



K2's AI Confidential

Privacy And Artificial Intelligence

Tommy Stephens



CPA from Woodstock, Georgia

Member, K2 Enterprises


Thirty-eight years of public accounting & private industry experience including twenty-eight years as a CPE discussion leader


BSBA (Accounting), Auburn University and MS (Finance), Georgia State University


Please contact me via email at tommy@k2e.com or Twitter [@TommyStephens](https://twitter.com/TommyStephens)


Overview




 Software licenses and privacy policies

 Artificial intelligence laws and regulations

 Key terms from NIST

 Language models

 AI Risk management

Learning Objectives



Identify at least one tool which helps users to organize and identify key sections of license agreements

Select the correct definition for key terms used in license agreements and privacy policies

Explain how to identify key sections in license agreements, including how to "opt out" of features which may compromise your privacy

Are There Dangers With AI? ***Absolutely!***



Biased
Outputs

Copyright
infringement

Data privacy

Data security

Deepfakes

Hallucinations

Are There Dangers With AI? *Absolutely!*



Biased
Outputs

Copyright
infringement

Data privacy

Data security

Deepfakes

Hallucinations

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



SOFTWARE LICENSES AND PRIVACY POLICIES

What Is Software Licensing?



- Intellectual property rights have always been a problem in the most advanced societies of the world
 - Criminal prosecution of property crimes seems to have dropped off
 - Civil recovery seems to be more popular, with fees/fines and/or asset forfeiture
- Software piracy is protected under copyright in the US and Canada and provides severe civil and criminal penalties for those who use software for which they do not possess the rights to do so or use the software in ways that violate a licensing agreement
- Further, with the advent of data as a marketable product, security risks and privacy risks have increased exponentially

Now, Add AI Into The Mix



- Making a challenging subject even more so, now consider the impact of Artificial Intelligence (AI) when added to the mix
- Could creating a prompt asking for tax advice expose your personal data or that of a client?
- Could uploading financial data for a privately-held company to an AI platform cause that data to leak?
- Can we trust what the AI companies are telling us about data security and privacy?

About Software Licensing



Software licensing is like airfare pricing in many ways:

- Its objective is to make it possible for the company/seller to maximize its revenue by segmenting its customers
- There are special deals for big customers which are not available to small customers
- The terms of what is allowed for each product segment vary depending on what you bought, how much you paid, and the sales needs of the licensor

Why Software Licenses Are Critical



- To better understand the risks associated with privacy and AI, we need to **READ** and **UNDERSTAND** the major documents associated with the application
- Two of the key documents associated with your rights/license to use software or cloud-based services include:
 - **End User License Agreement (EULA) / Terms of Service (ToS)**
 - **Privacy Policy**
- There are also common contract terms that need to be understood, particularly as you are using third-party hardware, software, and AI models to process confidential information

A Note About Software Licensing



- There are numerous bundles and SKU's which change frequently
- Even the “experts” struggle to explain the logic underlying the pricing strategies
- Every software company writes its own contracts, terms of service, and privacy policies and license conditions
- We will focus on three basic documents/contracts related to your contractual licensing of software:
 - End User License Agreement
 - Terms of Service
 - Privacy Policy

End User License Agreement (EULA) / Terms of Service (ToS)



- Document which states the terms which govern your use of an application or service
- Let software companies define the terms for the use of their software or service in a way which is favorable to their business
- Are often accepted without ever reading them at all
- May incorporate other documents, policies, and terms by reference

Word Count/Complexity of EULAs

- Intuit QuickBooks Online
 - 57,053 words
 - Flesch-Kincaid grade 14.6
- QB Desktop US
 - 24,619 words
 - Flesch-Kincaid grade 14.1
- Xero
 - 5,332 words
 - Flesch-Kincaid Grade 11.8

Many EULAs are long, complex, difficult to understand, and often disclose as few specifics as possible about any practices which might be a concern to end users

Privacy Policy



- Document which discusses a company's privacy policy, including data like:
 - What data is gathered from you
 - How your information will be used
 - The purpose of gathering that data and how your data may be used
 - When your data will be disclosed others, including sensitive personal data and information
 - Not always specific on with whom it will be shared
 - Security policies and procedures

Word Count - Privacy Policies

- Intuit 12,221
- Xero 2,671
- ADP
 - General 13,288
 - Glossary 2,685
 - For client employees 912
- Yodlee Investnet
 - 5,971 words
 - Flesch-Kincaid grade 14.4

Privacy Policy Extracts - Intuit



- Your Content remains yours, which means that you retain any intellectual property rights that you have in your Content. By sharing your Content on the Platform, **you hereby grant Intuit a license to use your Content**, as described in more detail below.
 1. **What's covered** - This license covers your Content to the extent your Content is protected by intellectual property rights.

Privacy Policy Extracts - Intuit



2. Scope - This license is:

- **Worldwide**, which means it's valid anywhere in the world;
- **Non-exclusive**, which means you can license your Content to others; and
- **Royalty-free**, which means there are no fees for this license

Privacy Policy Extracts - Intuit



3. Rights - This license allows Intuit to:

- **Host, reproduce, distribute, communicate, sublicense and use your Content** — for example, to save your Content on our systems and make it accessible from anywhere you go;
- **Publish or publicly display your Content, if you've made it visible to others**; and
- **Modify and create derivative works based on your Content**, such as reformatting or translating it

ADP's AI Ethics Statement



ADP's privacy statements include an [AI ethics statement](#), which explains things like:

- The organization's approach to AI,
- Where AI is used in its products,
- Data quality processes,
- Principles which are followed when using AI, including "privacy-by-design",
- How AI models are evaluated,
- How AI is governed, and more – see it [on ADP's website](#)

ADP's AI Ethics Principles

- 1. Human oversight*
- 2. Governance*
- 3. Privacy-by-design*
- 4. Explainability & transparency*
- 5. Data quality*
- 6. Culture of responsible AI*
- 7. Inclusion and training*

Acceptable Use Policy



- Just as the EULA/ToS, and privacy policy spell out the rights and responsibilities of both parties in a relationship between an end user and a software company, an Acceptable Use Policy (AUP) governs the acceptable use of the organization's technology hardware, software, and data by its employees and contractors
- While acceptable use policies are not required by law, they help both employees and companies properly set expectations about how these tools will be used (and how they will NOT be used) so all parties know their rights and responsibilities

Acceptable Use Policy Addresses



Ownership and general use of technology

Security and handling confidential information

Types of unacceptable use of systems

E-mail and communication guidelines

Blogging and social media

Consequences for violation of these policies



AI LAWS AND REGULATIONS

AI Laws And Regulations



- EU – Artificial Intelligence Act
- US Executive Order 14110 - Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (10/30/2023)
- [US AI Safety Institute](#), established in early 2024 as part of National Institute of Standards and Technology (NIST)/US Dept of Commerce
- NIST AI Risk Management Framework (NIST AI 100.1) (January 2023)
- US General Accounting Office – “Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities” (June 2021)
- National Artificial Intelligence Initiative Act of 2020 (P.L. 116-283)

EU Artificial Intelligence Act



- EU – Artificial Intelligence Act was passed in 2021 by the EU in response to the advent of generative AI systems like ChatGPT
- Classifies applications into four categories (“unacceptable”, “high”, “limited”, and “minimal”) based on their risk to cause harm, plus an additional category for general-purpose AI
 - Unacceptable risks in apps are banned
 - High risk apps must comply with more rigorous requirements for security, transparency, and quality, and must have conformity assessments
 - Limited risk apps only have transparency obligations
 - Minimal risk apps are unregulated
 - General purpose AI have transparency requirements and must be evaluated when risks are above the “limited” level

Executive Order 14110



- “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence” ([text](#) – 47 pages) ([WH summary](#))
- Signed by President Biden on October 30, 2023
- Significant resources are available online at [AI.gov](#)
- Creates an Office of AI within NIST/Office of Science and Tech Policy
- Proposes that **DoD, Energy, and HHS create regulations related to AI models that might pose a serious risk to national security, critical infrastructure, or public health and safety**
 - Energy and Homeland Security are involved with this due to their charge to mitigate risks related to nuclear and biological weapons
 - AI models must be evaluated by the government and must share the results of red team safety tests

Executive Order 14110



- There are some privacy provisions, but the order is well short of a comprehensive privacy policy/statute like the [Canadian Privacy Act](#) or the EU’s General Data Protection Regulation (GDPR)
 - Reviews data brokers and how commercially available data is used, and will recommend privacy guidance
 - Develop guidelines for federal agencies to evaluate the effectiveness of privacy-preserving techniques
- The **Commerce Department is charged with creating best practices for detecting deepfakes such as text, images, and sounds which are not distinguishable from real text, images, or recordings**
- Increase the ability for those with AI skills to stay in the US

Executive Order 14110

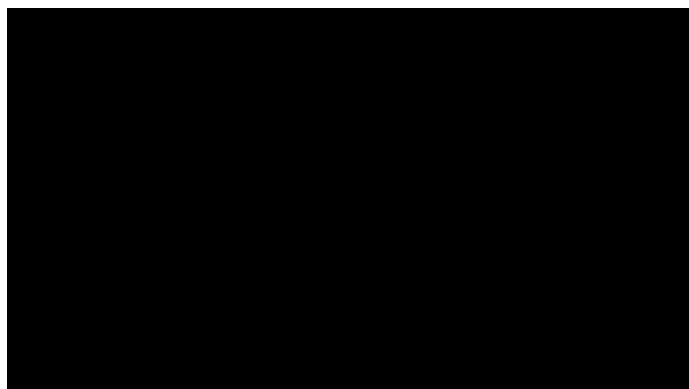


- Create cybersecurity program to develop AI tools to find and fix vulnerabilities in critical infrastructure
- Increases government investment in AI and government use of AI
- Actions to provide guidance to landlords, federal benefit programs, and federal contractors to avoid algorithmic discrimination, and provide best practices in the criminal justice system
- Safety program to remedy harms and unsafe healthcare practices using AI
- Transform education by creating resources to support educators with AI-enabled education tools
- Create best practices to maximize benefits of AI for workers
- Increase global collaboration surrounding AI

NIST Trustworthy & Responsible AI Resource Center



- Available online at <https://airc.nist.gov>
- Resources include
 - NIST AI Risk Management Framework ([AIRMF](#))
 - AIRMF [Playbook](#) and [glossary](#)
 - AIRMF [Roadmap](#)
 - [Crosswalks](#) to various standards and frameworks



Get an introduction to the RMF by [watching the video](#) at NIST

NIST AI Risk Management Framework

- Issued in January 2023 by National Institutes of Standards and Technology (NIST), the US Federal Government Agency which creates technology, privacy, and security standards for all government departments and agencies
- Currently voluntary, not mandatory, this could change in the next twelve to eighteen months

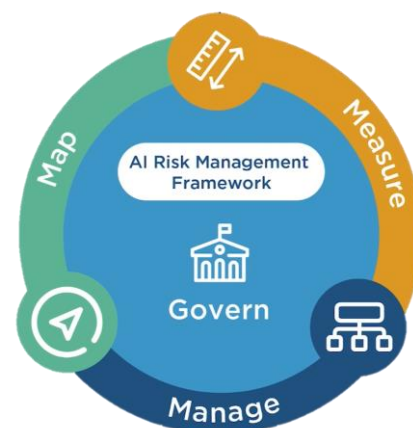


Artificial Intelligence Risk Management Framework (AI RMF 1.0)

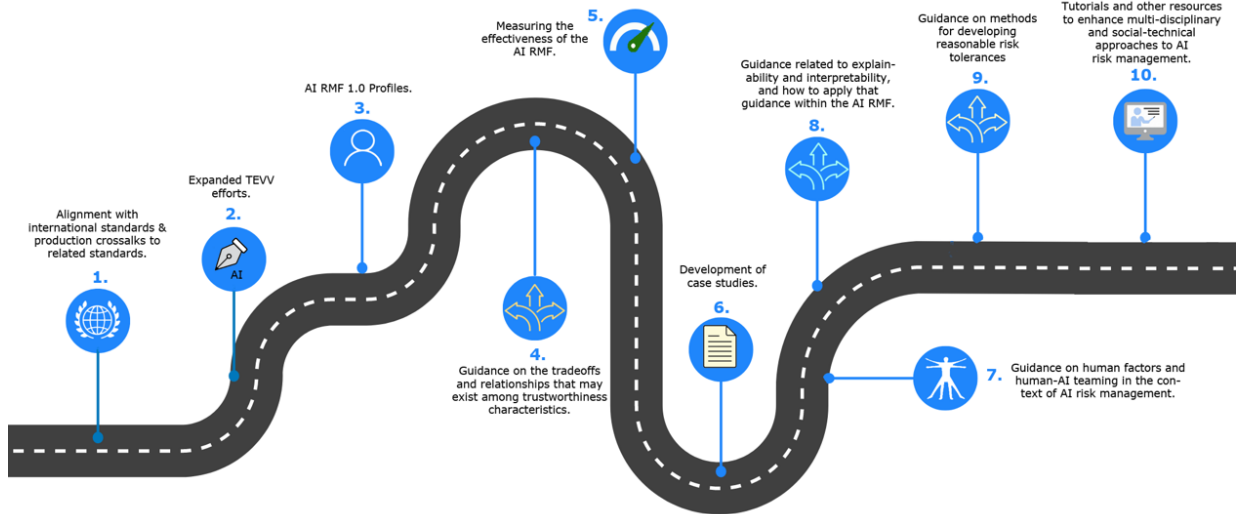
This publication is available free of charge from:
<https://doi.org/10.6028/NIST.AI.100-1>

NIST AI Risk Management Framework

- It seeks to **incorporate trustworthiness considerations** into the design, development, use, and evaluation of AI products, services, and systems.
- Four major components
 - **Govern:** Establishing governance structures and policies for AI risk management.
 - **Map:** Identifying and assessing AI-related risks.
 - **Measure:** Quantifying and evaluating risks.
 - **Manage:** Implementing risk mitigation strategies.

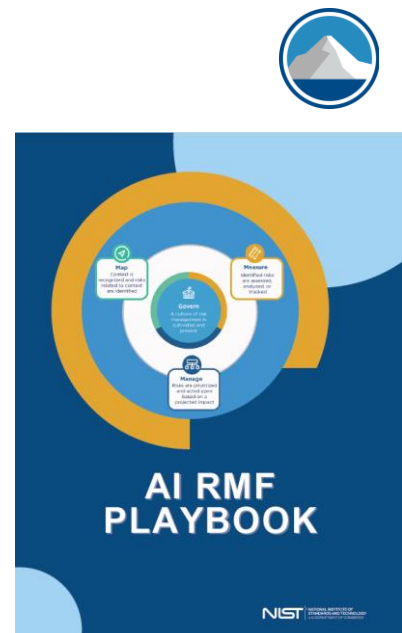


NIST AI Risk Management Framework Roadmap



NIST AI Risk Management Framework Playbook

- A set of practice aids called the “AI Risk Management Playbook” which provides voluntary suggestions for documenting, identifying, and mitigating risk
 - **IMPORTANT** – This document contains voluntary suggestions and agencies are NOT currently required by NIST to use this tool (as of 3/2024)
- The free tools offer assistance with governance, mapping of risks, risk measurement, and risk management
- Like risk management frameworks from COSO, ISACA (COBIT), and others



Potential Harms From AI Systems



Source: "Artificial Intelligence Risk Management Framework" (AI 100.1) by US National Institutes for Standards and Technology (NIST)



SO, WHAT ARE THE AI COMPANIES SAYING?

ChatGPT Concerns



- OpenAI (ChatGPT's parent company) collects:
 - IP address, location, browser type, date/time, length of session, device name, and operating system
 - Uses cookies to track browsing activities both in chat window and site
 - Records complete transcripts of your prompts and conversations
 - ChatGPT reserves the right record any data you upload, such as an Excel file or a set of financial statements
- To enhance security and privacy, consider opting out of model improvement and deleting chat history

Gemini Concerns



- Google publicly stated that Gemini collects the following information about your use of Gemini
 - Conversations, locations, feedback, and usage info
- Regarding who has access to your Gemini conversations, Google says the following: *We take your privacy seriously, and we do not sell your personal information to anyone. To help Gemini improve while protecting your privacy, we select a subset of conversations and use automated tools to help remove user-identifying information (such as email addresses and phone numbers).*

Gemini Concerns



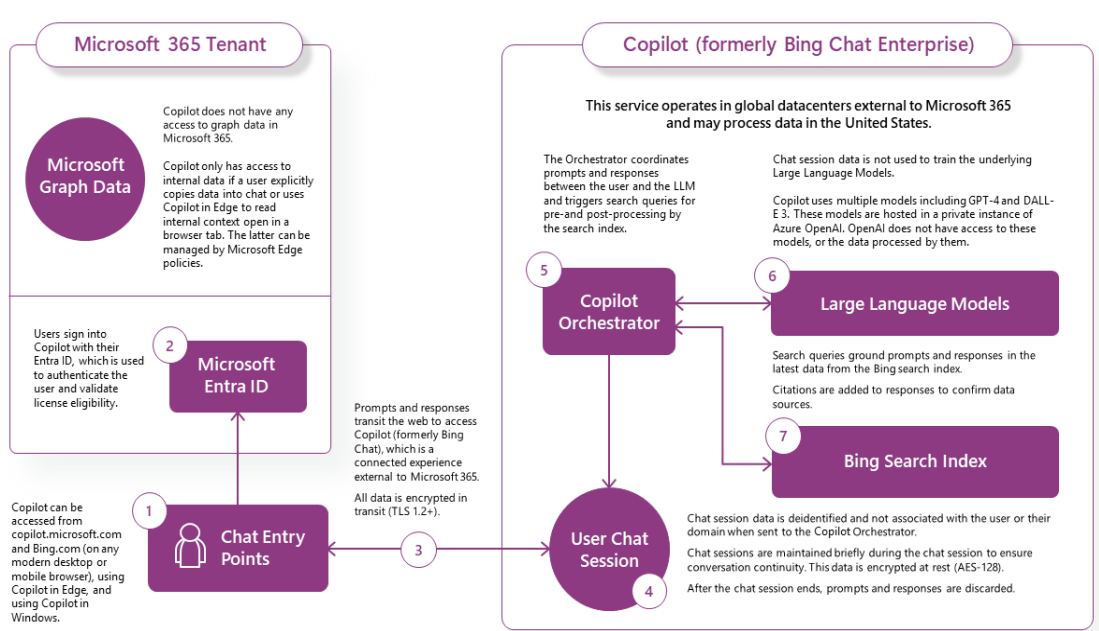
- Google goes on to state: *Please don't enter confidential information in your conversations or any data you wouldn't want a reviewer to see or Google to use to improve our products, services, and machine-learning technologies.*
- *Gemini Apps conversations that have been reviewed by human reviewers are not deleted when you delete your Gemini Apps activity because they are kept separately and are not connected to your Google Account. Instead, they are retained for up to three years.*

Microsoft's AI Copilots



Name	Products	Monthly Cost	Commercial Data Protection Included?
Copilot for MS 365 (Business/Enterprise)	Microsoft 365 apps (Word, Excel, PowerPoint, Outlook, Teams)	\$30 per user	Yes
Copilot in Windows (Bing Chat)	Windows OS	Free	Not for home users, included with most business/enterprise O365/M365 plans
Copilot Pro for Individuals	Advanced features on top of standard Copilot, plus integration with home Microsoft 365 apps	\$20/user/mo.	Not specified
Copilot for Security	Microsoft's cybersecurity products	Consumption-based fee - \$4/hour	Not specified
Copilot for Finance, Sales, and Service	Financial operations, sales optimizations, service enhancements	\$50/user/mo., \$20/user/mo. if already have MS 365	Not available to other customers, runs on Microsoft cloud in separate instance of ChatGPT, not used by MS to train models by default
Designer for Copilot	Image creation and editing	Not available	No
Copilot GPTs and Azure AI Studio	Custom generative AI assistants and solutions	Not specified	Not specified

Copilots and Data Protection



So, What Should I Do Now?



- Proactively managing the security and privacy settings in you're the AI platforms that you use
- Never enter or upload private or sensitive data into your generative AI prompts
 - Scrub names, SSN's, account numbers, etc. from your data before uploading it to a generative AI tool
- Train your team members on how to use these tools safely and securely...remember the survival of your business may depend upon it!

Evaluating Generative AI Risks



Three of the AI risks to consider include:

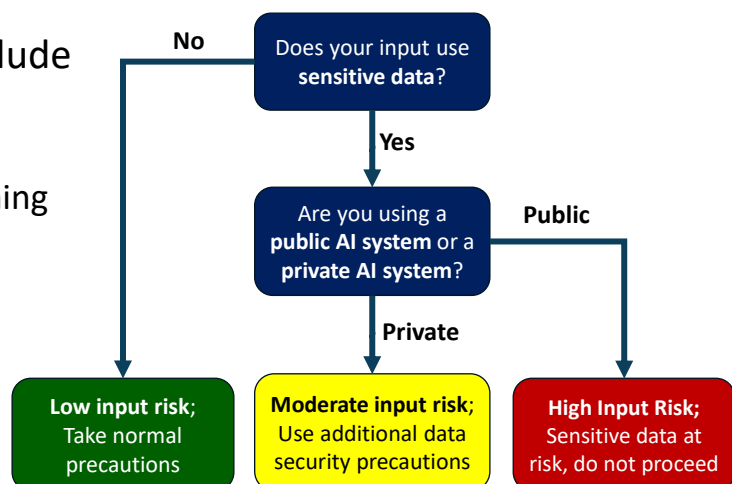
- **Input risks** – The risks associated with inputting your proprietary data into an AI system and that data becoming compromised resulting in unauthorized disclosure of confidential information
- **Output risks** – The risks that the outputs from the AI model will be low quality, inaccurate, or incomplete and the models lose their integrity based on including an unacceptable number of erroneous data points
- **System risks** – Risks associated with the servers hosting the AI system being compromised and the data model needs to be recovered from backups

Gen AI Input Risk Decision Tree



• Types of input attacks include attempts to:

- Crash AI model
- Exfiltrate memorized training data



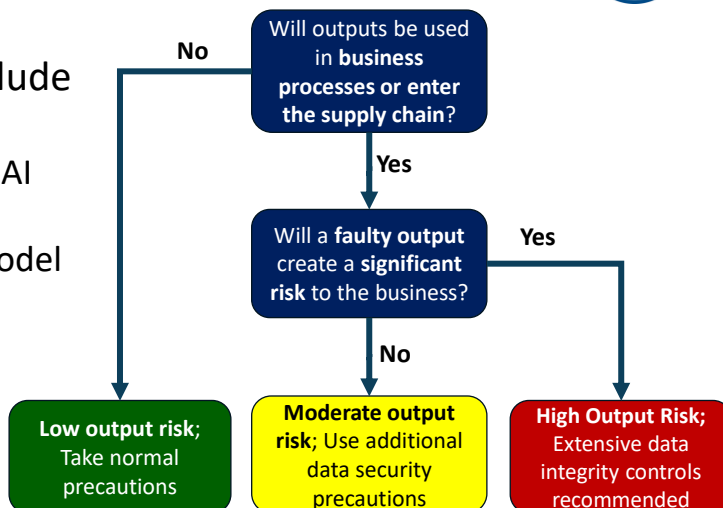
Source: "Address Security & Privacy Risks for Generative AI" by InfoTech Research Group

Gen AI Output Risk Decision Tree



Types of output attacks include attempts to:

- Data poisoning to corrupt AI output
- Weaponization of an AI model
- Sponging to slow down processing speed of AI model

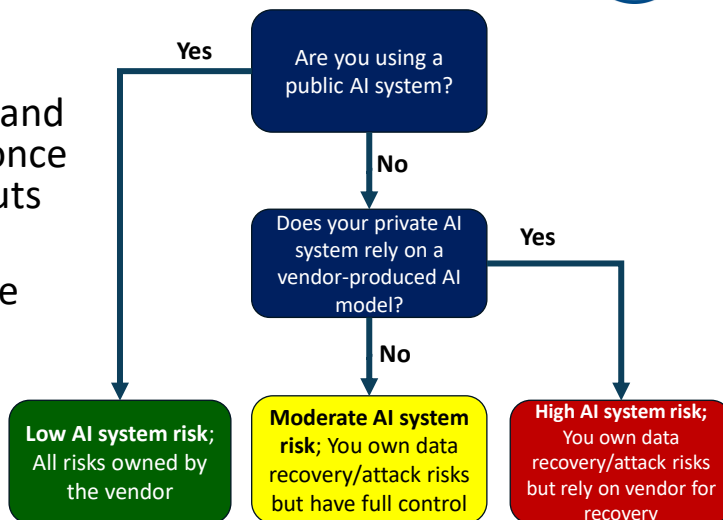


Source: "Address Security & Privacy Risks for Generative AI" by InfoTech Research Group

Gen AI System Risk Decision Tree



- Public AI systems like ChatGPT, Google Gemini, and Bing chat are developed once and trained based on inputs from many users
- Private AI systems must be trained, managed, and maintained by employees using internal organization resources



Source: "Address Security & Privacy Risks for Generative AI" by InfoTech Research Group



Questions?

THE END



Summary And Wrap Up

- Generative AI tools such as ChatGPT, Gemini, and Copilot have taken the world by storm...and for good reason!
- These tools offer incredible productivity gains
- However, there are potential security and privacy dark sides associated with these platforms
- Ensure you and your team are aware of these risks and take appropriate steps to mitigate them before embarking on your AI journey to reduce the risk of compromising sensitive data!