INTERNAL AUDIT'S ROLE IN CYBER SECURITY & ESG DISCLOSURE REQUIREMENTS

AGENDA

- CYBER SECURITY DISCLOSURE REQUIREMENTS AND IA'S ROLE
- ESG DISCLOSURE REQUIREMENTS AND IA'S ROLE
- Q&A

SEC CYBER SECURITY DISCLOSURE: BACKGROUND

On July 26, 2023, the Securities and Exchange Commission (SEC) issued a final rule requiring registrants to provide enhanced and standardized disclosures regarding cyber security, risk management, strategy, governance and incidents

Why

- Timely investor access to cyber events impacting investments
- Foster reporting consistency across registrants
- Enhance investor confidence around cyber security landscape of investments

What

- Disclosure of material cyber security incidents
- Disclosure of identification, assessment, and handling of cyber security incidents
- Disclosure around management role in cyber security risk
- Disclosure of the Board of Directors role in oversight of cyber security risk

Who

- Public companies subject to 1934 Securities Act including:
- Emerging Growth Company's (EGCs)
- Smaller Reporting Companies (SRCs)
- Foreign Private Issuers (FPIs)

SEC REQUIREMENT SUMMARY

- The SEC has issued new guidelines for public companies regarding the reporting of cybersecurity incidents.
- Companies are required to disclose **material** cybersecurity incidents within **4 days** of determining that a materially-significant incident has occurred.
- Intent is to ensure transparency for investors and stakeholders and prevent insider trading based on non-public information about such incidents.
- Disclosures must include the nature and scope of the incident, its impact on operations, and the company's response.
- Companies must provide updates on material developments related to the incident in subsequent filings.
- The SEC **does not** provide definitive guidelines on what constitutes a material incident; it is up to each company to determine that based on the incident and the company's methodology in assessing such incidents.

KEY DEFINITIONS FROM SEC

SEC has defined the following in the new guidance:

Cyber Security Incident

- an unauthorized occurrence 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.

Cyber Security Threat

- any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.

Information Systems

- 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.

UNDERSTANDING YOUR CYBER LANDSCAPE

- In understanding and evaluating the Company's cyber landscape, the following should be considered by IA:
  - The Company's
    - Business information network
    - Cloud presence
    - Operations technology network
    - AI, social media and other cyber interactive policies/safeguards
  - Any data owned or managed by the Company that could lead to a potential negative impact to the Company if disclosed inappropriately
    - General Data Protection Regulation (GDPR) impacts depending on your operations
  - The Company's applicable cyber incident types and their potential sources
    - Ransomware
    - Malware
    - Data Leakage
    - Denial of Service

HOW ARE CYBER INCIDENTS IDENTIFIED & TRACKED?

- Help Desk: Are information security events reported to the IT Service Help Desk? If so, how are they managed?
- IT Security Operations Centers (SOCs): Does the Company rely on third-party SOC service for endpoint monitoring? If so, how are those monitored and managed? Is there a reporting process in place with each service for urgent incidents?
- Operational Incidents: How are these identified? Hotline/Email? How are they reported and managed? What, who, how, where?
- Vendor Notifications: Are there processes to identify and address critical vendors/suppliers who are part of the Company's Supply Chain that could also impact the Company? How are these identified, reported, and managed?
- Cyber Incident Team/Person: Is there an IT Incident Response Team or Designated Person? If so, what are their responsibilities? What methodology do they utilize to evaluate and report incidents?

SEVERITY ASSESSMENT METHODOLOGY

Is there an operational assessment and materiality assessment methodology in place?

Assessing operational impact severity level is based on fundamental questions:

- What has happened or is happening?
- How bad could this be?
- What is the scope? Global? Regional? Country Specific? Operations Specific?
- Which system(s) and/or user(s) could be impacted?
- How likely is the worst possible scenario to occur?
- How likely are other, lesser severity scenarios to occur?
- Do we have mitigating plans or controls in place for this?
- If so, are they functioning? Have they been tested?

Assessing materiality should be based on current practice of materiality assessment by the company and Accounting should be involved for financial impacts.

An assessment framework should be utilized with defined and designated levels such as low, medium, high, severe etc.

ESCALATION PROCESS?

Has an escalation process been defined?

What are the escalation steps?

Who is part of escalation?

When is it triggered?

How is it triggered?

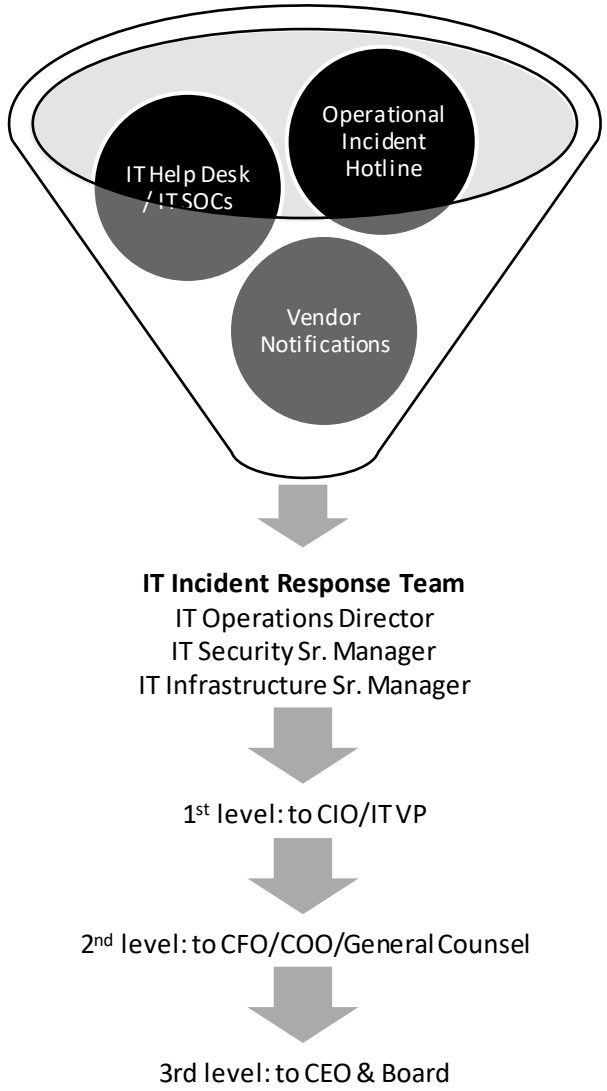
Who is in charge of the escalation process?

What methodology do they utilize to escalate?

Is there a documented playbook?

What are expected remediation paths?

Example Escalation Path



SEC ESG REQUIREMENTS: BACKGROUND

On March 6, 2024, the Securities and Exchange Commission (SEC) adopted the final climate rule.

SEC considered over 20K letters in drafting the final rule.

Another term: Task Force on Climate-Related Financial Disclosures (TCFD)

Why

- Increasingly important factor for investors
- Consistency, comparability and reliability across registrants
- Enhance investor confidence

What

- Material climate-related risks and their material impacts, including those on strategy, business model and outlook
- Governance
- Risk Management
- Material targets and goals (including those related to the reduction of greenhouse gas (GHG) emissions)
- Scope 1 & Scope 2 GHG Emissions

Who

- Public companies subject to 1934 Securities Act including:
- Emerging Growth Company's (EGCs)
- Smaller Reporting Companies (SRCs)
- Foreign Private Issuers (FPIs)

SEC REQUIREMENT SUMMARY & TIMELINE

- Required S-K disclosures should be based on **materiality**, evaluated using existing federal securities law framework (consistent with other SEC rules and regulations)

Registrant Type	Disclosures		Assurance		Electronic Tagging
	Disclosures other than GHG Emissions	Scope 1 & Scope 2 GHG Emissions	Limited Assurance	Reasonable Assurance	
Large Accelerate Filers	FYB 2025	FYB 2026	FYB 2029	FYB 2033	FYB 2026
Accelerated Filers	FYB 2026	FYB 2028	FYB 2031	N/A	FYB 2026
SRCs, EGCs, and non-accelerated filers	FYB 2027	N/A	N/A	N/A	FYB 2027

CLIMATE RELATED RISKS & THEIR IMPACTS

Companies will be required to describe, among other items:

- Material climate-related risks,
- Actual and potential material impacts of each risk,
- Material expenditures and material impacts on financial estimates and assumptions that directly result from activities to mitigate or adapt to the risks

Additional disclosures will be required if the Company:

- Has adopted a plan to manage a material transition risk
- Uses scenario analysis to assess the impact of climate-related risks and, as a result, determines a climate-related risk is reasonably likely to have a material impact on the registrant
- Uses an internal carbon price that is material to how it evaluates and manages a climate-related risk

Internal Audit:

- Has materiality been defined? How is it updated?
- How are actual and specific potential impacts evaluated & calculated?
- Verification and validity of expenditures, estimates and assumptions.
- Reasonableness of scenario analysis
- Basis for internal carbon price
- Overall process and controls around this disclosure requirement.

GOVERNANCE

Companies will be required to describe:

- The board of directors' oversight of climate-related risks, including:
  - Any board committees or subcommittees responsible for the oversight of climate-related risks, if applicable
  - How the board is informed about climate-related risks and oversees progress toward climate-related targets or goals or transition plans

Management's role in assessing and managing material climate-related risks, including:

- Whether and which management positions or committees are responsible and their relevant expertise
- Processes to assess and manage climate-related risks
- Whether management reports information about the risks to the board and its committees or subcommittees

Internal Audit:

- Communicate the requirements to the Board
- Update entity level controls to incorporate Board oversight controls
- Understand management's role in assessing and managing material risk
- Understand and help document detail processes and control points
- Evaluate and test the processes and controls, including any IT dependencies and reporting integrity

TARGETS & GOALS

Companies will need to disclose any climate-related targets or goals that have materially affected or are reasonably likely to materially affect their business, results of operations or financial condition, including:

- The scope of activities included in the target
- The unit of measurement
- The defined time horizon for intended achievement and whether the time horizon is based on one or more goals established by a climate-related treaty, law, regulation, policy or organization
- Any established baselines and a description of how related progress will be tracked
- How they intend to meet their targets or goals

Internal Audit:

- Understand how scope is determined and related documentation
- Understand the basis, reasonableness and preparedness of claims being made

TARGETS & GOALS (CONT.)

Companies will need to also describe:

- Any progress made toward meeting their targets or goals and how it was achieved
- Material impacts of the target or goal or the related actions taken to make progress
- Material expenditures and material impacts on financial estimates and assumptions resulting directly from the target or goal

Additional disclosures will be required if carbon offsets or renewable energy credits or certificates (RECs) are a material component of a registrant's plan to achieve its targets or goals

Internal Audit:

- Validate any
  - Progress claims
  - Material impacts on goals and actions
  - Material expenditures
  - Material impacts on financial statements
- Validate
  - Renewable energy credits or certificates

GHG SCOPE 1 & SCOPE 2 EMISSIONS

Accelerated and large accelerated filers will be required to disclose gross direct GHG emissions from operations they own or control (Scope 1) and/or indirect emissions from purchased electricity and other forms of energy their operations consume (Scope 2), if material

- Scope 1 and Scope 2 emissions will need to be reported separately and in the aggregate in terms of carbon dioxide equivalents
- If any of the seven GHGs defined in the rules is individually material, it will need to be disaggregated
- EGCs and SRCs will be exempt from the requirements to disclose GHG emissions

Disclosures will be required for the most recently completed fiscal year and, to the extent previously disclosed or required to be disclosed, for the historical fiscal year(s) for which audited consolidated financial statements are included in the filing

Internal Audit:

- Internal auditors are likely to allocate a significant portion of their time to this area.
- Understand and document process and controls around Scope 1 and Scope 2 emissions calculations.
- Plan testing of controls

GHG SCOPE 1 & SCOPE 2 EMISSIONS ASSURANCE

- The Scope 1 and Scope 2 emissions disclosures made by accelerated and large accelerated filers will be subject to limited assurance by an independent provider beginning with the third fiscal year of reporting the emissions
- Disclosures by large accelerated filers will subsequently be subject to reasonable assurance, beginning with the seventh fiscal year of reporting the emissions
- Assurance providers will need to be independent and have significant experience in measuring, analyzing, reporting or attesting to GHG emissions
- Registrants will be required to make disclosures about the current assurance provider and any previously engaged providers who resigned, declined to stand for reappointment or were dismissed

Internal Audit:

- Engage with your disclosure teams to understand plan and timing
- Engage with your GHG assurance providers as soon as possible to plan and execute IA activities
- Understand readiness of Disclosure Committees
- Understand Board and Audit Committee requirements and preparations needed

QUESTIONS?

THANK YOU

Abu Aziz, VP Internal Audit, Excelerate Energy

abu.aziz@excelerateenergy.com

https://www.linkedin.com/in/abuaziz/