Strategic Governance: Audit Committee Oversight of AI and Digital Resilience under an Evolving SEC Regulatory Landscape

A Practical Governance Framework for Investment Fund Directors & Audit Committee Chairs

Executive Summary

As fund directors—and specifically Audit Committee Chairs—our fiduciary obligations regarding technology oversight have fundamentally shifted. We have moved from receiving static, annual IT updates to maintaining active, continuous governance over systemic operational risks. With the SEC's heightened regulatory enforcement surrounding cybersecurity (including updated Regulation S-P safeguards and strict incident reporting expectations) alongside aggressive scrutiny of Artificial Intelligence (AI) and Predictive Data Analytics (PDA), board oversight can no longer be treated as a periodic compliance exercise.

Because investment companies—particularly closed-end funds (CEFs)—operate primarily through delegated service models, our primary exposures do not stem from internal IT infrastructure. Rather, our risks reside within the complex web of third-party service providers: investment advisers, sub-advisers, custodians, transfer agents, and fund administrators. Audit Committees must focus on **delegated operational resilience, vendor risk architecture, model integrity, and disclosure accuracy.**

Below is an executive framework mapping the key SEC focus areas to concrete Audit Committee oversight actions and practical reporting metrics.

Oversight Domain	Primary SEC / Regulatory Driver	Board & Audit Committee Action	Practical Reporting Artifacts / Metrics
Cyber Incident Readiness & Materiality	SEC Cyber Rules & Reg S-P updates (Materiality reporting; strict notification triggers)	Establish joint materiality protocols with the Adviser; pre-define threshold triggers for Board notification vs. SEC disclosure.	• Cyber Incident Log (Material & aggregated immaterial) • Table-top execution debriefs • Mean Time to Detect (MTTD) / Respond (MTTR)
Third-Party & Supply-Chain Risk	Service Provider Oversight & Safeguards Rules	Review Adviser's Third-Party Risk Management (TPRM) framework; verify continuous monitoring of critical vendors (custodians, fund accounting).	• SOC 1 / SOC 2 Type II bridge letters • Vendor security rating reports • Sub-adviser contingency & backup plans
AI & Algorithmic Model Governance	SEC PDA Rules / AI Guidance & Model Risk Management	Require Adviser to maintain an active AI inventory; mandate independent validation of investment, trading, and	• Centralized AI Asset Inventory • Annual Model Risk Management (MRM) Audit • Back-testing & drift

		operational algorithms.	analysis logs
Disclosure Integrity & 'AI Washing'	SEC Enforcement Priorities & Form N-CSR / ADV disclosures	Benchmark public statements regarding cyber resilience and AI capabilities against actual Adviser operational practices.	• Disclosure Committee cross-check sign-offs • Form ADV Part 2A & Prospectus alignment reviews

Section I: Cybersecurity Oversight—Operationalizing SEC Expectations

1. Navigating Materiality and Incident Response

The SEC's mandate requiring prompt disclosure of material cybersecurity incidents requires the Audit Committee to work proactively with management before a crisis occurs. In a fund environment, an incident rarely involves a direct breach of the fund itself; instead, it involves a ransomware attack on the fund administrator, a compromised data pipeline at a sub-adviser, or a breach at the transfer agent.

Audit Committees should establish clear operational definitions for "Fund Materiality":

- Quantitative Triggers: Direct financial loss, unexpected fund expenses, or operational disruption impacting Net Asset Value (NAV) calculation by a defined basis-point threshold.
- Qualitative Triggers: Breach of nonpublic personal information (NPI) under Regulation S-P, compromised portfolio trading systems, or temporary inability to execute fund portfolio management strategies.

INCIDENT ESCALATION & DECISION FRAMEWORK

Step 1: Incident Detection — Service Provider reports security disruption to Adviser.
Step 2: Adviser IR Evaluation — Incident Response Team assesses impact on NAV, trading, or NPI data.
Path A: Immaterial Disruption — Logged in Aggregate Incident Registry; reviewed quarterly by Audit Committee.
Path B: Potential Material Impact — Triggers immediate pre-defined Board Escalation protocol (Mandatory Audit Committee Chair notification within 12-24 hours).
Step 3: Joint Assessment & Action — Joint materiality assessment conducted by Fund Board & Adviser Legal, leading to required SEC filings (Form N-CSR / disclosures) and shareholder notices as mandated under updated Regulation S-P rules.

2. Oversight of Delegated Service Providers (TPRM)

Fund boards do not manage IT infrastructure, but we bear fiduciary responsibility for selecting and monitoring those who do. The Audit Committee's focus must be on verifying that the Adviser's Third-Party Risk Management (TPRM) program is rigorous, documented, and actively enforced.

- SOC Report Scrutiny: Do not rely on high-level executive summaries. Audit Committees should mandate that the Adviser review Complementary User Entity Controls (CUECs) in SOC 1 and SOC 2 Type II reports from transfer agents, custodians, and pricing services, ensuring the fund satisfies its half of the shared-responsibility model.

- Contractual Safeguards: Ensure contracts with key providers contain explicit notification SLAs (e.g., requiring service providers to notify the Adviser within 24–48 hours of any security event impacting fund operations or data).

Section II: Artificial Intelligence—Navigating Algorithmic Risk & SEC Scrutiny

As advisers increasingly integrate Generative AI, machine learning, and predictive analytics into portfolio management, quantitative trading, risk management, and investor communications, Audit Committees must expand their risk framework beyond traditional software oversight.

TAXONOMY OF AI IMPLEMENTATION IN FUND OPERATIONS

Investment & Trading Models: Algorithmic execution, sentiment analysis, alternative data integration, and automated portfolio rebalancing.
Operations & Reporting AI: Automated NAV reconciliation, financial statement tagging (XBRL/HTML), fraud detection, and AML monitoring.
Compliance & Marketing AI: Predictive Data Analytics (PDA) tools, personalized shareholder communications, and investor targeting platforms.

1. Model Governance and Risk Management (MRM)

In funds where the Adviser uses proprietary or third-party algorithms for trading or portfolio allocation, model failure represents direct market and reputation risk. Audit Committees should ensure the Adviser has a robust Model Risk Management (MRM) policy covering:

- Data Lineage and Quality: Verification that data inputs used to train models are accurate, non-biased, and free of non-public or proprietary leaks.
- Model Validation and Drift: Regular back-testing of models to detect "concept drift"—where changing market conditions degrade algorithmic accuracy.
- Explainability & Transparency: Ensuring portfolio managers understand why an AI algorithm generates specific buy/sell signals, avoiding black-box reliance.

2. Mitigating "AI Washing" and Disclosure Risk

The SEC has made it clear that exaggerated claims regarding AI capabilities constitute securities fraud. Audit Committees must safeguard the fund from disclosure mismatch:

- Operational Alignment: If the fund's registration statements or marketing materials reference the use of "Advanced AI algorithms" or "Machine Learning models" in portfolio selection, the Audit Committee must verify that these systems are deployed in production as claimed, supported by documented processes.
- Human-in-the-Loop Protocols: Conversely, if the Adviser utilizes GenAI tools in drafting operational or financial disclosures, strict human-in-the-loop (HITL) review protocols must be confirmed.

Section III: Practical Audit Committee Execution Plan

To move these governance concepts from theory to board execution, Audit Committees should adopt a structured quarterly oversight cadence.

Quarter	Governance Focus Area	Primary Agenda Deliverables
Q1 Focus	Policy & Inventory Review	• Review updated AI & Cyber inventories across Adviser and sub-advisers. • Approve annual CISO & CCO reporting schedule and testing scopes.
Q2 Focus	Third-Party & Vendor Audit	• Deep-dive review of SOC 1 / SOC 2 Type II reports for critical service providers. • Audit Adviser's vendor risk assessments and core SLA compliance.
Q3 Focus	AI Model & Algorithmic Oversight	• Review Model Risk Management (MRM) audit reports and algorithmic back-testing. • Evaluate model drift metrics and data governance protocols.
Q4 Focus	Incident Readiness & Disclosure Audit	• Review annual Cyber Risk Assessment & Regulation S-P compliance status. • Perform annual benchmarking of public disclosures vs. operational reality.

KEY QUESTIONS THE AUDIT COMMITTEE CHAIR SHOULD ASK

CYBERSECURITY QUESTIONS FOR CISO & ADVISER CIO:

• Ransomware & Operational Outage: "If our primary transfer agent or fund administrator suffers a total ransomware lockout today, what is our operational recovery time objective (RTO), and how do we calculate NAV during the outage?"

• Incident Aggregation: "How do we track and aggregate 'immaterial' security incidents across our service provider network to determine if they cumulatively constitute a material impact?"

ARTIFICIAL INTELLIGENCE QUESTIONS FOR ADVISER MANAGEMENT:

• Asset Inventory: "Does the Adviser maintain a complete inventory of all AI tools used in managing our fund—including third-party software embedded with GenAI capabilities?"

• Strategy Safeguards: "What controls prevent our proprietary investment strategies or nonpublic shareholder data from being input into public or unvetted Large Language Models (LLMs)?"

• Disclosure Alignment: "How do our public statements regarding our investment process align with the actual day-to-day role AI plays in portfolio construction?"

Conclusion

Board oversight of cybersecurity and AI is not about turning directors into software engineers or data scientists. It is about applying rigorous, inquisitive risk management to modern technology exposures. By focusing on service-provider oversight, establishing clear materiality protocols, demanding model transparency, and ensuring strict alignment between practice and disclosure, Audit Committees can fulfill their fiduciary duty—protecting fund assets and investor value in an increasingly complex digital landscape.

Regulatory References & Sources

- SEC Cybersecurity Risk Management Rules for Investment Advisers and Registered Investment Companies.
- SEC Regulation S-P Safeguards and Incident Notification Amendments.
- SEC Enforcement Priorities regarding Predictive Data Analytics (PDA) and AI Disclosure Alignment.

© 2026 MARESCA GOVERNANCE ADVISORS | WWW.MARESCAGOVERNANCE.COM | ALL RIGHTS RESERVED