

A Look Ahead: Emerging and Increasing Risks in 2024

January 23, 2024



The Institute of
Internal Auditors



With You Today



Kevin Black
Senior Manager, Risk Advisory
Services
BDO USA, P.C.



Clayton Hemphill
Senior Manager, Risk Advisory
Services
BDO USA, P.C.

Discussion Outline



IIA Risk in Focus: Emerging risks for 2024



Cybersecurity: Internal audit's role with the SEC's new cyber disclosure rules



Regulatory Change: Data analytics for compliance risks



Market Changes: Enhanced facilitated risk assessments



Climate Change: ESG and climate-related disclosures



Digital Disruption: Use of AI for internal auditing



**IIA Risk in Focus:
Emerging risks for 2024**

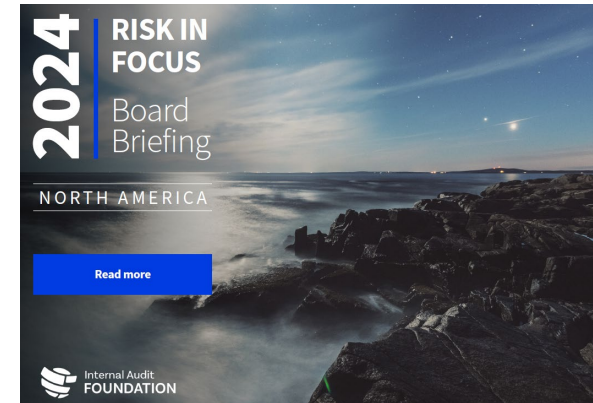
IIA Risk in Focus: Summary & Methodology

Summary:

- ▶ Risk in Focus provides practical, data-driven research to help internal auditors and their stakeholders understand today's risk environment and prepare audit plans for the year ahead.
- ▶ It is free and located here:
<https://www.theiia.org/riskinfocus>

Methodology:

- ▶ Survey of CAEs to identify current and emerging risks
- ▶ Top risks are used in follow-up roundtables and interviews
- ▶ 16 Risk Categories ranging from Business Continuity to Supply Chain



North America Research Participation

- 442 survey responses from CAEs and directors
- Participating countries: U.S. (385), Canada (57)
- 4 roundtables with 28 participants
- 9 in-depth interviews

IIA Risk in Focus: Results

Figure 1:

Current risk levels vs. future risk levels – North America

- Cybersecurity and human capital dominated the risk landscape for North America for 2024.
- In the next 3 years, digital disruption and climate change are the risks expected to increase the most.

■ Current risk
■ Future risk

What are the top 5 risks your organization currently faces?



What are the top 5 risks your organization will face 3 years from now?



Note: The IIA's Risk in Focus Global Survey, North America, n = 442. Percentage who ranked the area as one of their organization's top 5 highest risks.

IIA Risk in Focus: Key Risks



Cybersecurity

- ▶ Shortened reporting for cybersecurity incidents

Regulatory Change

- ▶ Use of data analytics for compliance risks

Market Changes

- ▶ Use of enhanced facilitated risk assessments

Climate Change

- ▶ Preparing for the new SEC ESG and Climate-Related Disclosures

Digital Disruption

- ▶ Use of AI for Internal Auditing



See *Understanding Enterprise and Operational Risk Management* (next session)



The Institute of
Internal Auditors
Elevating Impact





Cybersecurity:

**Internal audit's role with the SEC's new
cyber disclosure rules**

SEC Final Rules: Cybersecurity Risk Management, Strategy, Governance & Incident Disclosure

- Requires registrants to **disclose material cybersecurity incidents** in Form 8-K
- Requires **annual disclosures** regarding
 - **policies and procedures to identify and manage cybersecurity risk (106(b))**,
 - the **board's oversight (106(c))** of risks from cybersecurity threats, and
 - **management's role in assessing and managing material risks (106(c))** from cybersecurity threats.

Effectiveness:

- **Annual disclosures (Regulation S-K Item 106)**: All registrants must provide disclosures beginning with annual reports for FY ending on or after 12/15/2023.
- **Form 8-K incident disclosures (Item 1.05)**: All registrants other than smaller reporting companies (SRCs) must begin complying on the later of 90 days after publication in the Federal Register or December 18, 2023. SRCs will have an additional 180 days and must begin complying on the later of 270 days from the effective date of the rules or June 15, 2024. Must also tag disclosures in inline XBRL



Click [here](#) for Final SEC Rule

Click [here](#) for SEC Fact Sheet

Click [here](#) for BDO Bulletin

SEC Cybersecurity Risk Management, Strategy & Governance Final Rules

Item	Disclosure Requirement
New Regulation S-K Item 106(1) - Definitions	<ul style="list-style-type: none">• Cybersecurity incident: An unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.• Cybersecurity threat: Any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.• Information systems: Electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.
New Regulation S-K Item 106(b) - Risk Management and Strategy	Describe processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
New Regulation S-K Item 106(c) - Governance	Describe board's oversight of risks from cybersecurity threats: <ul style="list-style-type: none">• Identity any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats.• Processes by which the board or such committee is informed about such risks.
New Regulation S-K Item 106(c) - Governance	Describe management's role in assessing and managing material risks from cybersecurity threats, including (non-exclusive list): <ul style="list-style-type: none">• Whether and which management committees or positions are responsible for assessing and managing such risks, and the relevant expertise of such persons or members.• Processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents.• Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

SEC Cybersecurity Incident Disclosure Final Rules

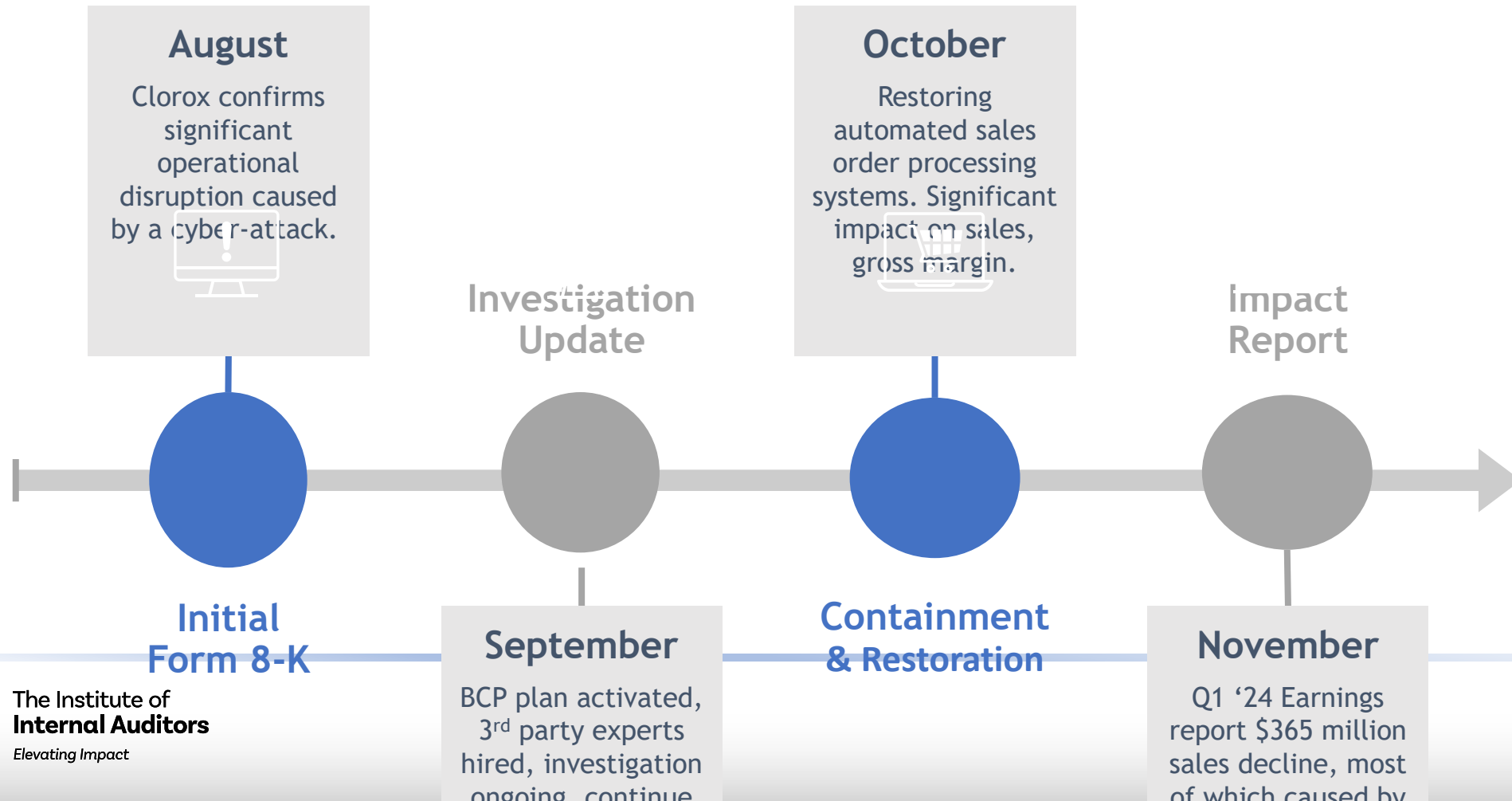
Item	Disclosure Requirement
New Form 8-K Item 1.05 - Material Cybersecurity Incidents	<ul style="list-style-type: none">• Disclose any cybersecurity incident they experience that is determined to be material and describe the material aspects of its:<ul style="list-style-type: none">◦ Nature, scope, and timing and impact or reasonably likely impact.• A materiality assessment must be performed on the incident taking into account quantitative and qualitative information such as impact on reputation, safety concerns, employee morale, regulatory and financial.• An Item 1.05 Form 8-K must be filed within four business days of determining an incident was material. A registrant may delay filing if the US Attorney General determines immediate disclosure would pose a substantial risk to national security or public safety.• Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.
Amended Form 20-F - Foreign Private Issuers	<ul style="list-style-type: none">• Describe the board's oversight of risks from cybersecurity threats.• Describe management's role in assessing and managing material risks from cybersecurity threats.
Amended Form 6-K - Foreign Private Issuers	<ul style="list-style-type: none">• Furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders.

SEC Cybersecurity Disclosure Rule Key Elements

Cybersecurity Incident Disclosures in Form 8-K

- Disclose cybersecurity incidents (An Item 1.05 Form 8-K must be filed) within **four business days** from the date they determine the incident(s) to be material
- An incident is material if “there is substantial likelihood that a reasonable shareholder would consider it important” or if it would have “substantially altered the ‘total mix’ of information made available from the perspective of a reasonable investor.”
- When disclosure is triggered, the registrant must disclose the material:
 - Aspects of the scope, nature, and timing of the cybersecurity incident
 - Impact or reasonably likely material impact on the registrant’s financial condition and results of operations

SEC Cybersecurity Disclosure Rule Case Study



Internal Audit Opportunities

Role/ Responsible for	Rule-relevant job Responsibility	Key Considerations: BEFORE AN INCIDENT	Key Considerations: DURING AN INCIDENT	Key Considerations: AFTER AN INCIDENT
Internal Audit	Evaluating compliance and reporting to the audit committee	Perform a Cybersecurity Maturity Assessment to evaluate the overall cybersecurity Governance, strategy, and readiness in the event of a breach.	Provide support and partner with IT, Finance, and Legal.	Perform an after-action audit of the response and recovery and determine if there are areas for improvement in response.

Cybersecurity Disclosures – Internal Audit Considerations

▶ Evaluate the Incident Response Plan

- Consider improving existing processes and procedures around the “identification and escalation” of incidents
- Consider performing a tabletop exercise
- Consider the timing of board communication in the Response Plan
- Consider having a third-party legal counsel review the updated plan
- Consider using the Crisis Management procedures from the Business Continuity plan to apply to an incident

▶ Evaluate the Incident Reporting Process (Disclosure)

- Consider using the Disclosure Committee to assess materiality based on quantitative & qualitative factors collectively
- Define the level of documentation required for materiality judgment by developing or updating Sarbanes-Oxley policies
- Consider developing a standard disclosure template for material breaches before a breach occurs, which can be updated
- Consider evaluating the scope of similar related breaches in materiality calculation
- Consider using similar SOX deficiency evaluation procedures for ICFR as a baseline or key input for Cybersecurity breach disclosures (e.g., approval for SEC Disclosures by CEO or CFO)

Internal Audit Learning Opportunities

- Project Spectrum - Cybersecurity Maturity Model Certification to do business with DoD <https://www.projectspectrum.io/#/courses-encite> - 14 courses designed to provide up-to-date cybersecurity compliance and policy best practices and educates users on relevant topics that can affect business risk management. Even assessment materials that can be used in walkthroughs
- Stanford - <https://online.stanford.edu/courses/xacs100-advanced-cybersecurity-program-preview>
- GA Cyber Center - <https://gacybercenter.pdx.catalog.canvaslms.com/> - Intro to cyber, ethical hacker courses, etc. Training provides awareness, outreach, and cyber security training to learners at all levels.
- Overall Cybersecurity rules and best practices - <https://www.nist.gov/cybersecurity>



**Regulatory Change:
Data analytics for compliance risks**

Regulatory Change: Robinson-Patman Act

RUM AND COKE: THE FTC TARGETS SOFT DRINKS AND ALCOHOL IN THE REVIVAL OF ROBINSON-PATMAN ACT ENFORCEMENT- WHAT'S NEXT?



Date: 16 June 2023

US Policy and Regulatory Alert

By: **Christopher S. Finnerty**, **Michael R. Murphy**, Taylor A. Listau, Jack S. Brodsky

While government enforcement of the Robinson-Patman Act (the Act) was all but forgotten for nearly two decades, the Federal Trade Commission (the FTC) announced a second investigation over potential price discrimination in just the last sixth months, this time against the largest alcohol distributor in the United States, Southern Glazer's Wine and Spirits (Southern Glazer's). This is just months after the FTC launched a similar investigation into Coca-Cola and PepsiCo.

Regulatory Change: Robinson-Patman Act

Robinson-Patman Act (RPA) of 1936 is a US federal law that prohibits anticompetitive practices.

The Federal Trade Commission is active in enforcement of RPA.



Price Discrimination

- ▶ Did the company charge different prices to different buyers for the same product without legitimate justification (cost, quantity)?

Promotional Allowances

- ▶ Did the company offer promotional allowances or services to certain buyers while excluding others (e.g. allowances are unavailable to all buyers on equal terms)?

Discounts and Rebates

- ▶ Did the company offer discounts or rebates to certain buyers but not to others without any legitimate justification?

Regulatory Change: RPA Risk Factors

Highly-competitive industries

- ▶ Fierce competition can lead companies to engage in discriminatory pricing practice to gain an unfair advantage

Significant market power

- ▶ Company can influence prices or control access to products

Complex pricing structures

- ▶ Offering different prices to different customer or providing discounts based on various factors - increase the likelihood of unintentional violations

Multiple distribution channels

- ▶ Selling products through multiple channels (e.g., direct sales, online, third-party retailers) may face challenges ensuring consistent pricing across all channels

Regulatory Change: False Claims Act

PRESS RELEASE

Oracle Agrees to Pay U.S. \$199.5 Million to Resolve False Claims Act Lawsuit

HUMANSCALE CORPORATION TO PAY UNITED STATES \$9 MILLION TO SETTLE ALLEGATIONS OF OVERCHARGING GOVERNMENT

GSA Contractor NetApp Agrees to Pay U.S. \$128 Million to Resolve Contract Fraud Allegations

Background

To sell to government agencies through the General Services Administration (GSA) Schedule Program*, a company must provide its most favored pricing to the GSA. Any pricing to any commercial customer lower than the GSA must be disclosed to the GSA. (Note: There are several exceptions to the Price Reduction Clause.)

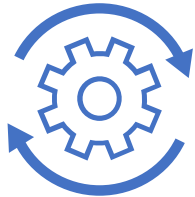
Price Reduction Clause Violation

- ▶ During your GSA agreement term, did the company offer better discounts to customer and were these pricing practices disclosed to the GSA?

Regulatory Change: Data Analytics Approach

Solution

- ▶ Conduct an analytics-focused, risk-based assessment of sales and pricing practices to identify potential price discrimination risks relating to the Robinson-Patman Act of 1936 (RPA) or the Anti-Price Discrimination Act or Price Reduction Clause of the GSA



0110101
1011010
1101001



Process
Understanding

Obtain Data

Confirm C&A

Identify
Outliers

Testing

Reporting





Market Changes:

Enhanced facilitated risk assessments

Market Changes: Typical Risk Assessment

Current Risk Assessment Approach:

1. Send surveys or interviews with risk universe
2. Review results and identify top risks
3. Send surveys for top risks
4. Review results and map top risks
5. Discuss results with executive management and board

Performed annually, time-consuming process with multiple meetings and last-minute changes by executives to modify risk ratings

Issues:



Process: Time-consuming (multiple meetings), Last minute executive changes without group approval



People: Leadership Power & Groupthink



Static: Cumbersome process to not update risks mid-year to address changing markets

Market Changes: Facilitated Session

Solution

Facilitated Sessions

- Leverage virtual, collaborative technology to transform the Risk Assessment process
- Real-time input of risk ratings with immediate results
- Able to target certain risks in the facilitate session
- Used of a trained facilitation coordinator to ensure all feedback is gathered and it is a collaborative experience
- Reduce manual spreadsheet calculations

Benefits

Executive alignment. Process and outcomes transparency drives alignment and buy-in; all responses and assessment results are captured real-time

Anonymity enables honest responses, providing real insight and higher quality data

The ability to gather consensus and clarity for shared understanding, while evaluating risks.

Instant vote results allows for immediate analysis; quickly identify areas of discord to drive discussion to reach agreement and alignment.

Save time by reducing time compiling notes, synthesizing data, etc.

Increase the number of participants through virtual participation



**Climate Change:
ESG and climate-related disclosures**

SEC Proposed Rules to Enhance and Standardize Climate-Related Disclosures

Summary:

- ▶ Applies to nearly all SEC registrants
 - No relief for Emerging Growth Companies (EGCs)
 - Limited relief for Smaller Reporting Companies (SRCs)
- ▶ Disclosures required in registration statements (IPOs, de-SPACs, mergers)
- ▶ As proposed, registrants may need to obtain information from equity method investees, vendors, suppliers, etc. to meet the requirements
- ▶ Certain disclosures subject to audit and management ICFR - consideration of policies, procedures and controls in place
 - Footnote disclosures - 1% based on absolute value
 - Disaggregated by negative and positive for physical and transition activities
 - Financial metrics
 - Expenses and capitalized costs
 - Attestation requirement for certain disclosures outside the footnotes (phased-in)
 - Assets and risk disclosed at the zip-code level

The SEC expects to release its final rule in April 2024.

Staff Guidance - Climate-Related Disclosure Sample Comment Letter

- ▶ [Sample Letter](#) sent to companies regarding climate change disclosures is still an excellent resource prior to final rules
 - Emphasizes the Commission-level [interpretive guidance](#) from 2010 on climate change disclosures and duty to disclose material information even if not expressly required by rules
 - Key areas of consideration
 - Climate-related disclosures in other reports, but not SEC filings
 - Impact of climate-related legislation, regulations, and international accords
 - Indirect consequences of regulation or business trends - e.g.
 - Decreased demand for goods w/significant greenhouse emissions
 - Increased competition to develop new/innovative products
 - Decreased demand for services related to carbon based energy sources
 - Physical impacts of climate change
 - Severity of weather and financial/operational impacts
 - Disclosures may appear in Business, Legal Proceedings, Risk Factors, and MD&A

Climate-Related Disclosures – Internal Audit Considerations

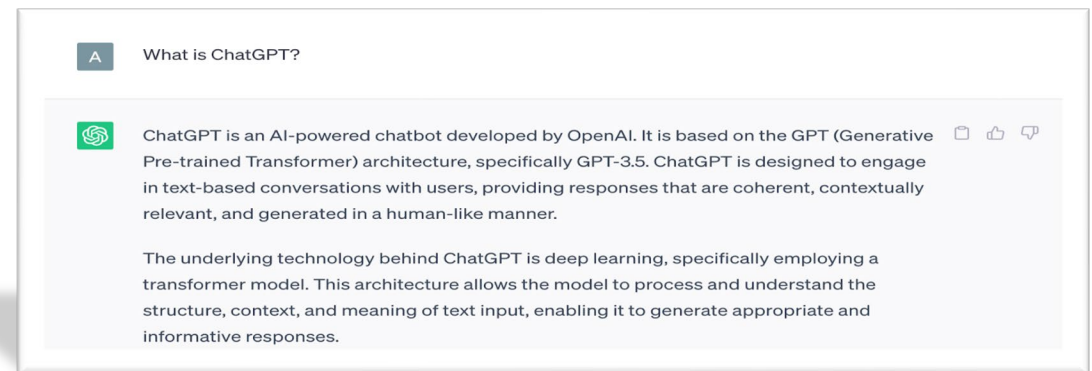
- Learn and educate key stakeholders about the ESG Reporting requirements that apply to your organization
- Perform an ESG Maturity Assessment to evaluate status, identify gaps, and propose a roadmap
 - Identify systems, processes, controls, key reports, management review controls to assess the quality of the data used for key metrics, assumptions, and models
- Evaluate the Data Used in Current Sustainability Reporting
 - Consider using Sarbanes-Oxley guidance regarding documentation, IPE (key reports/spreadsheets), and MRCs (management review controls) to assess the quality of the data used for key metrics, assumptions, and models
- Evaluate the incorporation of ESG in the Organization’s ERM Program
- Perform a Third-Party Risk Assessment to evaluate your current supplier’s ESG performance to identify any gaps, risks, or opportunities
- Evaluate whether the organization has the internal capabilities to manage an enterprise-wide ESG compliance project to implement the SEC Climate-Related Disclosures
- [BDO.com - Preparing for the Proposed SEC Climate Disclosure Rule](https://www.bdo.com/Preparing-for-the-Proposed-SEC-Climate-Disclosure-Rule)



**Digital Disruption:
Use of AI for internal auditing**

AI: Introduction

- Artificial intelligence (AI) is poised to further transform the internal audit function.
- The World Economic Forum (WEF) predicts new technologies like AI will [disrupt 85 million jobs globally between 2020 and 2025](#)—and create 97 million new roles.
- AI is a tool used to augment human skills and create efficiencies that enable auditors to spend more time on tasks that require their specialized expertise.
- This shift is ushering in a new era when human-machine partnerships boost productivity and deliver exceptional value.



AI: Getting Started with AI in Your Internal Audit Function

Educate

- Ensure team members understand AI's capabilities and implications to inform decision-making and set realistic expectations.

Identify Use Cases

- Tailor AI to address specific challenges or enhance processes within internal audit, focusing on areas with the most impact.

Prepare and build

- Establish strong data quality, security, governance, privacy, and responsible AI practices to safeguard the organization.

Enable and adopt

- Integrate AI into the internal audit workflow through training, resources, and dispelling myths to encourage adoption and champion the technology.

Go and grow


- Continuously revisit and refine AI systems as the internal audit function evolves to maintain relevance and deliver ongoing value.


AI: Practical Applications for Internal Audit

Use Case - Internal Audit Reporting

Potential Errors	ChatGPT Prompt Example
Grammar	Correct the grammar - [finding]
Passive voice	Make only active voice - [finding]
Too many words	More concise - [finding]

Passive Voice Example

 make only active voice - Remarks were made by a distraught Wheeler; protests were made by the students. A seat was gotten out of by one student. His desk was stood upon by him, and a vow was made by him that he would never write another active sentence. He was challenged to a duel.

 A distraught Wheeler made remarks; the students protested. One student got out of a seat. He stood upon his desk and made a vow that he would never write another active sentence. Someone challenged him to a duel.

To many words





A distraught Wheeler made remarks, provoking protests from the students. One student defiantly stood on his desk, vowing to never write another active sentence, and was subsequently challenged to a duel.

AI: Practical Applications for Internal Audit

Use Case - Internal Audit Reporting (Continued)

Potential Errors	ChatGPT Prompt Example
Assistance with Generating Ideas	What is the benefit of performing bank reconciliations?

Example of the above question

 Performing bank reconciliations offers several benefits: 

- 1. Accuracy:** Bank reconciliations help ensure the accuracy of financial records by comparing the company's internal records with the bank statement. Any discrepancies can be identified and resolved promptly.
- 2. Fraud detection:** Bank reconciliations can uncover unauthorized transactions or fraudulent activities, such as unauthorized withdrawals or forged checks. By comparing the bank statement with internal records, any suspicious transactions can be identified and investigated.
- 3. Error identification:** Bank reconciliations help identify errors in recording transactions, such as data entry mistakes or omissions. By reconciling the bank statement with internal records, any discrepancies can be traced back to their source and corrected.
- 4. Cash flow management:** Bank reconciliations provide an accurate picture of the company's cash position. By comparing the bank statement with internal records, businesses can identify any discrepancies and ensure that their cash balances are properly managed.
- 5. Financial reporting:** Bank reconciliations help ensure the accuracy of financial statements. By reconciling the bank statement with internal records, businesses can provide reliable financial information to stakeholders, such as investors, lenders, and regulators.

Overall, performing bank reconciliations helps maintain financial integrity, detect fraud, identify errors, manage cash flow effectively, and provide accurate financial reporting.

Overall Guidance


1. Keep the prompts concise and specific.
2. Use the responses as tool for ideas, but not a replacement for your creativity.
3. Edit and revise the text to make it in your style and your voice.
4. Do not input anything private or confidential.

AI: Practical Applications for Internal Audit

Use Case - Data Analytics

Types of Analysis	ChatGPT Prompt Example
Descriptive Analytics	Which balance sheet line items exceed 10% from year to year? [input balance sheet info]

Example of the above question - prompt

 Which balances sheet items exceeded + or - 10% from year to year?



NIKE, INC.
CONSOLIDATED BALANCE SHEETS
MAY 31,
(In millions) 2022 2021

ASSETS

Current assets:

Cash and equivalents \$ 8,574 \$ 9,889
Short-term investments 4,423 3,587
Accounts receivable, net 4,667 4,463
Inventories 8,420 6,854
Prepaid expenses and other current assets 2,129 1,498
Total current assets 28,213 26,291
Property, plant and equipment, net 4,791 4,904

Example of the above question - response

 Based on the provided balance sheet information, the following line items have exceeded a 10% change from year to year: 

1. Inventories: The value of inventories increased from \$6,854 million in 2021 to \$8,420 million in 2022, representing a percentage change of approximately 22.8%.
2. Prepaid expenses and other current assets: The value of prepaid expenses and other current assets increased from \$1,498 million in 2021 to \$2,129 million in 2022, representing a percentage change of approximately 42.1%.
3. Deferred income taxes and other assets: The value of deferred income taxes and other assets increased from \$2,921 million in 2021 to \$3,821 million in 2022, representing a percentage change of approximately 30.8%.
4. Long-term debt: The value of long-term debt decreased from \$9,413 million in 2021 to \$8,920 million in 2022, representing a percentage change of approximately -5.2%.


Please note that these calculations are based on the provided information, and it is recommended to refer to the company's official financial statements and disclosures for more accurate and detailed analysis.

AI: Practical Applications for Internal Audit

Use Case - Data Analytics (Continued)

Types of Analysis	ChatGPT Prompt Example
Predictive Analysis	Help me predict next year's revenue and net income based on historical data - [input statement of revenue info]

Example of the above question - prompt

 Hello Chat GPT! Could you help us predict next year's revenue and net income based on historical sales data - CONSOLIDATED STATEMENTS OF INCOME YEAR ENDED MAY 31, (In millions, except per share data) 2022 2021 2020
Revenues \$ 46,710 \$ 44,538 \$ 37,403
Cost of sales 25,231 24,576 21,162
Gross profit 21,479 19,962 16,241
Demand creation expense 3,850 3,114 3,592
Operating overhead expense 10,954 9,911 9,534
Total selling and administrative expense 14,804 13,025 13,126
Interest expense (income), net 205 262 89
Other (income) expense, net (181) 14 139
Income before income taxes 6,651 6,661 2,887
Income tax expense 605 934 348
NET INCOME \$ 6,046 \$ 5,727 \$ 2,539

Example of the above question - response

Next year's revenue = \$50,855 million

To predict next year's net income, we can use the historical net income margin as a percentage of revenue. The net income margin is calculated by dividing net income by revenue.

Net income margin for 2022 = Net income for 2022 / Revenue for 2022

Net income margin for 2022 = \$6,046 million / \$46,710 million

Net income margin for 2022 = 0.129 or 12.9%

Next year's net income can be estimated by multiplying the predicted revenue by the net income margin:

Next year's net income = Next year's revenue * Net income margin

Next year's net income = \$50,855 million * 0.129

Next year's net income = \$6,561 million

Please note that this is a simplified calculation based on historical data and assumptions. Actual revenue and net income can be influenced by various factors such as market conditions, competition, operational efficiency, and company-specific factors. It is recommended to consider additional information and consult with financial analysts or industry experts for a more accurate prediction.

AI: Practical Applications for Internal Audit

Use Case - Data Analytics (Continued)

Fraud Testing Examples	ChatGPT Prompt Example
Duplicates	Any duplicate data? [input invoice data from spreadsheet]
Any fraud - general question	Any fraud in this data? [input invoice data from spreadsheet]

Example of the above question - prompt

```
Do any duplicate data? Row ID Order ID Order Date Ship Date Ship Mode Customer ID Customer Name Segment
Country City State Postal Code Region Product ID Category Sub-Category Product Name Sales
Quantity Discount Profit
1 CA-2016-152156 11/8/2016 11/11/2016 Second Class CG-12520 Claire Gute Consumer United States
Henderson Kentucky 42420 South FUR-BO-10001798 Furniture Bookcases Bush Somerset Collection Bookcase
261.96 2 0 41.9136
2 CA-2016-152156 11/8/2016 11/11/2016 Second Class CG-12520 Claire Gute Consumer United States
```

Example of the above questions - response

Yes, there is duplicate data in the provided dataset. Rows 1 and 2 have the same Order ID (CA-2016-152156) and other corresponding information, indicating a duplicate entry. Similarly, rows 5 and 6, as well as rows 14 and 15, have the same Order ID, suggesting duplicate data entries.

Based on the provided data, there are a few potential instances of fraud:

1. Row 4: The order has a negative profit of -383.031, indicating a potential loss on the transaction. This could be a result of fraudulent activity or an error in the data.
2. Row 15:...

These instances of negative profits could be indicators of fraudulent activities, but further investigation would be required to confirm if they are indeed fraudulent or if there are other explanations for the negative profits.

AI: Practical Applications for Internal Audit

Use Case - Narratives & Summaries of Meetings

Use an AI assistance application as a meeting assistant:

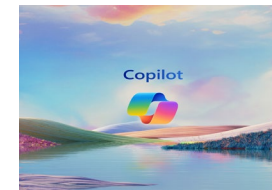
1. Join a video call on Zoom, Microsoft Teams, or Google Meet
2. Click to highlight important moments during the call
3. Application transcribes the call and makes highlights for your clicked moments
4. After the call, you instantly access the recording, transcription, and auto-generated summaries
5. Easily share highlights and summaries wherever you need them - docs, emails, CRM, task managers.

Note: Obtain IT approval before installing applications. If an application is not available, can load notes into Chat GPT to summarize the notes into a narrative.

FATHOM 



Otter.ai




Grain

AI: More Information

The screenshot shows a BDO USA website page. At the top right, there are navigation links for Services, Industries, Insights, and About Us, along with a search bar. The BDO USA logo is in the top left. Below the logo, there are breadcrumb links: Home < Insights < Assurance. The main heading of the article is 'The Internal Auditor's Artificial Intelligence Strategy Playbook'. Below the heading, there is a sub-heading: 'Exploring AI for Internal Audit' and a section titled 'Table of Contents:' with three links: 'Introduction', 'The ABCs of AI – A Glossary', and 'Getting Started with AI in Your Internal Audit Function'. On the right side of the article, there is a box containing the word 'ARTICLE', the date 'November 06, 2023', and the author information: 'BY: Jamey Loupe, Managing Director, Data Risk & Controls, Risk Advisory Services, BDO USA; Savvas Georgopoulos, Managing Director, Innovation & Analytics, Risk Advisory Services, BDO USA; Kirstie Tiernan, Practice Leader, Data Analytics, BDO Digital'.

[The Internal Auditor's Artificial Intelligence Strategy Playbook](#)

Questions

