



# SOX Compliance in 2024

## *What's New and What's Next*

March 27, 2024



# Today's Speakers



**Maggie Berkeley**  
Principal

Maggie focuses on process, risk and controls methodologies, including leading RSM's Risk Consulting SOX methodology team. She has over 16 years of experience leading engagements focused on assisting clients in preparing for and implementing control improvements required by the Sarbanes-Oxley Act (SOX).



**Anthony DeCandido**  
Partner

As a lead advisor within RSM's ESG advisory practice, Anthony guides companies and boards of directors through ESG strategy development, data collection, and reporting and communications.



**Dietz Ellis**  
Director, Security and  
Privacy Risk Consulting

Dietz serves as the national security and privacy leader with over 18 years of experience assisting organizations in solving their business and information technology-related challenges and improving their cybersecurity, compliance and privacy capabilities.



**Emma Wieczorek**  
Director

Emma focuses on process, risk and controls methodologies. She has over 11 years of experience assisting companies in the life sciences and technology industries prepare and implement control improvements required by the Sarbanes-Oxley Act (SOX).

# Agenda

## 01 Introductions & Course Objectives

---

## 02 SOX Trends

---

- SOX Focus Areas
  - Material Weaknesses & Contributing Factors
  - Regulatory Update – SEC & PCAOB
- 

## 03 SEC Final Rule on Climate Disclosures

---

- Key Changes
  - Governance & Risk Management
  - GHG Emissions Metrics
  - Targets & Goals
  - Compliance
  - Next Steps
- 

## 04 Cybersecurity Update

---

- SEC Cybersecurity Disclosure Rule Framework
- Cybersecurity Control Considerations
- Common Themes in SEC Rule Adoption

# Course Objectives

01

Know the latest requirements for internal controls over financial reporting

02

Understand current trends and how to incorporate related changes into a SOX compliance program

03

Gain insights related to evolving SOX compliance guidance



# SOX Trends

Focus Areas, Common Material Weaknesses and Contributing Factors,  
SEC and PCAOB Update

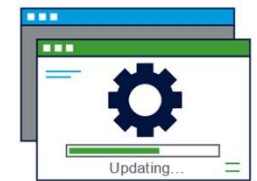
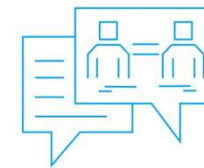
# Continued SOX Focus Areas – Top 10



# Increased Attention Around....

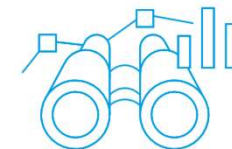
## Information Provided by the Entity (“IPE”)

- Increased expectations around documentation of procedures
- Confirm completeness and accuracy of key report inventory
- Emphasis on validating the true source system/application
- Adapting procedures when IPE is produced by an application/tool that is not in-scope



## SOC 1 Reports

- Identifying relevant sub-service providers
- Assessing the impact of the period covered in relation to fiscal year-end
- Confirming what automation and key reports are covered under the scope of the SOC 1 report
- Proactively performing these assessments as part of scoping & planning phase



# Increase in Material Weaknesses

Common MWs we've seen include:

Segregation of Duties

IT General Controls

Technical Accounting Assessments



# Frequent Contributing Factors in Material Weaknesses

## Improper technology implementation or integration

What can you do....

Proactively integrate an assessment of control impact of system implementations and/or updates

## Inadequate use of tools to avoid manual error

What can you do....

Reassess your controls and procedures to identify where automation can be effectively leveraged

## Poor accounting organization structure

What can you do....

Reassess roles and responsibilities in your organization against current control environment to ensure key activities are performed at appropriate levels and workflow is manageable

## Ineffective segregation of duties (SOD)

What can you do....

Incorporate performance of SOD analysis/refresh into periodic user access reviews

# Regulatory Update

What's New with the SEC and PCAOB?



2024 inspections will focus on identifying methods for improving audit quality

Roundtable to discuss NOCLAR proposal

PCAOB named new Director of Office of Internal Oversight and Performance Assurance ([\\*full article here](#))

2023 was a **record setting year** for standard setting and rulemaking, with **four proposals** in 2023 with **excepted 2024 adoption**

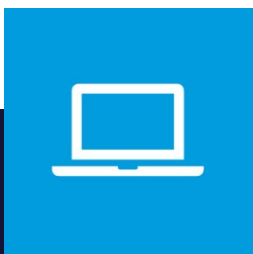
**2023**



Four proposals expected in 2024. Focus areas include **attestation, going concern, firm and engagement performance metrics, and substantive analytical procedures**

**2024**

# Regulatory Update – Key Reminders



- SEC adopts rule on cyber disclosures
  - On July 26, 2023, new rule was adopted to enhance and standardize disclosures around cybersecurity risk management strategy and material cyber incidents
  - New rule is effective for Form 10-K and Form 20-F disclosures for fiscal years ending on or after December 15, 2023
  - <https://www.sec.gov/news/press-release/2023-139>



- SEC adopts rule to standardize climate-related disclosures for investors
  - Disclosure of climate-related risks that have material impact on business strategy, results of operations, or financial condition;
  - Disclosure of actual and potential material impacts of identified risks on the business and consolidated financial statements
  - Disclosure of capitalized costs, expenditures expenses, charges, and losses incurred due to severe weather events and related to carbon offsets and renewable energy credits or certificates (RECs)
  - <https://www.sec.gov/news/press-release/2024-31>



- SEC adopts rule to enhance investor protections against SPACs, shell companies, and projections
- Enhancements in three areas: disclosure, use of projections and issuer obligations
- Requires enhanced disclosures around conflicts of interest, SPAC sponsor compensation, and dilution
- <https://www.sec.gov/news/press-release/2024-8>



# SEC Final Rule on Climate Disclosures

Key Changes, Governance, Risk Management, GHG Emissions Metrics, Targets & Goals, Compliance, and Next Steps

# SEC Climate-Related Disclosure: Final Rule

In an open meeting on Wednesday, March 6, 2024, the Securities and Exchange Commission (“SEC”) approved in a 3-2 vote a **Final Rule on climate disclosures** that will “**require registrants to provide certain climate-related information** in their registration statements and annual reports”.

The Final Rule will be effective **60 days** after its publication in the Federal Register. Key areas include:



New disclosures of greenhouse gas (GHG) emissions



Governance and oversight of material climate-related risks



Impact of climate risks on the company’s strategy, business model, and outlook, risk management processes for climate-related risks



Climate targets and goals



*The requirements are subject to certain materiality thresholds, registrant applicability, and an adoption phase-in timetable.*

# Key Changes from Proposed Rule

The Final Rule differs from the proposed rule (Proposed Rule) issued almost two years prior in applicability

## Greenhouse Gas (GHG) emissions disclosures

- Allowing registrants to determine the organizational boundaries which may differ from those used for financial reporting purposes
- Elimination of the requirement to disclose Scope 3 GHG emissions
- Exemption of non-accelerated filers, smaller reporting companies (SRC) and emerging growth companies (EGC) from compliance with the required GHG emissions disclosures
- Extending the adoption timeline for GHG emissions disclosures and related assurance requirements.

## Financial statement disclosures

- Reducing financial statement disclosures by eliminating certain metrics and narrowing the scope of the requirements for other metrics.
- Eliminating the requirement to disclose material changes to climate-related disclosures in a registrant's quarterly reporting (e.g., Form 10Q)
- Removing the requirement to disclose the impact of weather events, natural conditions, and transition activities.
- Requiring financial statement disclosures only for the registrant's most recent fiscal year.

## Disclosures outside of the financial statements other than GHG emissions-related items

- Exempting immaterial items from certain climate related disclosures, including the impact of climate-related risks, scenario analysis and the internal carbon price
- Accepting a less rigid approach to areas such as disclosures of climate-related risk, board oversight, and risk management

# Governance & Risk Management

## Governance

The Final Rule requires disclosures about a registrant's board of director's governance and, It also requires governance disclosures related to management's role in assessing and managing material climate-related risks.

### Board Oversight

- Identification of the board or committee responsible and the process by which the board is informed of such risks
- If a target goal or transition plan is otherwise disclosed, the governance disclosure must include whether and how the board oversees the progress against the target, goal or transition plan

### Management Oversight

- The identity of management positions or committees responsible for assessing and managing climate-related risks and the relevant expertise of such position holders or members
- The process by which such positions or committees are informed about and monitor climate-related risks

## Risk Management

Registrants are required to disclose their processes for identifying, assessing and managing climate-related risks and whether those risks are integrated into the registrant's overall risk management system or processes



# GHG Emissions Metrics, Targets & Goals





## GHG Emissions Metrics

The Final Rule requires Scope 1 (direct GHG emissions from operations owned or controlled by the registrant) and Scope 2 (indirect GHG emissions from the generation of purchased or acquired electricity, steam, heat, or cooling that is consumed by operations owned or controlled by the registrant) emissions to be separately disclosed, on a gross basis, before consideration of any offsets.

Registrants must also disclose the relevant protocol or standard utilized to report the GHG emissions, including the methodology and significant inputs and assumptions used in the calculation.

## Targets & Goals

Registrants are required to disclose:

-  Description of the activities to be performed and how the targets and goals will be met
-  Scope and timing of the related activities, and where applicable, the baseline being measured against
-  Impact of carbon offsets or RECs if they are expected to be a material part of the plan for achieving these climate related targets or goals.
-  Annual updates on the progress toward the targets or goals



# Compliance Dates and Phase-In Periods

The following table summarizes the Final Rule and includes a phased-in compliance schedule based on a registrant's filing status and the type of information or reporting.

| Compliance Dates                               |   |   |                                   |   |          |
|--|---|---|-----------------------------------|---|----------|
| Type of registrant                             | Financial statement disclosures and other disclosures except material expenditures and impacts and GHG emission | Disclosures about material expenditures and impacts | Scope 1 and Scope 2 GHG emissions | Attestation on Scope 1 and Scope 2 GHG emission disclosures   | XBRL     |
| Large accelerated filers                       | FYB 2025  | FYB 2026  | FYB 2026                          | Limited assurance: FYB 2026<br>Reasonable assurance: FYB 2033 | FYB 2026 |
| Accelerated filers (other than SRC's and ECGs) | FYB 2026  | FYB 2027  | FYB 2028                          | Limited assurance: FYB 2031<br>Reasonable assurance: N/A      | FYB 2026 |
| SRCs, ECGs and non-accelerated filers          | FYB 2027  | FYB 2028  | N/A                               | N/A   | FYB 2027 |



# Next Steps

Final Rule **significantly increases** the disclosure requirements for public registrants, both within and outside the financial statements.

Registrants should **engage the relevant stakeholders** and **develop a plan to ensure compliance** with the Final Rule. Such initial plan should include, among other things:



## Determine Applicability

Take a broad view of all new regulations including the Final Rule to determine the scope of required sustainability reporting applicable to the registrant.



## Update Governance Protocols

Communicate the key provisions of the Final Rule to department heads and management, and the board of directors, and begin to build capacity within the organization. Define board and management roles and responsibilities and ensure that they are reflected in formalized documents.



## Document the Current State

Gather a full list of all climate related information that has been organized or disclosed and document the related sources of data, processes, and controls over such information.



## Identify Disclosure and Control Gaps

Identify and assess any identified or potential gaps related to data, controls, and reporting, including disclosures both in and outside the financial statements.



# Cyber Security Update

# SEC Cybersecurity Disclosure Rule Framework

## DOMAINS



### 1. Security IT Governance

*Define Board's oversight of cybersecurity risks and management's role in assessing and managing material risks from those threats*



### 2. Security Risk Management

*Formalize and execute processes for assessing, identifying and managing material risks from cybersecurity threats*



### 3. Security Monitoring

*Establish the governance and capability to evaluate, identify, and classify cyber events*



### 4. Incident Response

*Develop mechanisms to escalate and classify "material" events and perform required disclosures*

## KEY ACTIVITIES

Establish cyber governance structure

Implement processes to manage and report cybersecurity risk

Define Cybersecurity Materials for disclosure

Perform periodic (annual) company-wide cybersecurity risk assessments

Establish monitoring governance and formalized policies & procedures

Deploy capabilities to monitor, alert, and prioritize potential cyber events

Perform recurring training and monitoring of performance

Document processes used to evaluate, prioritize, and escalate cyber events

Perform recurring "tabletop" evaluation of cyber incident response plan

Define process to determine materiality and steps for required disclosures

### Legend

Needed to adhere to SEC requirements

Supports but not explicitly needed to adhere to SEC requirements

# Cybersecurity Control Considerations



## Stakeholder Identification

Determine IT / cybersecurity personnel (control owners) need to conduct audit



## Determine Control Scope

Consider controls providing the most mitigation and/or considered compensating controls



## Conduct Testing

Perform control testing follow company and/or professional services' methodologies



## Reporting & 10-K Consideration

Report internally only while determining if control testing should be disclosed in the 10-K

To help gain confidence that cybersecurity capabilities are consistently in place and effective, organizations are considering smaller sets of cybersecurity controls for testing. The nature and objective of these controls vary between companies, the below are just examples.

| SEC Requirement          | Control Objective   |
|--------------------------|---|
| Security IT Governance   | Cybersecurity policies have been established to provide for the overall direction of information security of implemented applications, databases, network and communication devices, and system software. |
| Security Risk Management | The organization applies results from risk management assessments to continuously track relevant issues and risks, resolve identified incidents in a timely manner, and develop a threat matrix.          |
| Security Monitoring      | Security operations analysts monitor and log security activity and security threats on endpoints while reporting identified violations to personnel responsible for cybersecurity.                        |
| Incident Response        | Management has formalized procedures to timely assess and document materiality of incidents to determine whether the incident has or will have a material impact.   |
| Incident Response        | Management has formalized procedures to disclose incidents that have a material or reasonably likely material impact within four business days after the incident is determined to be material.           |

# Common Themes in SEC Rule Adoption

Large discrepancy in capabilities between newly public versus more established and mature companies; the level of effort for rule adoption varies significantly

Small companies have sparse IT / security teams and have considered managed security service providers (MSSP) to enable or supplement capabilities at a lower cost point than net new headcount

Difficulty in striking the right balance of transparency and factual capabilities within 10-Ks

Companies struggle with materiality determination for cybersecurity risks for inclusion within 10-Ks and as a trigger to file an 8-K

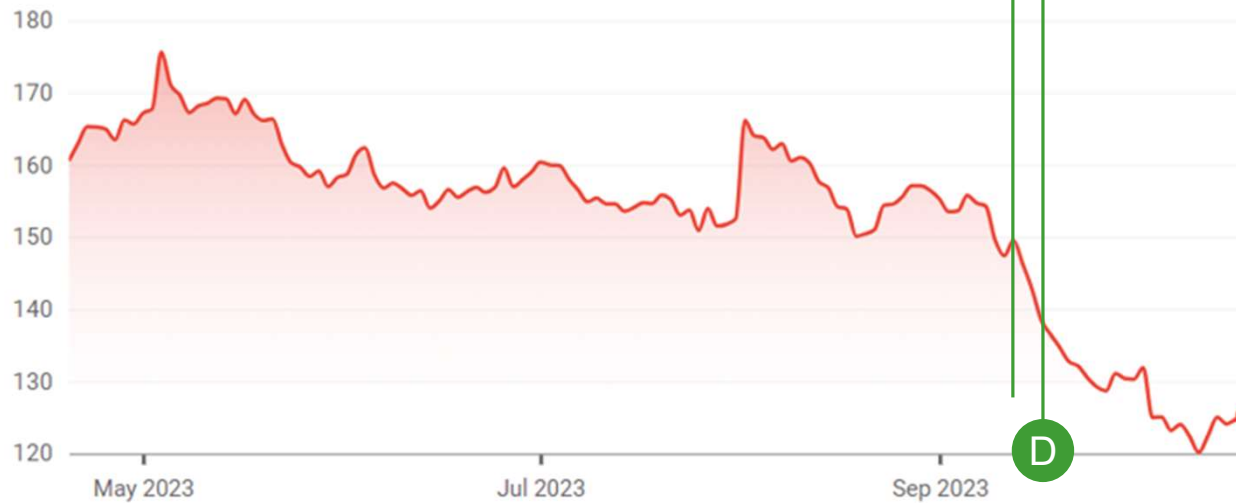
There has been inconsistencies in 8-K filings, in particular the articulation of how cybersecurity incidents have or could materially impact business operations and financials

# Disclosure Impact

**\$125.13** ↓ 22.06% -35.41 6M

Oct 19, 11:39:42 AM UTC-4 · USD · NYSE · Disclaimer

1D 5D 1M 6M YTD 1Y 5Y MAX



Time To Detection

Impact Analysis

4 Day Disclosure

A

1/1/2024

B

C

1/4/2024

D

# Questions





Thank you





## THE POWER OF BEING UNDERSTOOD ASSURANCE | TAX | CONSULTING

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute assurance, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent assurance, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit [rsmus.com/aboutus](https://rsmus.com/aboutus) for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.

© 2024 RSM US LLP. All Rights Reserved.