning



Washing



Excessive
Agency



Weapons



Tool Spread

Summary



- Generative AI is truly a **game-changer for virtually everyone!**
- Consider the impact of generative AI tools such as **Claude**, **ChatGPT**, **Gemini**, and **Copilot** on how you work
 - How can you use these tools for improved efficiency and productivity?
 - How can these tools help to free team members from mundane tasks?
 - What are some potential negative impacts of implementing generative AI tools?
- No doubt, AI has come a long way in just three short years...
imagine what AI will be ten years from now!