

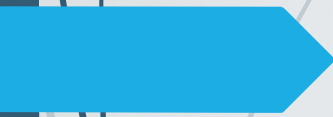


# Using AI to Conduct Audit Work

Emil Tzanov, CIA, CFA



Prompt: Who is better at performing IT audits, ChatGPT or the average IT auditor?



Polling Question #1

What do you think ChatGPT answered in response to the prompt:  
“Who is better at performing IT audits, ChatGPT or the average IT auditor?”

Prompt: Who is better at performing IT audits, ChatGPT or the average IT auditor?

ChatGPT: That's a fun question! Here's a lighthearted take:

"ChatGPT is great at analyzing tons of data and spotting patterns in seconds, but the average IT auditor wins when it comes to navigating office politics, asking just the right follow-up question, and remembering to grab coffee before a long meeting. So, maybe they make the perfect audit team!"

Would you like me to dive deeper into how generative AI can complement an IT auditor's work?



# Learning Objectives

- Understand what Artificial Intelligence (“AI”) is and is not
- Learn to differentiate between various AI tools
- Explore various applications of AI within the Internal Audit Process
- Discuss the regulatory, ethical, privacy, and other issues related to the adoption and use of AI within Internal Audit



# Artificial Intelligence – Basic Anatomy



# What is Artificial Intelligence - Definitions

- Artificial Intelligence (AI) Term first used by John McCarthy in 1956:  
**“the science and engineering of making intelligent machines”**
- “AI is a branch of computer science that uses advanced analytical and statistical methods, such as machine learning and artificial neural networks, to simulate intelligent behavior in computers. AI can perform tasks that typically require human intelligence, such as speech recognition, visual perception, decision-making, and language translation “
- “The capacity of machines to mimic human cognitive functions such as learning, problem-solving, and pattern recognition, enabling them to perform tasks that normally require human intelligence. It includes various subfields, such as machine learning and natural language processing. “



# What may be confused for AI

- ▶ Rule-Based Systems (Expert Systems): These programs follow predefined rules set by humans to solve problems. They don't "learn" or adapt, but simply apply logic to a situation, like a tax preparation software following tax rules, or early generations chess playing apps. People sometimes mistake them for AI because they perform tasks that seem intelligent, *but they lack the ability to learn or improve without human input.*
- ▶ Chatbots with Predefined Responses: Some chatbots, especially early or simpler versions, are built on a set of predetermined responses. They might give the illusion of intelligence, but they don't analyze or learn from conversations. Unlike true AI-based chatbots, *these can't adapt or improve based on user input.*
- ▶ Automation Scripts and Macros: These are just sets of instructions that automate repetitive tasks, such as filling in forms or moving data between applications. While they save time, they don't have the ability to "think", learn, or make decisions like AI.



# Types of AI

- ▶ Artificial narrow intelligence (ANI), which has a narrow range of abilities
  - ▶ Goal-oriented, designed to perform singular tasks - i.e. facial and speech recognition, driving a car, swarm intelligence - and is very good at completing the specific task it is programmed to do.
- ▶ Artificial general intelligence (AGI), which is on par with human capabilities
  - ▶ the concept (*not yet fully achieved*) of a machine with general intelligence that mimics human intelligence and behaviors, with the ability to learn and apply its intelligence to solve any problem. AGI can think, understand, and act in a way that is indistinguishable from that of a human in any given situation.
- ▶ Artificial superintelligence (ASI), which is more capable than a human
  - ▶ the *hypothetical* AI that doesn't just mimic or understand human intelligence and behavior; ASI is where machines become self-aware and surpass the capacity of human intelligence and ability.



# Large Language Models & Tools

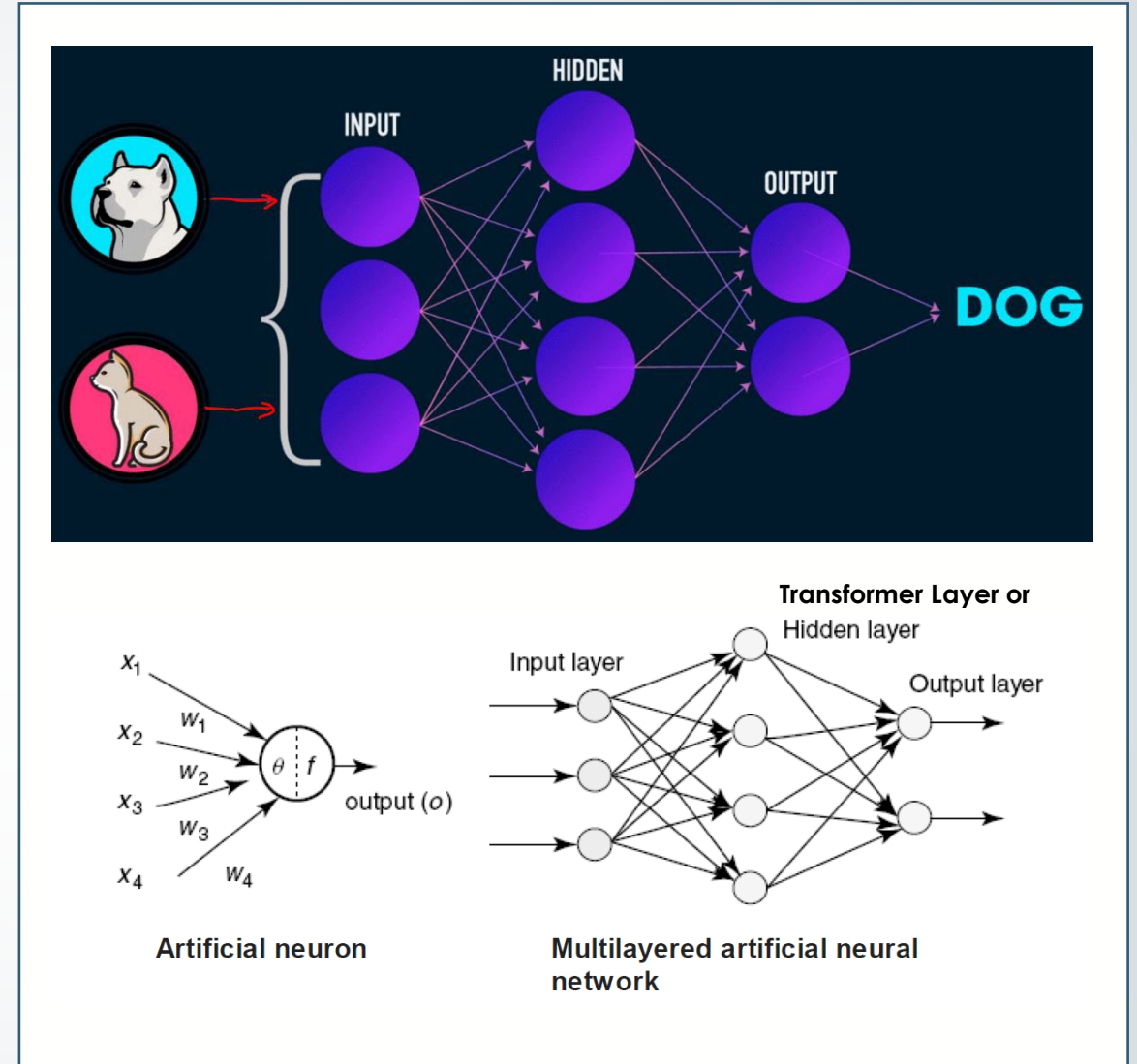
- ChatGPT – OpenAI
- Gemini - Google
- Claude – Anthropic
- Llama 3.1 – Meta

A large language model (LLM) is a type of artificial intelligence (AI) designed to process and generate human language. At its core, it is based on deep learning—a subset of machine learning—using neural networks with billions of parameters. These parameters allow the model to capture complex patterns, structures, and relationships in natural language.



# Artificial Neural Networks & Machine Learning

**Machine learning** is a process and field of science where computers learn from data to make predictions. **Deep learning** is a specific subset of machine learning that utilizes artificial neural networks with multiple layers to analyze complex data, often achieving better results on tasks like image recognition and natural language processing but requiring significantly more data and computational power; essentially, deep learning is a more advanced form of machine learning that mimics the structure of the human brain to learn from data.



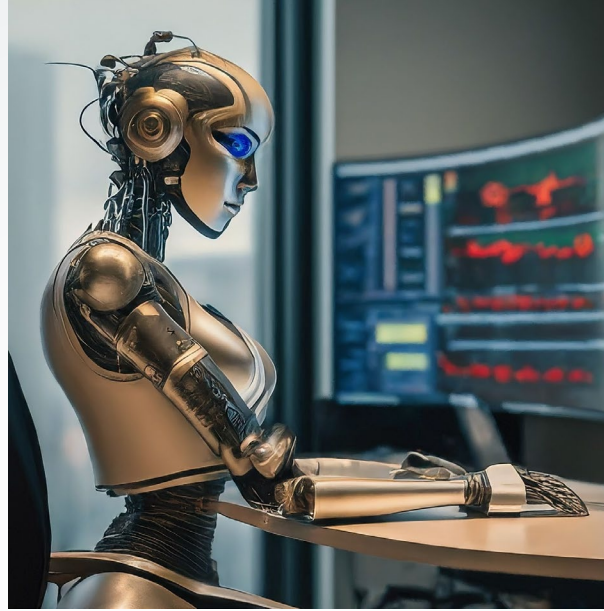


## Polling Question #2

What does “GPT” in “ChatGPT” stand for?

- a. Generally Pretends to Think
- b. Genuine Positive Thinker
- c. Great Personal Tester
- d. None of the above

# Applications of AI in Internal Audit



“Get on the AI train”

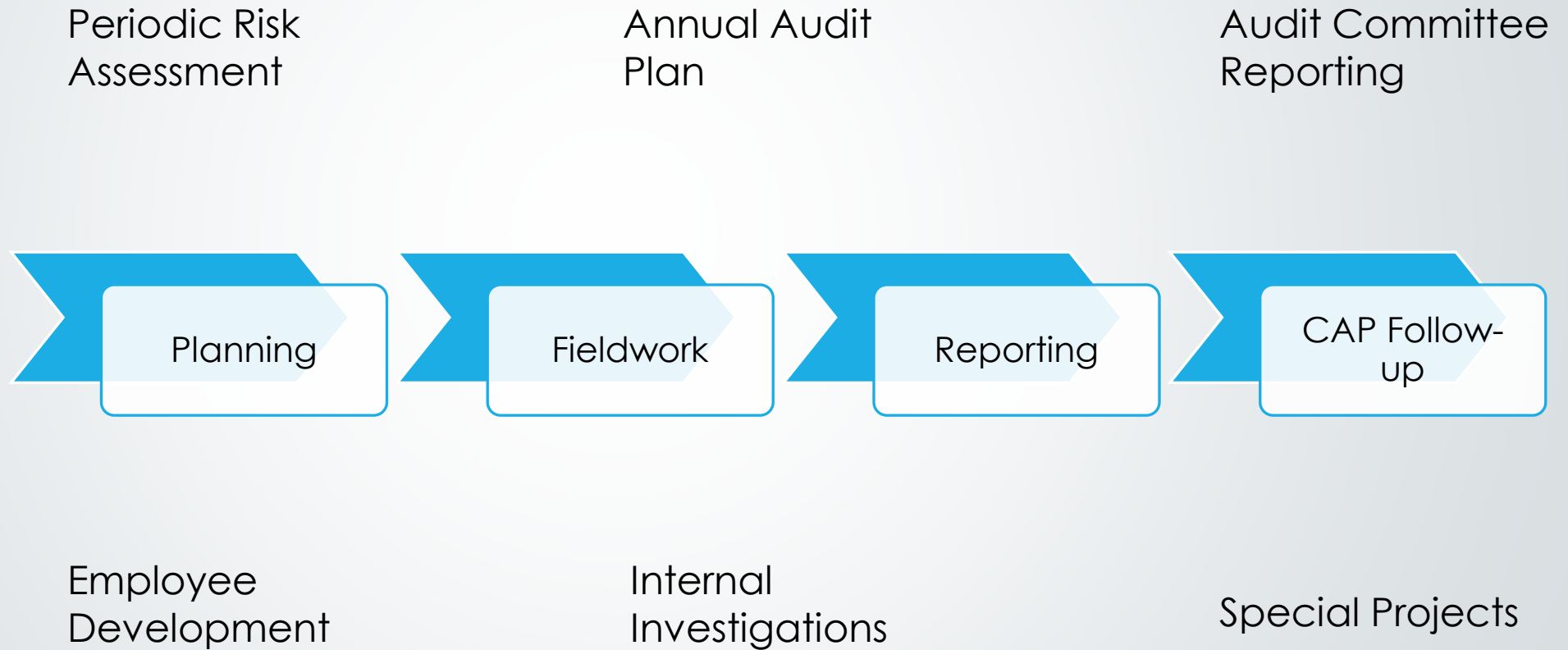


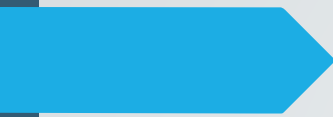
NYSE then: 5000 people / 1366 traders



NYSE now: 300 traders

# The Internal Audit Environment





# Prompt (1) for Chat GPT:

I am an internal auditor. I work for a city government. I need to perform an internal performance audit of the city water utility which supplies water to the citizens of my city. What are the top ten risks that my audit should focus on?

## ➔ Chat GPT:

When auditing a city water utility, it's crucial to focus on various risks that could affect the performance, efficiency, and effectiveness of the utility. Here are the top ten risks you should consider:

### 1. **Water Quality and Safety:**

- Risk of non-compliance with water quality standards, which could lead to public health issues.
- Potential for contamination due to aging infrastructure or inadequate treatment processes.

### 2. **Infrastructure Integrity:**

- Risks associated with the aging or deteriorating infrastructure, including pipelines, treatment plants, and storage facilities.
- Maintenance and repair backlogs that could lead to service disruptions.

### 3. **Financial Management:**

- Risks related to financial sustainability, including inadequate revenue collection, budget deficits, and inefficient use of funds.
- Potential for fraud, waste, or abuse in procurement and contracting.





#### 4. **Regulatory Compliance:**

- Non-compliance with local, state, or federal regulations, which could result in fines, legal action, or loss of public trust.
- Inadequate documentation or failure to meet reporting requirements.

#### 5. **Water Supply and Demand Management:**

- Risks of water shortages due to poor planning, climate change, or inadequate resource management.
- Inefficiencies in water distribution leading to high levels of water loss or unaccounted-for water.

#### 6. **Emergency Preparedness and Response:**

- Inadequate preparedness for emergencies such as natural disasters, infrastructure failures, or contamination incidents.
- Insufficient communication plans to inform the public during emergencies.

#### 7. **Customer Service and Satisfaction:**

- Risks associated with poor customer service, including billing inaccuracies, slow response to complaints, or lack of transparency.
- Potential for reputational damage if the utility is perceived as unresponsive or ineffective.



## 8. Cybersecurity and Data Management:

- Vulnerabilities in IT systems that could lead to data breaches, ransomware attacks, or disruptions in service.
- Inadequate protection of sensitive customer information and operational data.

## 9. Workforce Management:

- Risks related to staffing, including shortages of skilled personnel, high turnover, or inadequate training.
- Potential impacts on service delivery due to workforce issues.


## 10. Environmental Sustainability:

- Risks associated with non-sustainable practices, including over-extraction of water sources, energy inefficiency, or failure to implement conservation measures.
- Potential regulatory and reputational risks related to environmental impact.

Focusing on these risks will help ensure a comprehensive audit that can identify areas for improvement and strengthen the overall performance of the water utility.

## Risk #8 Drill Down





**Follow-up prompt :** Under risk number 8 above, list three important cybersecurity risks. Be specific.

► **Chat GPT:** Under the category of **Cybersecurity and Data Management**, here are three specific cybersecurity risks that should be closely examined:

**1. Vulnerability to Ransomware Attacks:**

- The water utility may be at risk of ransomware attacks that could encrypt critical data and disrupt operations. Such attacks could shut down water treatment facilities or compromise SCADA (Supervisory Control and Data Acquisition) systems, leading to significant service disruptions and requiring expensive recovery efforts.

**2. Insufficient Network Segmentation:**

- Inadequate network segmentation between IT and OT (Operational Technology) environments can expose critical infrastructure, such as water treatment and distribution systems, to cyber threats. A breach in the IT network could potentially allow attackers to access and manipulate OT systems, leading to unauthorized control over water treatment processes or distribution mechanisms.

**3. Inadequate Patch Management:**

- Failure to regularly update and patch software and systems can leave the utility vulnerable to known security vulnerabilities. Unpatched systems are prime targets for attackers who exploit these weaknesses to gain unauthorized access, disrupt operations, or steal sensitive information.

**Follow-up prompt:** Can a cyber attacker alter the chemistry of the city water? If yes, how can that occur:

➔ **Chat GPT:**

Yes, a cyber attacker can potentially alter the chemistry of the city water, especially if they gain unauthorized access to the utility's Operational Technology (OT) systems, such as SCADA (Supervisory Control and Data Acquisition) systems, which control the treatment and distribution of water.

➔ **How This Could Occur:**

**1. Access to SCADA Systems:**

- SCADA systems control critical processes in water treatment plants, including the addition of chemicals like chlorine, fluoride, and other treatment agents. If an attacker gains access to these systems through vulnerabilities (e.g., weak passwords, unpatched software, or phishing attacks), they could manipulate the chemical dosing processes.

**2. Manipulation of Chemical Injection Systems:**

- Once inside the SCADA system, an attacker could change the settings for chemical injection, increasing or decreasing the dosage

of chemicals used to treat the water. This could result in over-chlorination, making the water toxic, or under-chlorination, leading to insufficient disinfection and potentially allowing harmful pathogens to survive.

**3. Interruption of Monitoring and Alarm Systems:**

- Attackers could disable or alter monitoring and alarm systems designed to detect abnormal chemical levels or system malfunctions. Without these alerts, operators might not be aware of the changes until after the water supply is already compromised.

**4. Remote Control of Physical Equipment:**

- Some SCADA systems allow for remote control of physical equipment, including pumps, valves, and chemical feeders. An attacker with control over this equipment could directly alter the water flow and pressure, leading to changes in water chemistry or distribution patterns that could go unnoticed until the impact is significant.



➤ **Mitigation Measures:**

➤ To prevent such scenarios, it's critical for the water utility to implement robust cybersecurity measures, including:

- **Strict Access Controls:** Limiting access to SCADA systems to authorized personnel only, using strong authentication methods.
- **Network Segmentation:** Separating IT and OT networks to prevent unauthorized access from one system to another.
- **Regular Security Audits and Patch Management:** Ensuring all systems are regularly updated and audited for vulnerabilities.
- **Real-time Monitoring and Incident Response Plans:** Implementing real-time monitoring of systems and having a well-prepared incident response plan to quickly address any breaches

**Follow-up prompt:** What specific audit tests can I perform to verify that the IT and OT networks are properly segmented ?

### Chat GPT:

To verify that the IT (Information Technology) and OT (Operational Technology) networks are properly segmented in your audit, you can perform the following specific audit tests:

#### 1. Review Network Architecture Diagrams

- **Test:** Obtain and review the network architecture diagrams to understand how the IT and OT networks are structured. Look for clear separation between the two networks, with firewalls or other security devices in place to prevent direct communication between them.
- **Objective:** Ensure that the diagrams reflect actual network segmentation and identify any potential points of connectivity between IT and OT systems.

#### 2. Examine Firewall Configurations

- **Test:** Review the firewall rules and configurations that control traffic between the IT and OT networks. Verify that the rules are configured to block unauthorized

traffic and only allow necessary communication, such as specific protocols or services required for legitimate operations.

- **Objective:** Confirm that the firewall effectively enforces segmentation and prevents unauthorized access from IT to OT or vice versa.

#### 3. Network Traffic Analysis

- **Test:** Conduct a network traffic analysis to monitor data flow between the IT and OT networks. Use network monitoring tools to capture and analyze traffic patterns, looking for any unauthorized or suspicious communication between the two segments.
- **Objective:** Validate that the IT and OT networks are not improperly interconnected and that no unauthorized traffic is passing between them.



#### 4. Vulnerability Scanning

- **Test:** Perform vulnerability scans on both the IT and OT networks to identify any common vulnerabilities or misconfigurations that could allow cross-network attacks. Focus on identifying weaknesses in the network segmentation controls.
- **Objective:** Detect any vulnerabilities that could compromise the integrity of the network segmentation.

#### 5. Access Control Review

- **Test:** Review access controls and permissions to verify that users with IT network access do not have unnecessary access to the OT network. Check for the presence of multi-factor authentication (MFA) and other strong authentication methods for accessing critical OT systems.
- **Objective:** Ensure that proper access controls are in place to prevent unauthorized access from the IT network to the OT network.

#### 6. Review of Network Logs

- **Test:** Analyze network logs to review historical traffic between the IT and OT networks. Look for any unusual or unauthorized attempts to access OT systems from the IT network.
- **Objective:** Identify any past security incidents or breaches that may indicate improper segmentation.

#### 7. Penetration Testing

- **Test:** Conduct penetration testing on the IT network to assess whether an attacker could pivot from the IT network to the OT network. This involves simulating an attack scenario to test the effectiveness of network segmentation controls.
- **Objective:** Verify that the segmentation between IT and OT networks is strong enough to prevent lateral movement by attackers.



## 8. Physical Security Controls Review

- **Test:** Review the physical security controls protecting network infrastructure, such as routers, switches, and firewalls that separate the IT and OT networks. Ensure that these devices are physically secure and inaccessible to unauthorized personnel.
- **Objective:** Confirm that physical access to network segmentation devices is restricted, reducing the risk of tampering or unauthorized changes.

## 9. Policy and Procedure Review

- **Test:** Review the organization's policies and procedures regarding network segmentation, including how changes to the network are managed and

documented. Verify that there are clear guidelines for maintaining and auditing network segmentation.

- **Objective:** Ensure that proper policies are in place and followed to maintain effective network segmentation over time.

By performing these tests, you can assess the effectiveness of the network segmentation controls and ensure that the IT and OT networks are properly isolated to reduce the risk of cyberattacks.



## Prompt (2) for Chat GPT:

The text below contains my company's purchase card procedures. Please extract and list all controls from text:

### ► Chat GPT:

Sure! Please share the text containing your company's purchase card procedures, and I'll identify and list the controls for you:

#### ► 1. Becoming a Cardholder

- **Training Requirement:** Cardholders must complete required training before activation, with a 90-day deadline. If not completed, the card will be canceled.
- **Approval:** Cardholder must be approved by the Budgetary Approver.
- **User Access Form:** Cardholders must submit the Concur-P-Card User Access Request Form for processing.
- **Electronic Agreement:** Cardholders must electronically sign the

Purchasing Card Agreement before receiving the card.

#### ► 5. Changes and Renewals

- **Account Changes:** Cardholders must promptly report personal information changes to P-Card Services.
- **Card Renewal:** P-Cards are reissued every 3 years and mailed to the cardholder via Campus Mail.

These controls help to ensure compliance, accountability, and appropriate use of the P-Card system at the University



**Follow-up prompt:** “For each of the controls you listed above, please add the possible risks which the control is intended to mitigate”

**ChatGPT:** Here’s a breakdown of each control with the corresponding risks that each is intended to mitigate:

## ▶ 1. Becoming a Cardholder

### • Training Requirement

- **Risk Mitigated:** Inadequate understanding of policies and improper card usage. Without proper training, cardholders may misuse the P-Card, violate policies, or fail to follow appropriate procedures, leading to financial discrepancies or unauthorized purchases.

### • Approval

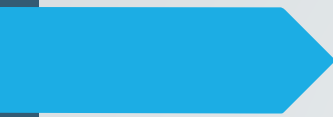
- **Risk Mitigated:** Unqualified or unauthorized individuals gaining access to the P-Card. Approval ensures that only suitable employees with appropriate responsibilities are cardholders.

### • User Access Form

- **Risk Mitigated:** Unauthorized or incorrect issuance of P-Cards. The access form ensures the request is properly documented and reviewed, preventing errors or fraud.

### • Electronic Agreement

- **Risk Mitigated:** Lack of commitment or acknowledgment of responsibilities. Ensures that cardholders formally agree to comply with the program’s rules, reducing the risk of non-compliance or misunderstanding of responsibilities.



**Follow-up prompt:** “I am in the process of updating the policy above, are there any controls which are missing in the current document which I should include in my revision?”

**ChatGPT:** Yes, there are additional controls that could be included in your policy to strengthen risk mitigation, improve compliance, and enhance oversight. Below are suggestions for missing controls you might consider adding during your revision :

▶ **6. Real-Time Alerts for High-Risk Transactions**

- **Purpose:** Notify cardholders, supervisors, or administrators immediately of suspicious or non-compliant transactions.
- **Risk Mitigated:** Delays in detecting and addressing misuse or fraud.
- **Implementation:** Enable automated alerts through the card issuer's system for transactions above thresholds or flagged categories

.....

▶ **16. Centralized Incident Log**

- **Purpose:** Maintain a centralized record of policy violations, disputes, and actions taken.
- **Risk Mitigated:** Inconsistent handling of incidents or repeat violations by cardholders.
- **Implementation:** Require departments to report incidents to a central database for tracking and analysis.

# The Internal Audit Engagement Lifecycle & AI Applications



- Risk Assessment
- Risk Description
- Controls
- Audit Scope

- Audit Interview Questions
- Audit Interview Summary
- Applicable Research
- Evidence Evaluation

- Correct Grammar
- Improve style and language

- Are we there yet
- ???

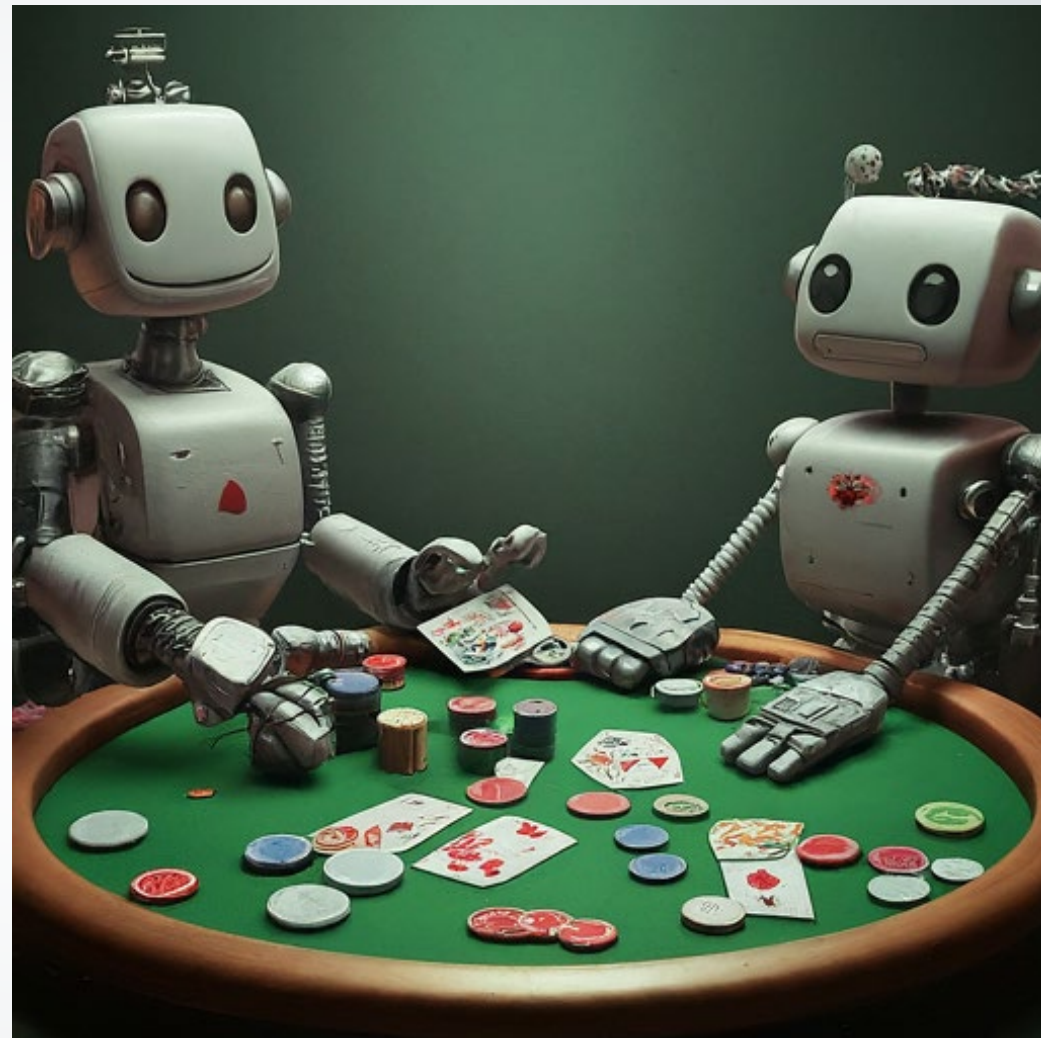
### Polling Question #3

If a fully autonomous self-driving car based on AI technology was available on the market today at an affordable price, would you buy one?

- a. Yes.
- b. Never
- c. Maybe. I will consider it after it has been 2-3 years on the market

# AI – Tips & Risks

“Keep going....”





# Prompt “Engineering” in AI

*Prompt engineering is the art of crafting effective prompts to guide AI models towards high-quality and relevant outputs. Most auditors make pretty good prompt engineers....*

## 1. Specificity and Clarity:

- ▶ **Be precise:** Clearly define the desired output. Avoid vague or ambiguous language.
- ▶ **Provide context:** Give the AI relevant information to help it understand the task.
- ▶ **Use specific instructions:** Guide the AI towards the desired outcome with clear instructions.

## 2. Conciseness:

- ▶ **Keep it simple:** Avoid unnecessary complexity.
- ▶ **Focus on essentials:** Include only the most relevant information.
- ▶ **Avoid redundancy:** Repeat information only if necessary.

## 3. Creativity and Experimentation:

- ▶ **Think outside the box:** Try different approaches to see what works best.
- ▶ **Be open to new ideas:** Experiment with different prompts.
- ▶ **Learn:** Continuously improve your prompts based on results.



# Accountability & Risks

## You are accountable:

- ▶ The auditor is 100% accountable for the quality of her/his work product. Apply critical thinking and consider the context and reliability of the information provided by AI.
- ▶ AI should be used legally and responsibly, in compliance with applicable regulations and internal policies.

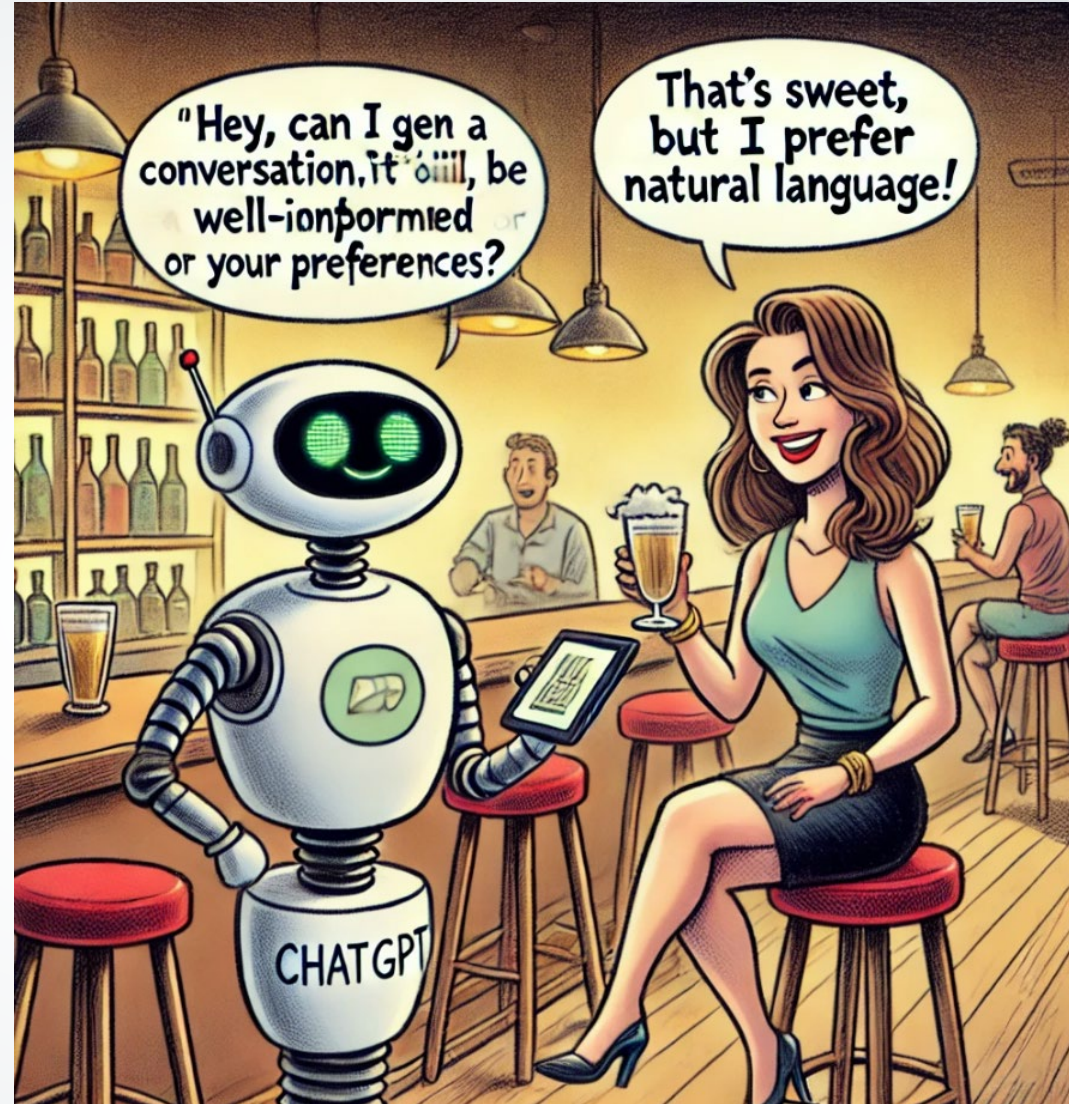
## Risks:

- ▶ **Inaccurate information:** AI models are trained on imperfect data and algorithms; hence they may provide incorrect or misleading information at times.
- ▶ **Privacy & security concerns:** What's entered in AI stays in AI. AI platforms should be treated as public spaces, and confidential or personal information should not be used.
- ▶ **Social Bias:** AI models can inadvertently reflect biases present in the training data, leading to biased or unfair responses.
- ▶ **Legal & Ethical issues:** Intellectual property rights, copyright infringement, data protection, employment impact, etc...



### Original ChatGPT Dialog:

- ➔ ChatGPT says “Hey, can I generate a conversation? I promise, it’ll be well informed and optimized for your preferences”
- ➔ She replies “That’s sweet, but I prefer natural language”





# The Black Box vs. Explainable AI

- ▶ Many (if not most) of the advanced machine learning and neural network-based AI appear as a black box – users can't understand what goes into a decision that results in a recommendation
- ▶ To increase trust and to make sure algorithms are ethical and accurately understood, explainable AI approaches are being developed
  - “White box” AI is the **idea** of a system that is understandable, justifiable and auditable by humans
  - The DARPA XAI Program (Explainable AI) is a research initiative by the Defense Advanced Research Projects Agency (DARPA) aimed at developing AI systems that can explain their reasoning and decision-making processes to humans. The goal is to make AI more transparent, accountable, and trustworthy, particularly in high-stakes applications like defense and national security.

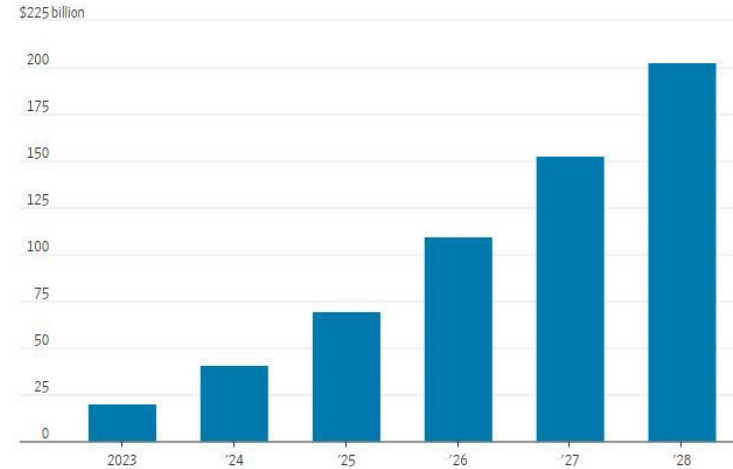
# AI – What is next

“I feed upon your every thought and so my power grows”

- Rapid growth in AI development and deployment
- Many of your organization's suppliers are using or attempt to use AI in their products or services sold to you.
  - How do you audit their AI use?
  - Is your agency ready to use services which incorporate AI?
- Can you help your organization distinguish hype vs. reality when evaluating AI - based solutions?

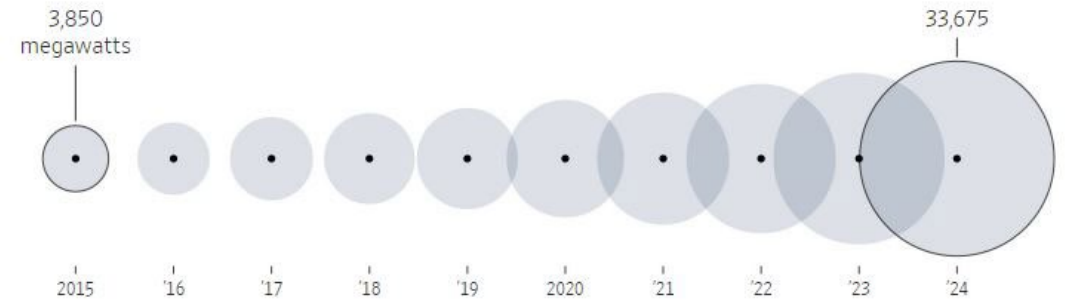
“And the people bowed and prayed to the neon god they made”

Projected worldwide spending on AI and generative AI solutions by enterprises (2023-2028)



Note: Forecasts published August 2024  
Source: International Data Corp

Commissioned power for U.S. and Canada data centers, yearly



Note: 2024 figure is a full-year projection  
Source: datacenterHawk

Source: The Wall street Journal



Questions