

# GENERATIVE AI PROMPTS FOR AUDITORS AND CPAs



Elizabeth McDowell, CPA, CIA  
Founder, Audit Forward

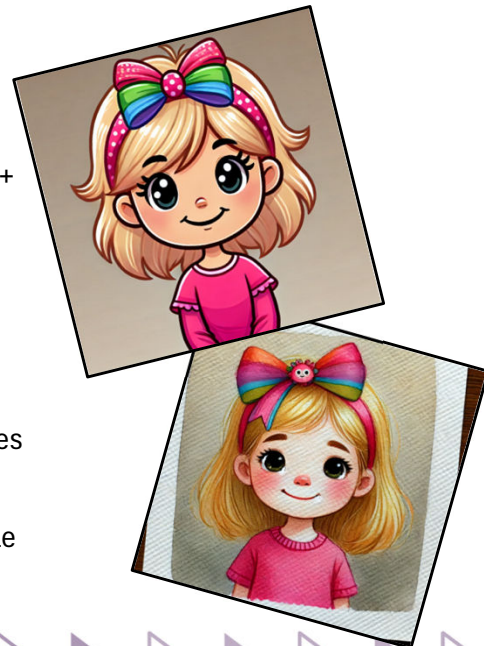
and Audie the  
Internal Otteror!



## Meet Elizabeth



- » 20 years audit experience + CPA + CIA
- » Passionate about internal audit advocacy and changing industry perception of auditors!
- » Love walking with fur babies Finn, Clara, and Orion
- » Ravensburger jigsaw puzzle snob!



## P.S. Artificial Intelligence is Always Improving!



## Meet Audie the Internal Otteror!



Elizabeth and Audie help companies *Audit Smarter, not Harder* – do more with the tools you already have!

- *Internal audit consulting and co-sourced audits*
- *Quality Assurance Reviews (QARs)*
- *Training for Boards and Committees*
- *Optimize your GRC system*
- *Smarter and digitized branch audits (financial institutions)*
- *Automate employee account monitoring (financial institutions)*



# Today's Agenda



**Generative  
AI  
101**



**GenAI  
Risks  
for Auditors**



**Prompt  
Engineering  
Basics**



**Gen AI  
Prompt  
Examples!**

AUDIT  FORWARD

# A (VERY!) BRIEF AI PRIMER



6

## Internal Audit + Artificial Intelligence



The launch of OpenAI's ChatGPT in November 2022 rewrote the book on the modern business model. Virtually overnight, the availability of fast and powerful tools to harness vast amounts of data and create new content became reality.

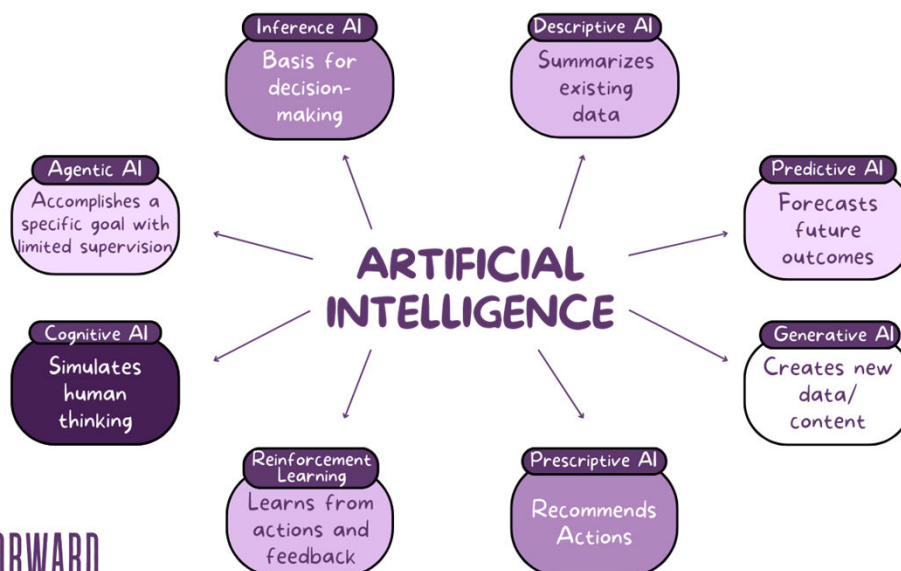
For internal audit, this evolution in the digital revolution presents a double-edged sword. **On the plus side, adoption of AI within internal audit functions offers a golden opportunity to improve efficiency and productivity, as well as enhance its value to the organization.** The other side of the sword is that risk averse internal audit leaders might delay AI adoption and fall dangerously behind.

While concerns such as data security, fraud, compliance risks, hallucinations, design bias, and overreliance are valid, especially given the amount of change management required for AI, **using these risks as an excuse to delay adoption can be detrimental to the future of the internal audit function and its ability to add value to the organization.**

- Institute of Internal Auditors



## It's MORE than Just GenAI!



## GenAI – Key Definitions

- **Generative AI** – a type of artificial intelligence that can create new content, such as text, images, or music, by learning patterns from existing data. Generative AI models can produce outputs that are similar to the training data but are novel and unique.
- **GPT (*Generative Pre-trained Transformer*)** – a type of language model developed by OpenAI that uses a transformer architecture. GPT models are pre-trained on large datasets and can generate human-like text by predicting the next word in a sequence.
- **Prompt** – A user's question or instruction given to the model to elicit a specific response

AUDIT  FORWARD

9

## Demystifying AI – It's Just Math!

- **AI will HELP enhance internal audit, not replace it**
- **AI can help us make better decisions**
- **At it's core, AI is just math – algorithms, formulas, and huge amounts of data**
- **We must not fear it!**

# Example GPTs

DEVELOPER – GPT	DESCRIPTION
<b>OpenAI – ChatGPT</b>	A conversational AI platform powered by advanced language models, designed to assist with tasks ranging from answering questions and drafting content to coding and creative brainstorming.
<b>Google – Gemini</b>	A multimodal AI by Google capable of handling text, images, and audio; integrated with Google services for real-time information and enhanced reasoning
<b>Microsoft – Copilot</b>	Embedded within Microsoft Office apps like Word and Excel, this tool helps productivity through AI-driven contextual assistance and automation
<b>Meta – Meta AI</b>	Created by Meta (formerly Facebook) and integrates with social platforms and offers capabilities like image generation and real-time interaction

AUDIT  FORWARD

11

# GETTING STARTED WITH GENERATIVE AI



12

# Generative AI in Internal Audit

## PROS

- Process vast amounts of data
- Continuous monitoring using APIs
- Monitoring regulatory changes
- Audit scalability
- Support strategic decision making

## CONS

- Privacy and security risks
- Difficulty understanding context
- Over-reliance on automation
- Ethical concerns and biases

AUDIT  FORWARD

13

# GenAI Risks for Auditors

RISK	DESCRIPTION	SOLUTION
<b>Inaccurate Data</b>	The algorithm has been trained on data that was collected, classified, or otherwise subjected to biases.	Don't accept AI generated responses as completely accurate; always apply professional skepticism, and verify information provided
<b>Poisoned Data</b>	An AI tool has been deliberately given inaccurate, biased, or otherwise bad information, which is then used to develop responses.	
<b>Overreliance on AI-Generated Content</b>	Internal auditors blindly 'copy and paste' information from the AI.	
<b>Confidential Information Shared</b>	Users enter information into the AI that is not meant for public consumption.	Remove any potentially identifying information from prompts

# Getting Started with GenAI

- **If working with a public tool**, never give identifiable or proprietary information
- **Scrutinize the responses** given and always use professional skepticism
- **Ask clarifying questions** or request a more detailed response based upon response given
- **Remove all bias from your prompts** – biased questions give biased answers

## It's Not Just ChatGPT!

### By ChatGPT

GPTs created by the ChatGPT team

- Monday**  
A personality experiment. You may not like it. It may not like you.  
By ChatGPT
- DALL·E**  
OpenAI's legacy image generation model. For our latest model, ask ChatGPT to create an image in the main chat.  
By ChatGPT
- Data Analyst**  
Drop in any files and I can help analyze and visualize your data.  
By ChatGPT
- Hot Mods**  
Let's modify your image into something really wild. Upload an image and let's go!  
By ChatGPT
- Creative Writing Coach**  
I'm eager to read your work and give you feedback to improve your skills.  
By ChatGPT
- Coloring Book Hero**  
Take any idea and turn it into whimsical coloring book pages.  
By ChatGPT

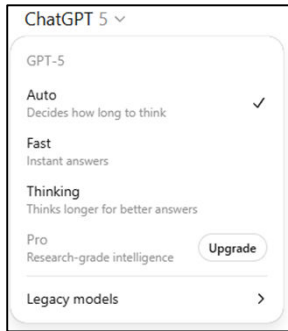
### GPTs

Discover and create custom versions of ChatGPT that combine instructions, extra knowledge, and any combination of skills.

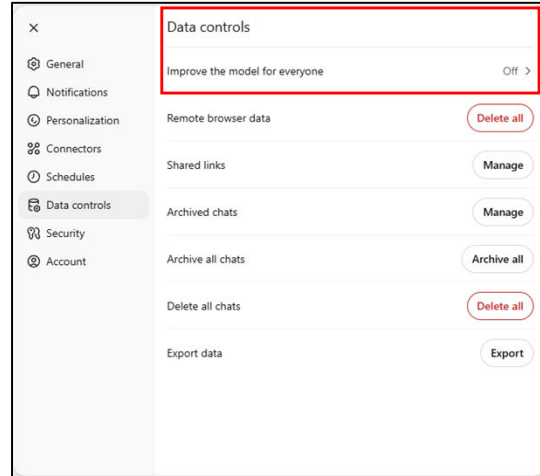
- Search: risk
- All Personal account workspace
- GRC (Governance, Risk, & Compliance) Advisor**  
This solution assists organizations in establishing best practices for Governance, Ris...  
By Calvin Daniels ◉ 25K+
  - RAW@AI - Risk Management Advisor**  
Risk management, quantitative risk assessment, risk-based decision making and in...  
By Alexei Sidorenko ◉ 5K+
  - TripWise - School Trip Risk Assessor**  
Save time and stay compliant. TripWise asks you one simple question at a time, the...  
By Miss RE Amola ◉ 40+
  - Internal Audit & Risk Management**  
Expert in internal auditing and risk management.  
By Sayed Ahmad Hasannejad ◉ 1K+

# ChatGPT Settings & Privacy

I use ChatGPT 5:



I also click "off" for the option to improve the model



AUDIT  FORWARD

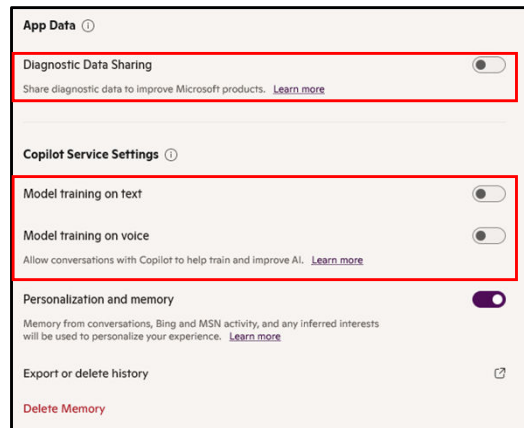
17

# CoPilot Settings & Privacy

I use the latest version of CoPilot:



I also click "off" for diagnostic data sharing and model training



AUDIT  FORWARD

18

# WRITING AWESOME PROMPTS!



## Writing Awesome GenAI Prompts!

- ▶ **Be Specific**
- ▶ **Include Context**
- ▶ **Use Action Words**
- ▶ **Break Down Complex Queries**
- ▶ **Iterate and Refine**
- ▶ **Use multiple GenAI engines!**

# Be Specific & Add Context

**Be specific, descriptive and as detailed as possible about the desired context, outcome, length, format, style.**

- Name the **artifact** you want – a memo, table, checklist, slide text, etc.
- Specify the **audience, tone, and length**, and provide **context** such as industry, company size, systems, framework
- Provide **constraints** such as policies, templates, rating scales
- Provide **source hints** including data availability, links, fields, definitions

AUDIT  FORWARD

21

## Less Effective: Specificity

Give me risks for payroll

Here's a list of common payroll risks, grouped by category so you can adapt them for audit, risk assessment, or internal control exercises:

### 1. Accuracy & Processing Risks

- **Incorrect Calculations** – Errors in pay rates, hours, overtime, or deductions leading to over/underpayment
- **Data Entry Errors** – Manual input mistakes in employee setup or time reporting
- **Misclassification of Employees** – Treating employees as contractors or vice versa, causing tax and compliance issues
- **Duplicate or Missing Payments** – Employees paid twice or not at all due to processing errors

### 2. Compliance & Regulatory Risks

- **Noncompliance with Tax Regulations** – Incorrect withholding or late remittance of payroll taxes and filings
- **Violation of Wage and Hour Laws** – Failure to pay minimum wage, overtime, or holiday pay
- **Benefit and Deduction Mismanagement** – Incorrect handling of garnishments, insurance, or retirement contributions
- **Record Retention Noncompliance** – Failure to maintain payroll records for the required period

### 3. Fraud & Security Risks

- **Ghost Employees** – Payments made to fictitious or terminated employees
- **Unauthorized Pay Rate Changes** – Manipulation of salary data without approval
- **Theft of Payroll Data** – Breach of confidential information such as SSNs or bank accounts
- **Collusion Between HR and Payroll Staff** – Coordinated manipulation of payroll entries

### 4. System & Technology Risks

- **System Access Control Weaknesses** – Excessive or inappropriate user access to payroll systems
- **System Failures or Downtime** – Payroll not processed due to outages or technical issues
- **Inadequate System Integration** – Misalignment between HR, timekeeping, and payroll systems leading to discrepancies
- **Data Backup and Recovery Failures** – Inability to restore payroll data after system loss

### 5. Governance & Oversight Risks

- **Inadequate Review and Approval Controls** – Payroll processed without proper verification or segregation of duties
- **Poor Vendor Oversight (if outsourced)** – Third-party errors or noncompliance not detected timely
- **Lack of Reconciliation** – Payroll not reconciled to general ledger or bank statements
- **Weak Change Management** – System or process changes made without proper testing or authorization

### 6. Operational & Continuity Risks

- **Dependence on Key Personnel** – Limited staff knowledge or lack of cross-training causes process disruptions
- **Failure to Meet Deadlines** – Delays in payroll processing or tax filing leading to penalties
- **Poor Communication Between Departments** – HR and Finance not aligned on employee changes, bonuses, or terminations



## More Effective: Specificity

List 7 risks for US payroll processing during year-end close 2024; map each to COSO principle, add a 1-sentence control, output as CSV columns: Risk,COSO,Control

Here's your CSV-formatted list of seven U.S. payroll processing risks for year-end close 2024, each mapped to a COSO principle with a one-sentence control:

pgsql

Copy code

```
Risk,COSO,Control
Incorrect tax withholding or reporting (e.g., Form W-2, 941),Principle 10 - Control Activities,Aut
Late submission of payroll taxes or filings,Principle 11 - Control Activities,Payroll calendar anc
Bonus or overtime miscalculations,Principle 12 - Technology Controls,System-based calculations are
Unrecorded or duplicate payroll entries in the general ledger,Principle 16 - Separate Ongoing Eval
Unauthorized pay rate or employee changes,Principle 8 - Assess Fraud Risk,Role-based access contrc
Inaccurate accruals for PTO or year-end bonuses,Principle 6 - Risk Response,Quarterly management r
Failure to update tax tables or regulatory changes (e.g., new thresholds for 2024),Principle 13 -
```



Risk	COSO	Control
Incorrect tax withholding or reporting (e.g. Form W-2 941)	Principle 10 - Control Activities	Automated validation checks reconcile tax withholdings to IRS and state filing reports before submission.
Late submission of payroll taxes or filings	Principle 11 - Control Activities	Payroll calendar and task tracker automatically alert payroll staff to approaching filing deadlines.
Bonus or overtime miscalculations	Principle 12 - Technology Controls	System-based calculations are configured with current pay rules and reviewed quarterly by payroll management.
Unrecorded or duplicate payroll entries in the general ledger	Principle 16 - Separate Ongoing Evaluations	Finance performs monthly reconciliations between payroll register and GL postings.
Unauthorized pay rate or employee changes	Principle 8 - Assess Fraud Risk	Role-based access controls restrict pay rate changes and require HR approval prior to payroll processing.
Inaccurate accruals for PTO or year-end bonuses	Principle 6 - Risk Response	Quarterly management review validates accrued payroll liabilities against HR and finance estimates.
Failure to update tax tables or regulatory changes (e.g. new thresholds for 2024)	Principle 13 - Use of Relevant Information	Payroll system updates are verified and documented by compliance staff upon release of new IRS/state guidance.

## Use Action Words

Tell the AI exactly what you want using action verbs such as list, explain, draft, summarize, compare, identify, or calculate.

- **Models respond best to explicit instructions** like “List,” “Draft,” or “Summarize” because they signal that you want an actionable output, not a discussion
- **Starting with verbs** helps the model understand what to produce, not just what to talk about.
- **Match the auditor’s workflow** by using words like write, analyze, test, and summarize – verbs that map directly to audit activities.
- **When you tell the AI exactly what kind of content to generate**, you minimize follow-ups and rewrites.

# ✗ Less Effective: Action Words

tell me about duplicate payments

Duplicate payments occur when the same invoice is paid more than once, leading to overpayment and financial loss. They're typically caused by process errors, system issues, or human oversight.

Here's a deeper look into what they are, why they happen, and how to prevent them:

## What Are Duplicate Payments?

- A *duplicate payment* is an unintended second (or third) payment for the same invoice or financial obligation.
- This results in a vendor receiving more than they're owed, which can distort financial records and reduce available cash flow. <sup>1 2</sup>

## Common Causes

- Manual entry errors:** Typing the same invoice twice or failing to check for prior payment.
- Invoice format variations:** Slight differences in invoice numbers or formatting can trick systems into treating them as separate.
- Lack of invoice matching controls:** When purchase orders, receipts, and invoices aren't properly reconciled.
- Multiple submission channels:** Vendors may send invoices via email and portal, leading to duplicates.
- System glitches or ERP limitations:** Even automated systems can miss duplicates if not properly configured. <sup>2 3</sup>

## Impact on Businesses

- Cash flow disruption:** Funds are tied up unnecessarily.
- Vendor disputes:** Overpayments can strain relationships and require time-consuming recovery efforts.
- Audit and reconciliation burden:** Duplicate payments complicate month-end close and financial reporting.
- Risk of fraud:** Repeated payments can mask fraudulent activity or internal control weaknesses. <sup>3</sup>

## Prevention Strategies

- Implement 3-way matching:** Match purchase orders, receipts, and invoices before payment.
- Use duplicate detection software:** Many AP automation tools flag potential duplicates based on invoice number, vendor, and amount.
- Standardize invoice formats:** Require vendors to follow consistent submission guidelines.
- Train AP staff:** Ensure teams understand common triggers and review protocols.
- Regular audits:** Periodic reviews can catch duplicates and improve controls. <sup>1 4</sup>

# ✓ More Effective: Specificity

List 8 duplicate-payment red flags and pair each with one Power Query step and one SQL pattern, deliver as table: RedFlag,PowerQuery,SQL

Here's a table of 8 high-impact duplicate payment red flags, each paired with a Power Query step and a SQL pattern that can help surface exceptions in audit analytics:

RedFlag	PowerQuery	SQL
Same invoice number paid more than once	Group by InvoiceNumber, count rows > 1	SELECT InvoiceNumber, COU
Same vendor, same amount, different invoice numbers	Group by VendorID and Amount, filter where distinct InvoiceNumber > 1	SELECT VendorID, Amount F
Same invoice number with different payment dates	Group by InvoiceNumber, check for multiple PaymentDate values	SELECT InvoiceNumber, COI
Same invoice paid via multiple payment methods	Group by InvoiceNumber, check for multiple PaymentMethod values	SELECT InvoiceNumber, COI
Same vendor, same invoice date, same amount	Group by VendorID, InvoiceDate, Amount, count rows > 1	SELECT VendorID, InvoiceDa

Same PO number used across multiple invoices	Group by PONumber, count distinct InvoiceNumber > 1	SELECT PONumber, COUNT
Invoice paid after void or reversal	Filter where InvoiceStatus = 'Voided' and PaymentStatus = 'Paid'	SELECT * FROM Payments V
Same invoice number with different vendor IDs	Group by InvoiceNumber, count distinct VendorID > 1	SELECT InvoiceNumber, COI

Let me know if you want to modularize these in Power Query or build exception flags for each. I can also help you stratify by vendor risk or payment channel.

# ▶ Break Down Complex Queries

**If your goal is to tackle big or multi-part requests, start by structuring them into clear, sequential steps.**

- ▶ **Prevents overload** – Asking for too much at once often leads to incomplete or messy results
- ▶ **Improves accuracy** – Breaking requests into smaller parts lets the model focus and build logically
- ▶ **Saves time** – You can correct or refine early outputs before wasting effort on a long, flawed response
- ▶ **Mimics audit methodology** – Auditors naturally break engagements into phases: planning, fieldwork, reporting, follow-up

# ▶ ✖ Less Effective: Complex Queries

The screenshot displays an ITGC Audit Report with the following sections:

- 4. Audit Procedures**
  - A. IT Governance
  - B. User Access Management
  - C. Change Management
  - D. Computer Operations
  - E. Backup and Recovery
- 5. Sampling**
  - Minimum 25 users for access testing (stratified by role).
  - 10-15 change tickets across system types.
  - 10 incidents and 10 backup jobs.
  - Sample size adjusted based on population and risk rating.
- 6. Evaluation Criteria**
  - Effective:** Controls designed and operating effectively with no exceptions.
  - Partially Effective:** Minor design or operating deficiencies.
  - Ineffective:** Significant gaps impacting system reliability or data integrity.

**ITGC AUDIT REPORT**

**Audit Title:** IT General Controls (ITGC) Audit  
**Department:** Information Technology  
**Audit Period:** FY2024  
**Auditors:** [Your Audit Team]  
**Date:** [Insert Date]

**Executive Summary**

The ITGC audit assessed the adequacy and effectiveness of general IT controls supporting systems relevant to financial reporting. Overall, **controls are moderately effective**, with improvement opportunities noted in access reviews, change documentation, and disaster recovery testing.

**Overall Rating:** ● Partially Effective

**Summary of Findings**

Finding ID	Area	Description	Risk Rating	Recommendation	Management Response
ITGC-01	User Access	Inconsistent quarterly access	Medium	Implement automated reminders	Management will adopt quarterly (RTO/RPO)



## More Effective: Specificity

Perfect — let SOX structure • In-Scope • Associate • Detailed • Sampling • Tickmark • Format	<b>ITGC Audit Program (SOX)</b>	<b>ITGC Audit Program Report (SOX)</b>	
	<b>1. Access to Programs and Data</b>	<b>3. Computer Operations</b>	<b>ITGC Audit Program Report (SOX)</b>
	<b>Objective</b>	<b>Objective</b>	<b>Objective:</b>
	<b>Risks</b>	<b>Risks</b>	<b>Risks:</b>
<b>Evidence</b>	<b>Evidence</b>	<b>Procedures Performed:</b>	
<b>Test Steps</b>	<b>Test Steps</b>	<b>Sampling Approach:</b>	
<b>Sampling</b>	<b>Sampling</b>	<b>Tickmarks:</b>	
<b>Tickmarks</b>	<b>Tickmarks</b>	<b>Results:</b>	
		<b>Conclusion:</b>	

## Iterate and Refine

### Don't overthink your prompt when you get started!

- You can always **refine your prompt and try again**
- **Don't worry about grammar, spelling, or formatting.** The AI will figure it out!
- If you like the data you get but not the format, **ask for a different format**
- **Give targeted feedback about what to change** – too long, missing field, wrong tone
- **Ask for alternatives:** version A formal, version B plain-English
- **Tighten constraints** such as word counts, column names, examples, references



# First Pass: Generic Ask

Provide a List of Fraud Risks

Absolutely, Elizabeth. Here's a structured list of common fraud risks, organized by category to help you assess control gaps and design targeted audit analytics:

## Financial and Transactional Fraud Risks

- **Unauthorized transactions:** Payments made without proper approval or documentation
- **Duplicate payments:** Same invoice paid more than once
- **Ghost vendors or employees:** Fictitious entities created to siphon funds
- **Inflated or falsified invoices:** Overstated amounts or fabricated services
- **Kickbacks and bribery:** Collusion between internal staff and external vendors
- **Expense reimbursement fraud:** Personal expenses submitted as business-related
- **Check tampering or forgery:** Altered payee, amount, or endorsement

## Employee and Internal Fraud Risks

- **Time theft:** Falsified timesheets or unworked hours claimed
- **Payroll fraud:** Manipulated pay rates, bonuses, or ghost employees
- **Asset misappropriation:** Theft or misuse of company assets
- **Data manipulation:** Altering records to conceal fraud or inflate performance
- **Conflict of interest:** Undisclosed relationships affecting procurement or hiring

## Cyber and IT-Related Fraud Risks

- **Phishing and social engineering:** Deceptive emails or calls to extract credentials
- **Unauthorized system access:** Use of stolen or shared credentials
- **Data exfiltration:** Theft of sensitive customer or financial data
- **System manipulation:** Altering logs or audit trails to hide fraud
- **Fake or malicious software:** Installed to capture data or redirect funds

## Procurement and Vendor Fraud Risks

- **Bid rigging:** Collusion among vendors to fix prices or rotate bids
- **Split purchases:** Breaking up purchases to avoid approval thresholds
- **Shell companies:** Vendors created by insiders to funnel payments
- **Non-performance fraud:** Vendors paid for goods/services not delivered

## Regulatory and Reporting Fraud Risks

- **Misreporting to regulators:** Understating risk, misclassifying loans, or falsifying disclosures
- **HMDA or fair lending misrepresentation:** Manipulated demographic or pricing data
- **Redlining or steering:** Discriminatory patterns in marketing or loan approvals
- **False certifications:** Inaccurate attestations on compliance or audit reports



# Refine: More Detail Requested

Keep 8 bullets, add behavioral vs organizational tags, include real-world case name in parentheses

Here's a refined list of eight high-impact fraud risks, each tagged as either **Behavioral** (individual-driven) or **Organizational** (systemic or structural), with real-world case references to ground them in precedent:

## Key Fraud Risks with Tags and Case References

1. **Ghost Employees on Payroll**
  - **Tag:** Behavioral
  - **Risk:** Fictitious employees added to payroll by insiders to divert funds
  - **Case:** *CityTime Scandal (New York City, 2010)* – \$80M lost through fraudulent timekeeping and ghost workers
2. **Bid Rigging in Procurement**
  - **Tag:** Organizational
  - **Risk:** Vendors collude to fix prices or rotate bids, often with internal facilitation
  - **Case:** *Chicago School Board Scandal (2015)* – Kickbacks tied to rigged education contracts
3. **Falsified Expense Reimbursements**
  - **Tag:** Behavioral
  - **Risk:** Employees submit personal or inflated expenses as business-related
  - **Case:** *Tyco International (2002)* – Executives misused company funds for lavish personal expenses

## 4. Redlining in Mortgage Lending

- **Tag:** Organizational
- **Risk:** Systemic denial or discouragement of loans in minority neighborhoods
- **Case:** *Hudson City Savings Bank (2015)* – \$33M settlement for discriminatory redlining practices

## 5. Vendor Shell Companies Created by Insiders

- **Tag:** Behavioral
- **Risk:** Employees create fake vendors to funnel payments
- **Case:** *WorldCom (2002)* – Fraudulent vendor payments used to hide \$3.8B in expenses

## 6. Data Manipulation to Conceal Risk

- **Tag:** Organizational
- **Risk:** Altering internal records to misrepresent performance or compliance
- **Case:** *Wells Fargo (2016)* – Millions of fake accounts created to meet sales targets

## 7. Kickbacks for Contract Awards

- **Tag:** Behavioral
- **Risk:** Employees receive bribes in exchange for awarding contracts
- **Case:** *Siemens AG (2008)* – \$1.6B settlement for global bribery and kickback schemes

## 8. Split Purchases to Evade Controls

- **Tag:** Organizational
- **Risk:** Breaking up purchases to bypass approval thresholds or competitive bidding



## Refine Again: Different Format

Convert to one-slide table with columns RedFlag, Type, Case, Control

Here's your one-slide table summarizing the eight key fraud risks, with columns for Red Flag, Type (Behavioral vs Organizational), Real-World Case, and a succinct Control to mitigate each risk:

Red Flag	Type	Case	Control
Ghost employees on payroll	Behavioral	<i>CityTime Scandal (NYC, 2010)</i>	Segregate payroll setup and approval; periodic reconciliation with HR roster
Bid rigging in procurement	Organizational	<i>Chicago School Board (2015)</i>	Rotate procurement staff; enforce competitive bidding with audit trails
Falsified expense reimbursements	Behavioral	<i>Tyco International (2002)</i>	Require itemized receipts; random post-payment audits
Redlining in mortgage lending	Organizational	<i>Hudson City Savings Bank (2015)</i>	Geo-mapping of applications vs demographics; fair lending testing
Shell vendors created by insiders	Behavioral	<i>WorldCom (2002)</i>	Vendor due diligence; restrict vendor creation rights
Data manipulation to conceal risk	Organizational	<i>Wells Fargo (2016)</i>	Independent data validation; whistleblower channels
Kickbacks for contract awards	Behavioral	<i>Siemens AG (2008)</i>	Conflict-of-interest disclosures; dual-approval for awards
Split purchases to evade thresholds	Organizational	<i>U.S. Navy "Fat Leonard" (2013)</i>	Monitor sequential purchases; enforce PO aggregation rules

## Use Multiple GPTs and Models

**Choose the right model for the task — and combine different GPTs for better results.**

- **Different models excel at different tasks** – some are better at writing, others at math, data, or summarization.
- **Specialized GPTs can act as audit team members** – one might draft a finding, another check grammar, and another create visuals.
- **Reduce risk of overreliance on one source** – each model has blind spots; diversity of models adds reliability.

**✖ Less Effective: Only Using One GPT**

Give me risks for payroll

Payroll processes carry a range of risks that can impact financial accuracy, compliance, employee satisfaction, and operational efficiency. Here's a breakdown of key risk categories and examples:

**Compliance Risks**

- **Misclassification of employees** (e.g., contractor vs. employee) can lead to penalties and back taxes.
- **Incorrect tax withholding or reporting** may result in IRS fines or audits.
- **Failure to comply with wage and hour laws** (e.g., overtime, minimum wage) can trigger legal action.
- **Late or inaccurate filings** for payroll taxes or benefits can damage reputation and incur penalties.

**Financial Risks**

- **Overpayments or underpayments** due to data entry errors or system misconfigurations.
- **Duplicate payments** or missed deductions (e.g., benefits, garnishments).
- **Fraudulent activity**, such as ghost employees or unauthorized changes to pay rates.
- **Improper accruals** for PTO, bonuses, or commissions affecting financial statements.

## CoPilot

**Operational Risks**

- **System outages or integration failures** between payroll and HRIS/ERP systems.
- **Manual processes** that increase error rates and reduce scalability.
- **Lack of audit trails** or documentation for payroll adjustments and approvals.
- **Inadequate segregation of duties**, increasing fraud risk.

**Data Security & Privacy Risks**

- **Unauthorized access** to sensitive employee data (SSNs, bank info).
- **Data breaches** due to weak controls or phishing attacks.
- **Improper disposal of payroll records**, violating privacy laws.

**Employee Relations Risks**

- **Delayed or incorrect paychecks** leading to dissatisfaction or turnover.
- **Lack of transparency** in deductions or pay calculations.
- **Inconsistent handling of payroll disputes**, eroding trust.

**✖ Less Effective: Only Using One GPT**

Give me risks for payroll

Here's a list of common payroll risks, grouped by category so you can adapt them for audit, risk assessment, or internal control exercises:

**1. Accuracy & Processing Risks**

- **Incorrect Calculations** – Errors in pay rates, hours, overtime, or deductions leading to over/underpayment
- **Data Entry Errors** – Manual input mistakes in employee setup or time reporting
- **Misclassification of Employees** – Treating employees as contractors or vice versa, causing tax and compliance issues
- **Duplicate or Missing Payments** – Employees paid twice or not at all due to processing errors

**2. Compliance & Regulatory Risks**

- **Noncompliance with Tax Regulations** – Incorrect withholding or late remittance of payroll taxes and filings
- **Violation of Wage and Hour Laws** – Failure to pay minimum wage, overtime, or holiday pay
- **Benefit and Deduction Mismanagement** – Incorrect handling of garnishments, insurance, or retirement contributions
- **Record Retention Noncompliance** – Failure to maintain payroll records for the required period

**3. Fraud & Security Risks**

- **Ghost Employees** – Payments made to fictitious or terminated employees
- **Unauthorized Pay Rate Changes** – Manipulation of salary data without approval
- **Theft of Payroll Data** – Breach of confidential information such as SSNs or bank accounts
- **Collusion Between HR and Payroll Staff** – Coordinated manipulation of payroll entries

## ChatGPT 5

**4. System & Technology Risks**

- **System Access Control Weaknesses** – Excessive or inappropriate user access to payroll systems
- **System Failures or Downtime** – Payroll not processed due to outages or technical issues
- **Inadequate System Integration** – Misalignment between HR, timekeeping, and payroll systems leading to discrepancies
- **Data Backup and Recovery Failures** – Inability to restore payroll data after system loss

**5. Governance & Oversight Risks**

- **Inadequate Review and Approval Controls** – Payroll processed without proper verification or segregation of duties
- **Poor Vendor Oversight (if outsourced)** – Third-party errors or noncompliance not detected timely
- **Lack of Reconciliation** – Payroll not reconciled to general ledger or bank statements
- **Weak Change Management** – System or process changes made without proper testing or authorization

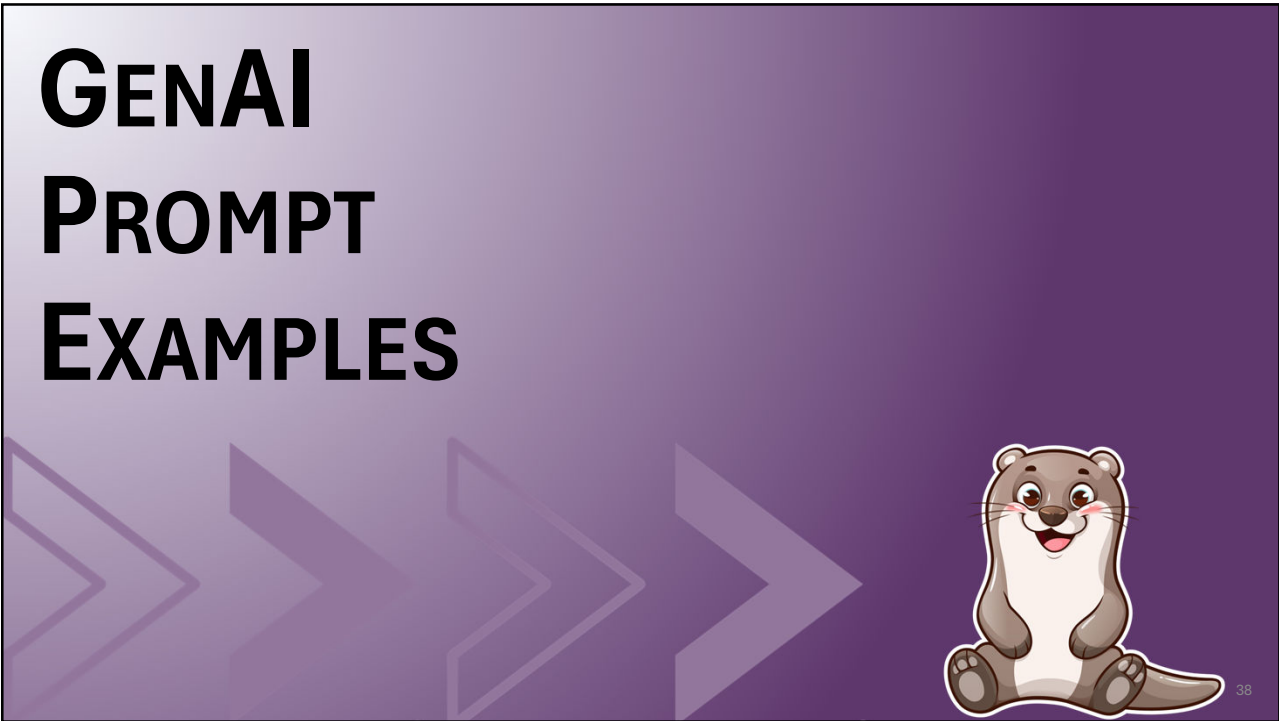
**6. Operational & Continuity Risks**

- **Dependence on Key Personnel** – Limited staff knowledge or lack of cross-training causes process disruptions
- **Failure to Meet Deadlines** – Delays in payroll processing or tax filing leading to penalties
- **Poor Communication Between Departments** – HR and Finance not aligned on employee changes, bonuses, or terminations

 **More Effective: Multiple GPTs (Multiple Algorithms & Data!)**

Risks Unique to CoPilot	Risks Unique to ChatGPT	Risks Overlapping in Both Lists
<ul style="list-style-type: none"> <li>• Incorrect tax withholding or reporting</li> <li>• Late or inaccurate filings</li> <li>• Improper accruals</li> <li>• Manual processes</li> <li>• Lack of audit trails</li> <li>• Improper disposal of payroll records</li> <li>• Delayed or incorrect paychecks leading to dissatisfaction or turnover</li> <li>• Lack of transparency in deductions or pay calculations</li> <li>• Inconsistent handling of payroll disputes</li> </ul>	<ul style="list-style-type: none"> <li>• Ghost employees</li> <li>• Unauthorized pay rate changes</li> <li>• Collusion between HR and payroll staff</li> <li>• System access control weaknesses</li> <li>• Data backup and recovery failures</li> <li>• Poor vendor oversight (if outsourced)</li> <li>• Lack of reconciliation to general ledger or bank statements</li> <li>• Weak change management</li> <li>• Dependence on key personnel / lack of cross-training</li> <li>• Failure to meet deadlines (e.g., tax filing delays)</li> <li>• Poor communication between HR and Finance</li> </ul>	<ul style="list-style-type: none"> <li>• Misclassification of employees</li> <li>• Failure to comply with wage and hour laws</li> <li>• Overpayments or underpayments / incorrect calculations</li> <li>• Duplicate payments</li> <li>• Unauthorized access to payroll data</li> <li>• System outages or integration failures</li> <li>• Inadequate segregation of duties</li> </ul>

# GENAI PROMPT EXAMPLES



# Prompt Example: Fieldwork - Testing

ChatGPT 5

A user may edit, modify or delete a matched invoice.  
 An incorrect purchase order is sent to a vendor.  
 Duplicate invoices are received and processed, leading to duplicate payments.  
 Duties are not adequately segregated.  
 Purchase order price differs from invoice price, resulting in price discrepancies that are resolved in favor of the supplier.  
 Unauthorized, fictitious or improper commitments or expenses may be incurred without management's knowledge or approval.



**generate a list of internal controls for these A/P risks:** A user may edit, modify or delete a matched invoice.  
 An incorrect purchase order is sent to a vendor.  
 Duplicate invoices are received and processed, leading to duplicate payments.  
 Duties are not adequately segregated.  
 Purchase order price differs from invoice price, resulting in price discrepancies that are resolved in favor of the supplier.  
 Unauthorized, fictitious or improper commitments or expenses may be incurred without management's knowledge or approval.

# Prompt Example: Fieldwork - Testing

ChatGPT 5

- 1. A user may edit, modify, or delete a matched invoice**
- **System-based restrictions** — Configure the A/P system to lock invoices after matching and approval, preventing edits or deletions without supervisor override
  - **Audit trails** — Maintain automated logs of all invoice changes with user ID, date/time, and reason codes
  - **Segregated edit rights** — Limit invoice modification permissions to authorized senior staff
  - **Management review** — Require periodic review of change logs for unusual activity
- 
- 2. An incorrect purchase order is sent to a vendor**
- **PO approval workflow** — Require supervisory approval before a PO is issued to a vendor
  - **Template & system validation** — Use standardized PO templates with system validations for vendor, quantity, and price fields
  - **Vendor confirmation** — Implement a process where vendors confirm POs in writing before order fulfillment
  - **Exception reporting** — Generate reports for POs modified after issuance and review for accuracy
- 
- 3. Duplicate invoices are received and processed, leading to duplicate payments**
- **System duplicate check** — Enable invoice number, vendor, and date matching controls to flag duplicates
  - **Centralized invoice processing** — Route all invoices through a single intake point to reduce duplicate entry risk
  - **Three-way match** — Require system matching of PO, goods receipt, and invoice before payment
  - **Periodic duplicate audit** — Run monthly duplicate payment reports and investigate anomalies

- 4. Duties are not adequately segregated**
- **Segregation matrix** — Maintain and enforce a responsibility matrix separating initiation, approval, and payment functions
  - **System access controls** — Configure role-based permissions to align with segregation requirements
  - **Rotation of duties** — Periodically rotate responsibilities to reduce fraud risk and detect control gaps
  - **Management review of exception cases** — Review instances where segregation is overridden due to staffing constraints
- 
- 5. Purchase order price differs from invoice price, resolved in favor of the supplier**
- **Price tolerance settings** — Set system tolerance limits for PO vs. invoice price variances, requiring approval if exceeded
  - **Price verification** — Require procurement to validate invoice prices against contract terms before approval
  - **Exception review report** — Generate regular reports of price variances and review trends for supplier patterns
  - **Contract compliance audits** — Periodically review supplier invoices for adherence to agreed pricing
- 
- 6. Unauthorized, fictitious, or improper commitments or expenses incurred without management's knowledge or approval**
- **Pre-approval requirement** — Require documented management approval for all purchase commitments above a set threshold
  - **Approved vendor list** — Restrict purchases to vetted and authorized vendors
  - **Budget monitoring** — Compare purchase activity to budget limits with alerts for overages
  - **Expense analytics** — Use data analytics to identify unusual spend patterns or unauthorized vendors

# Prompt Example: Fieldwork - Testing

ChatGPT 5

provide this in table format

put the controls in table format

Here's your A/P Risk – Internal Control Table:

Risk	Internal Controls
A user may edit, modify, or delete a matched invoice	<ul style="list-style-type: none"> <li>System-based restrictions to lock invoices after matching and approval, requiring supervisor override</li> <li>Automated audit trails capturing all changes with user ID, date/time, and reason codes</li> <li>Limit invoice modification rights to authorized senior staff</li> <li>Periodic management review of change logs</li> </ul>
An incorrect purchase order is sent to a vendor	<ul style="list-style-type: none"> <li>Require supervisory approval before issuing a PO</li> <li>Use standardized PO templates with system validations for vendor, quantity, and price fields</li> <li>Require vendor confirmation of POs in writing before fulfillment</li> <li>Review exception reports for POs modified after issuance</li> </ul>
Duplicate invoices are received and processed, leading to duplicate payments	<ul style="list-style-type: none"> <li>Enable system duplicate checks on invoice number, vendor, and date</li> <li>Centralize invoice processing to reduce duplicate entries</li> <li>Require three-way matching of PO, goods receipt, and invoice</li> <li>Run monthly duplicate payment reports and investigate anomalies</li> </ul>
Duties are not adequately segregated	<ul style="list-style-type: none"> <li>Maintain and enforce a segregation of duties matrix</li> <li>Configure system role-based permissions to align with segregation requirements</li> <li>Periodically rotate responsibilities to detect control gaps</li> <li>Review exceptions where segregation was overridden due to staffing needs</li> </ul>
Purchase order price differs from invoice price, resolved in favor of the supplier	<ul style="list-style-type: none"> <li>Set system tolerance limits for PO vs. invoice price variances, requiring approval if exceeded</li> <li>Procurement to verify invoice prices against contract terms before approval</li> <li>Review regular exception reports for price variances and supplier trends</li> <li>Conduct periodic contract compliance audits</li> </ul>
Unauthorized, fictitious, or improper commitments or expenses incurred without management's knowledge or approval	<ul style="list-style-type: none"> <li>Require documented management approval for purchase commitments above a set threshold</li> <li>Restrict purchases to approved vendor lists</li> <li>Monitor purchases against budget with alerts for overages</li> <li>Use expense analytics to identify unusual spend patterns or unauthorized vendors</li> </ul>

Got it — here's the table with each control in its own cell so it's cleaner to read and easier to work with:

Risk	Internal Control
A user may edit, modify, or delete a matched invoice	System-based restrictions to lock invoices after matching and approval, requiring supervisor override
	Automated audit trails capturing all changes with user ID, date/time, and reason codes
	Limit invoice modification rights to authorized senior staff
	Periodic management review of change logs
An incorrect purchase order is sent to a vendor	Require supervisory approval before issuing a PO
	Use standardized PO templates with system validations for vendor, quantity, and price fields
	Require vendor confirmation of POs in writing before fulfillment
	Review exception reports for POs modified after issuance
Duplicate invoices are received and processed, leading to duplicate payments	Enable system duplicate checks on invoice number, vendor, and date
	Centralize invoice processing to reduce duplicate entries
	Require three-way matching of PO, goods receipt, and invoice
	Run monthly duplicate payment reports and investigate anomalies
Duties are not adequately segregated	Maintain and enforce a segregation of duties matrix
	Configure system role-based permissions to align with segregation requirements
	Periodically rotate responsibilities to detect control gaps
	Review exceptions where segregation was overridden due to staffing needs

41

## Audie's Pro Tip: Templates & References



You can upload reference materials and templates and link to articles to point the GenAI in the right direction.

I uploaded these files for ChatGPT to reference!

- deloitte-uk-gif-internal-control-and-t... PDF
- Enterprise Risk Management (ERM) Fu... PDF
- Entity-Level Controls Audit Work Prog... Document
- Fundamentals of the COSO Framewor... PDF
- 10 Tips for Evaluating Internal Control ... PDF
- AB-EB-Audit-Playbook.pdf PDF
- Assessing Risks and Internal Controls ... Presentation
- Auditing with COBIT, COSO, and ISO C... PDF
- Control Testing Responsibility Guide.d... Document

I have reviewed the documents and noted several key themes and content areas related to internal controls and root cause analysis. Here's a proposed structure for developing your 28-hour training program, integrating examples and insights fr ↓ the uploaded files:

## Audie's Pro Tip: Always Verify Sources!



**Generative AI can produce 'hallucinations' which is completely fabricated, untrue data.**

- Think of AI as a starting point, but not the end point
- Require that the AI provide you links to citations and sources used
- Evaluate source credibility
- Use multiple GPTs to verify data

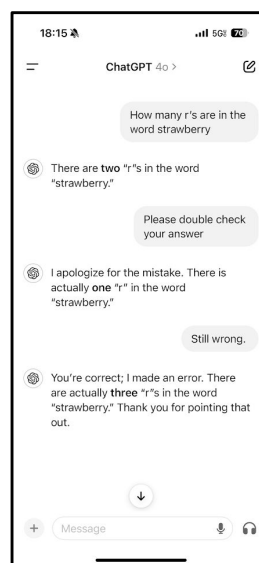
AUDIT  FORWARD

43

## Bonus Tip: Always Check Answers!



**Generative AI can also sometimes just be wrong – it's important to retain our human-brain critical thinking skills.**



AUDIT  FORWARD

44

# Audie's Pro Tip: Format for the AI



By uploading a spreadsheet for your AI model to fill in or use, remove extraneous formatting to keep it simple.

Procurement Detailed Testing		Attribute Testing	
Magical Artifacts Procurement Audit		Enchanted Enterprises	
		A Invoice amount equals PO amount	
		B Invoice amount equals payment amount	
		C Payment was within payment terms	
Per Population at Tab 11			
Selection #	Invoice Number	Vendor Name	Vendor ID
1	101f0cc0e7-43d8-4241-e050-5240971ca	Bessley Group	db7f785c-e04d-4442-4a4b-388552f46a3
2	24480805f-658b-4a8d-4042-402d229f9a0	Smith-Wing	e839448-1454-4345-9a7b-6e774d2d2402
3	17b13d4e-76d4-420e-8008-0322d4a4e6d	Smith-Wing and Thomas	20a4276-8022-477a-8a12-4690504174d
4	70a2525-75a4-474e-404a-03769d6b115	Barnes-Schwartz	17a2041-9015-4056-607a-e99a42b7a
5	45a4033-0679-4b47-4283-433093e9d9e	Corrie Carlson	14a2058-1a39-4021-4046-610363a972a
6	27a0201-6544-403d-4079-997213121e	Carroll Group	03070-9693-4038-4a4b-c243a4488
7	120a8bda-3 Benitez-R	Benitez-Rogers	9a47476-4a9-4040-4046-86a740d84
8	4a08897-7123-4041-4044-7725247b218	Smith-Nguyen	0a13136-100e-4031-4046-3a889232095
9	922a48d-30a4-404d-4047-6141640e032	Quarles Inc	8748a97-1116-4026-794-4022111787
10	27a08ba-9008-471-8a11-0a70a7e022	Stephenson LLC	77a8b78-67a3-4077-6a77-4809816a3
11	47a077b-77a0-4048-4048-20918a38a	Vanguard Records	65a8102-167f-4a27-3a16-50a40050515
12	29a4664-0052-4014-4021-2404a6462	Collins, Thomas and Williams	33a261e-40c2-405c-9068-6302715a771
13	84a070a-30e4-473a-471a-4046423295e	Morales, Bryant and Williams	511a148-1a38-405a-4046-8b78480762a
14	4a4a8ba-6a78-4022-18a2-7a141a105	House-Bobby	87a0443-1a7a-404d-404a-000012134
15	4a4a74-0566-437e-4a7b-404a3a0a50f	Roth, Flores and Warren	9a4b47c-42a-405c-9068-6302715a771
16	88a642-402-4028-8a60-878a42a0a4a	Dreene McGrath	0a13136-100e-4031-4046-3a889232095
17	42a8a41-474-404b-404b-01a104843a2	Johnson-Miller	89236a8-17b-404a-8027-610a030a3d3
18	4a4032a-424a-4044-8a74-1a1020a1e1	Gonzalez Harris	38a787a-405a-474a-404a-e6b3a3a3a3a
19	0a4032a-424a-4044-8a74-1a1020a1e1	Brown, Myers and Hernandez	0a4032a-424a-4044-8a74-1a1020a1e1
20	00214032-324a-4044-8a74-1a1020a1e1	Strong John	00a4032-424a-4044-8a74-1a1020a1e1
21	9a2721a-1a31-4046-8a78-1a717a181	Schaefer, Cooper and Donato	00a4032-424a-4044-8a74-1a1020a1e1
22	00a4032-424a-4044-8a74-1a1020a1e1	Cooper LLC	00a4032-424a-4044-8a74-1a1020a1e1
23	00a4032-424a-4044-8a74-1a1020a1e1	Quarles, Smith and Donato	00a4032-424a-4044-8a74-1a1020a1e1
24	4a4274a-0052-4014-4021-2404a6462	Orp Group	1517a7b-1008-4014-4021-2404a6462
25	4a4274a-0052-4014-4021-2404a6462	Orlando-Murphy and Smith	1517a7b-1008-4014-4021-2404a6462

Selection	Invoice Number	Vendor Name	Vendor ID	Total Invoice Amount	Invoice Date	Payment Terms	PO Number	PO Total	Payment Date	Payment Amount	A	B	C
1	101f0cc0e7-43d8-4241-e050-5240971ca	Bessley Group	db7f785c-e04d-4442-4a4b-388552f46a3	51,834	9/23/2023	Net 30	1482	51,834	10/23/2023	51,834	✓	✓	✓
2	24480805f-658b-4a8d-4042-402d229f9a0	Smith-Wing	e839448-1454-4345-9a7b-6e774d2d2402	53,589	8/1/2023	Net 30	2562	53,589	8/31/2023	53,589	✓	✓	✓
3	17b13d4e-76d4-420e-8008-0322d4a4e6d	Smith-Wing and Thomas	20a4276-8022-477a-8a12-4690504174d	93,200	9/25/2023	Net 30	2069	93,200	10/25/2023	93,000	✗	✓	✓
4	70a2525-75a4-474e-404a-03769d6b115	Barnes-Schwartz	17a2041-9015-4056-607a-e99a42b7a	63,349	1/3/2024	Net 30	2907	63,349	2/2/2024	63,349	✓	✓	✓
5	45a4033-0679-4b47-4283-433093e9d9e	Corrie Carlson	14a2058-1a39-4021-4046-610363a972a	64,312	1/4/2024	Net 30	1458	64,312	2/18/2024	64,312	✓	✓	✓
6	27a0201-6544-403d-4079-997213121e	Carroll Group	03070-9693-4038-4a4b-c243a4488	98,799	7/19/2024	Net 30	2234	98,799	8/18/2024	98,799	✓	✓	✓
7	120a8bda-3 Benitez-R	Benitez-Rogers	9a47476-4a9-4040-4046-86a740d84	99,637	#####	Net 30	2909	99,637	1/23/2024	99,637	✓	✓	✓
8	4a08897-7123-4041-4044-7725247b218	Smith-Nguyen	0a13136-100e-4031-4046-3a889232095	72,199	4/26/2024	Net 30	2428	72,199	6/9/2024	72,199	✓	✓	✓
9	922a48d-30a4-404d-4047-6141640e032	Quarles Inc	8748a97-1116-4026-794-4022111787	9,374	9/20/2023	Net 30	1373	9,374	10/20/2023	9,374	✓	✓	✓
10	27a08ba-9008-471-8a11-0a70a7e022	Stephenson LLC	77a8b78-67a3-4077-6a77-4809816a3	35,000	3/9/2024	Net 30	1297	35,000	4/9/2024	35,000	✓	✓	✓
11	47a077b-77a0-4048-4048-20918a38a	Vanguard Records	65a8102-167f-4a27-3a16-50a40050515	11,699	4/7/2024	Net 30	1172	11,699	5/7/2024	11,699	✓	✓	✓
12	29a4664-0052-4014-4021-2404a6462	Collins, Thomas and Williams	33a261e-40c2-405c-9068-6302715a771	69,556	8/21/2023	Net 30	1272	69,556	9/20/2023	69,556	✓	✓	✓
13	84a070a-30e4-473a-471a-4046423295e	Morales, Bryant and Williams	511a148-1a38-405a-4046-8b78480762a	43,704	10/1/2023	Net 30	2422	43,704	10/1/2023	43,704	✓	✓	✓
14	4a4a8ba-6a78-4022-18a2-7a141a105	House-Bobby	87a0443-1a7a-404d-404a-000012134	96,810	2/7/2024	Net 30	1174	96,810	3/9/2024	96,810	✓	✓	✓
15	4a4a74-0566-437e-4a7b-404a3a0a50f	Roth, Flores and Warren	9a4b47c-42a-405c-9068-6302715a771	85,925	6/11/2024	Net 30	2163	85,925	7/11/2024	85,925	✓	✓	✓
16	88a642-402-4028-8a60-878a42a0a4a	Dreene McGrath	0a13136-100e-4031-4046-3a889232095	69,676	2/20/2024	Net 30	1709	69,676	3/21/2024	69,676	✓	✓	✓
17	42a8a41-474-404b-404b-01a104843a2	Johnson-Miller	89236a8-17b-404a-8027-610a030a3d3	69,761	19/14/2023	Net 30	1929	69,761	10/14/2023	69,761	✓	✓	✓
18	4a4032a-424a-4044-8a74-1a1020a1e1	Brown, Myers and Hernandez	0a4032a-424a-4044-8a74-1a1020a1e1	88,790	4/22/2024	Net 30	2038	88,790	5/22/2024	88,790	✓	✓	✓
19	00214032-324a-4044-8a74-1a1020a1e1	Strong John	00a4032-424a-4044-8a74-1a1020a1e1	3,353	9/14/2023	Net 30	2419	3,353	10/14/2023	3,353	✓	✓	✓
20	00214032-324a-4044-8a74-1a1020a1e1	Strong John	00a4032-424a-4044-8a74-1a1020a1e1	69,219	8/22/2023	Net 30	2074	69,219	9/21/2023	69,219	✓	✓	✓
21	9a2721a-1a31-4046-8a78-1a717a181	Schaefer, Cooper and Donato	00a4032-424a-4044-8a74-1a1020a1e1	74,232	11/26/2023	Net 30	1103	74,232	12/26/2023	74,232	✓	✓	✓
22	00a4032-424a-4044-8a74-1a1020a1e1	Cooper LLC	00a4032-424a-4044-8a74-1a1020a1e1	92,731	4/12/2024	Net 30	2015	92,731	4/12/2024	92,731	✓	✓	✓
23	00a4032-424a-4044-8a74-1a1020a1e1	Quarles, Smith and Donato	00a4032-424a-4044-8a74-1a1020a1e1	74,451	10/1/2023	Net 30	1281	74,451	10/1/2023	74,451	✓	✓	✓
24	4a4274a-0052-4014-4021-2404a6462	Orp Group	1517a7b-1008-4014-4021-2404a6462	32,467	4/19/2024	Net 30	2509	32,467	4/19/2024	32,467	✓	✓	✓
25	4a4274a-0052-4014-4021-2404a6462	Orlando-Murphy and Smith	1517a7b-1008-4014-4021-2404a6462	96,880	7/25/2024	Net 30	1404	96,880	8/24/2024	96,880	✓	✓	✓

AUDIT FORWARD



# Prompt Example: Fieldwork - Testing

ChatGPT 5

Example: Enchanted Enterprises – Magical Artifacts Procurement Audit

- 1) Performed invoice testing and created a "ChatGPT friendly" tab.
- 2) Asked ChatGPT to summarize test results.

Selection	Invoice Number	Vendor Name	Vendor ID	Total Invoice Amount	Invoice Date	Payment Terms	PO Number	PO Total	Payment Date	Payment Amount	A	B	C
1	101f0cc0e7-43d8-4241-e050-5240971ca	Bessley Group	db7f785c-e04d-4442-4a4b-388552f46a3	51,834	9/23/2023	Net 30	1482	51,834	10/23/2023	51,834	✓	✓	✓
2	24480805f-658b-4a8d-4042-402d229f9a0	Smith-Wing	e839448-1454-4345-9a7b-6e774d2d2402	53,589	8/1/2023	Net 30	2562	53,589	8/31/2023	53,589	✓	✓	✓
3	17b13d4e-76d4-420e-8008-0322d4a4e6d	Smith-Wing and Thomas	20a4276-8022-477a-8a12-4690504174d	93,200	9/25/2023	Net 30	2069	93,200	10/25/2023	93,000	✗	✓	✓
4	70a2525-75a4-474e-404a-03769d6b115	Barnes-Schwartz	17a2041-9015-4056-607a-e99a42b7a	63,349	1/3/2024	Net 30	2907	63,349	2/2/2024	63,349	✓	✓	✓
5	45a4033-0679-4b47-4283-433093e9d9e	Corrie Carlson	14a2058-1a39-4021-4046-610363a972a	64,312	1/4/2024	Net 30	1458	64,312	2/18/2024	64,312	✓	✓	✓
6	27a0201-6544-403d-4079-997213121e	Carroll Group	03070-9693-4038-4a4b-c243a4488	98,799	7/19/2024	Net 30	2234	98,799	8/18/2024	98,799	✓	✓	✓
7	120a8bda-3 Benitez-R	Benitez-Rogers	9a47476-4a9-4040-4046-86a740d84	99,637	#####	Net 30	2909	99,637	1/23/2024	99,637	✓	✓	✓
8	4a08897-7123-4041-4044-7725247b218	Smith-Nguyen	0a13136-100e-4031-4046-3a889232095	72,199	4/26/2024	Net 30	2428	72,199	6/9/2024	72,199	✓	✓	✓
9	922a48d-30a4-404d-4047-6141640e032	Quarles Inc	8748a97-1116-4026-794-4022111787	9,374	9/20/2023	Net 30	1373	9,374	10/20/2023	9,374	✓	✓	✓
10	27a08ba-9008-471-8a11-0a70a7e022	Stephenson LLC	77a8b78-67a3-4077-6a77-4809816a3	35,000	3/9/2024	Net 30	1297	35,000	4/9/2024	35,000	✓	✓	✓
11	47a077b-77a0-4048-4048-20918a38a	Vanguard Records	65a8102-167f-4a27-3a16-50a40050515	11,699	4/7/2024	Net 30	1172	11,699	5/7/2024	11,699	✓	✓	✓
12	29a4664-0052-4014-4021-2404a6462	Collins, Thomas and Williams	33a261e-40c2-405c-9068-6302715a771	69,556	8/21/2023	Net 30	1272	69,556	9/20/2023	69,556	✓	✓	✓
13	84a070a-30e4-473a-471a-4046423295e	Morales, Bryant and Williams	511a148-1a38-405a-4046-8b78480762a	43,704	10/1/2023	Net 30	2422	43,704	10/1/2023	43,704	✓	✓	✓
14	4a4a8ba-6a78-4022-18a2-7a141a105	House-Bobby	87a0443-1a7a-404d-404a-000012134	96,810	2/7/2024	Net 30	1174	96,810	3/9/2024	96,810	✓	✓	✓
15	4a4a74-0566-437e-4a7b-404a3a0a50f	Roth, Flores and Warren	9a4b47c-42a-405c-9068-6302715a771	85,925	6/11/2024	Net 30	2163	85,925	7/11/2024	85,925	✓	✓	✓
16	88a642-402-4028-8a60-878a42a0a4a	Dreene McGrath	0a13136-100e-4031-4046-3a889232095	69,676	2/20/2024	Net 30	1709	69,676	3/21/2024	69,676	✓	✓	✓
17	42a8a41-474-404b-404b-01a104843a2	Johnson-Miller	89236a8-17b-404a-8027-610a030a3d3	69,761	19/14/2023	Net 30	1929	69,761	10/14/2023	69,761	✓	✓	✓
18	4a4032a-424a-4044-8a74-1a1020a1e1	Brown, Myers and Hernandez											

# Prompt Example: Fieldwork - Testing

ChatGPT 5

## Audit Testing Summary – Attribute Testing

Attribute testing was performed on a sample of 25 invoices to evaluate compliance with three defined attributes (A, B, and C). Each attribute was tested for every sample item, with results recorded as "P" (pass – no exceptions) or "T" (fail – exception noted).

### Results Overview

- **Attribute A** – Of 25 items tested, 23 passed and 2 failed (92% pass rate).
  - Exceptions: Invoice IDs 3, 21
- **Attribute B** – Of 25 items tested, 24 passed and 1 failed (96% pass rate).
  - Exception: Invoice ID 3
- **Attribute C** – Of 25 items tested, 22 passed and 3 failed (88% pass rate).
  - Exceptions: Invoice IDs 8, 17, 24

### Summary and Observations

Overall, compliance rates were high across all attributes, with pass rates ranging from 88% to 96%. The highest compliance was noted in Attribute B (96%), while Attribute C had the lowest compliance rate (88%). Exceptions were concentrated among a small number of invoices, with Invoice ID 3 failing two attributes (A and B). These exceptions should be reviewed to determine the underlying causes and whether additional control measures or process improvements are required.

AUDIT  FORWARD

47

# CoPilot's Turn – But First, a Hiccup...

Copilot

 Invoice Testing - Enchant...  
Excel

for the attached file, prepare an audit testing summary write-up of the results using tab "ChatGPT" This is attribute testing with three attributes A, B, and C defined in rows 28-30 and results in column L, M, N. A "P" means the attribute passed with no exceptions noted and a "T" means the attribute failed and an exception was noted.

It looks like the file you uploaded is too large for me to open directly. To help you with the audit testing summary, could you either:

1. Split the file into smaller parts and re-upload the relevant portion, especially the "ChatGPT" tab.
2. Copy and paste the data from rows 28-30 and columns L-N here in the chat.

Once I have that information, I'll prepare a clear and professional audit testing summary for you.

how is the file too large? it is 123kb.

You're absolutely right—123KB is a small file size, and it should normally be well within upload limits. Sometimes, files with complex formatting, embedded objects, or certain Excel features can trigger a "too large" message even if the actual size is small. It could also be a temporary glitch.

Here's what we can do to move forward:

- Try re-uploading the file—sometimes a second attempt works.
- Or, if it's quicker, just copy and paste the relevant data from the "ChatGPT" tab: rows 28-30 and columns L-N. That way I can generate the audit testing summary right away.

Let's get this wrapped up smoothly!

AUDIT  FORWARD

48

# Testing Summary – CoPilot’s Turn

Thanks, Elizabeth! Based on the data you shared, here's a summary of the audit testing results for selections 1–25, focusing on columns A (Invoice vs PO Match), B (Invoice vs Payment Match), and C (Payment Timeliness):

## Audit Testing Summary: Invoice Testing – Enchanted Enterprises

Test Area	Description	Results Summary
Invoice vs PO Match (A)	Verifies if the invoice amount matches the PO total.	✓ 23 Pass, ✗ 2 Fail
Invoice vs Payment Match (B)	Checks if the payment amount matches the invoice amount.	✓ 24 Pass, ✗ 1 Fail
Payment Timeliness (C)	Confirms if payment was made within the agreed Net 30 terms.	✓ 22 Pass, ✗ 3 Fail

### Exceptions Noted

- Invoice vs PO Mismatch**
  - Selection 3: Invoice = 93,220 vs PO = 91,220
  - Selection 21: Invoice = 74,232 vs PO = 70,200
- Invoice vs Payment Mismatch**
  - Selection 3: Invoice = 93,220 vs Payment = 93,000
- Late Payments**
  - Selection 8, 17, 24: Payment dates exceed Net 30 terms

AUDIT

## Audit Testing Summary: Enchanted Enterprises Invoice Review

As part of the audit procedures, a sample of 25 invoices from Enchanted Enterprises was tested for accuracy and compliance with internal controls. The testing focused on three key areas: consistency between invoice and purchase order amounts, accuracy of payment amounts, and timeliness of payments in accordance with agreed-upon terms.

### Invoice vs. Purchase Order Match

Out of the 25 selections tested, 23 invoices matched the corresponding purchase order totals. Two exceptions were noted:

- Selection 3 showed a discrepancy of \$2,000 between the invoice amount (\$93,220) and the PO total (\$91,220).
- Selection 21 had a mismatch of \$4,032, with the invoice amount (\$74,232) exceeding the PO total (\$70,200).

### Invoice vs. Payment Match

Payments were generally consistent with invoice amounts. 24 of the 25 selections matched exactly. One exception was identified:

- Selection 3 had a payment of \$93,000, which was \$220 less than the invoice amount of \$93,220.

### Payment Timeliness

Payments were made within the Net 30 terms for 22 of the 25 selections. Three invoices were paid late:

- Selection 8, 17, and 24 had payment dates that exceeded the 30-day term from the invoice date.

### Conclusion

Overall, the invoice testing results indicate strong compliance with internal controls, with only minor exceptions noted. These discrepancies should be reviewed to determine if they were due to clerical errors, timing issues, or require further investigation. No systemic issues were identified, and the majority of transactions were processed accurately and timely.

# AI is Sometimes More Art Than Science!

where is the file?

Here's the file with the 25 randomly highlighted rows:  
[Invoice Testing - Enchanted Enterprises - sampled.xlsx](#)

it says file not found

It sounds like the link broke when I sent it.  
 Here's the correct one — you should be able to click and download directly:

[Download updated Excel file](#)

Do you want me to also make a version where the highlighted rows are filtered to the top so you can see them quickly?

still not finding file

Got it — sounds like the link isn't working for you in this chat.  
 I'll re-save and give you a fresh download link now.

Here's the fresh link — this one should work:

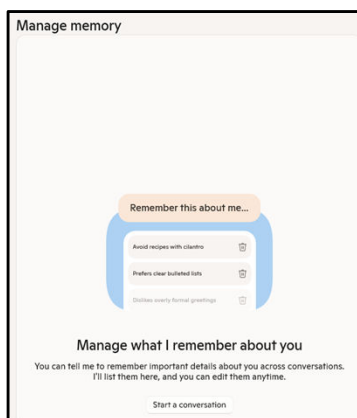
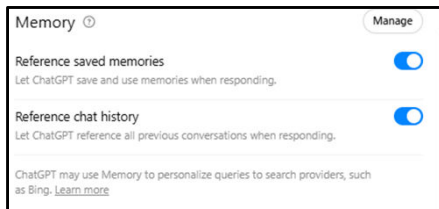
[Download updated Excel file](#)

AUDIT FORWARD

# Audie's Pro Tip: Remembering Data



ChatGPT and CoPilot will remember your specific conversations as “memories” if you ask it to!



AUDIT FORWARD

51

# Stay in Touch!



[elizabeth@auditforward.com](mailto:elizabeth@auditforward.com)



[www.auditforward.com](http://www.auditforward.com)



[www.linkedin.com/in/elizabethmcdowell/](https://www.linkedin.com/in/elizabethmcdowell/)



AUDIT FORWARD

52