To: [CEO Name]

From: Arnav Sahai, Chief Information Security Officer

Date: March 3, 2026

Re: Reframing Cyber as Enterprise Risk: NIST CSF 2.0 and ERM Integration for Board Oversight

Executive Summary

Cyber risk directly impacts our financial performance, operations, regulatory standing, and investor confidence. Ransomware, email compromise, and vendor breaches can cause significant losses. Regulators now expect boards to set clear cyber risk appetite, receive quantified reports, and oversee cyber governance aligned to NIST(National Institute of Standards and Technology) CSF (Cyber Security Framework)2.0.[1] I request CEO support to: **(1) classify cyber as a defined enterprise risk in our ERM(enterprise risk management) framework; (2) adopt NIST CSF 2.0 and authorize a gap assessment; and (3) formalize Board-level reporting and my role as accountable cyber officer.**

Why This Cannot Wait

Our focus on vulnerabilities, tools, and compliance is now seen as insufficient. Most firms lack board-approved cyber risk appetite statements, and current metrics often ignore business impact.[2] Governance failures are a major cause of corporate distress, affecting revenue, capital, and firm

[1] SEC Cybersecurity Risk Management Rule (2023); OCC Heightened Standards for Large Financial Institutions (2014); NIST Cybersecurity Framework 2.0 (2024).
[2] Verizon (2024). Data Breach Investigations Report; Zurich Insurance Group & Advisen (2018). Cyber Risk: Closing the Cyber Risk Gap.

viability.[3] We must adopt integrated risk management with defined risk categories, quantified scenarios, clear risk appetite, and targeted investment.

NIST CSF 2.0 and ERM Integration

NIST CSF 2.0 organizes cybersecurity across six functions, with "Govern" embedding cyber risk into corporate strategy.[4] I propose integrating CSF 2.0 into our ERM program in three areas: (1) Governance and Risk Appetite: define cyber/technology risk as a top ERM category with mapped scenarios and a Board-approved risk appetite statement; (2) Risk Management Structure: formalize my direct reporting to you and standing Board Risk Committee access, with authority to challenge excessive risk-taking; (3) Risk Identification and Reporting: conduct a CSF 2.0 assessment, develop 5–7 business-impact risk scenarios, and replace technical dashboards with a Board view showing residual risk vs. appetite and key risk indicators.

Track key risk indicators (e.g., MFA coverage, patching, incident dwell time) and prioritize investments to close gaps.

Implementation Roadmap and Decisions Requested

Phase 1 — 0–6 Months

• Complete CSF 2.0 gap assessment

• Define cyber risk appetite for Board approval

• Formalize Board reporting cadence

Phase 2 — 6–12 Months

---

[3] Cambridge Centre for Risk Studies (2022). Managing Emerging and Interconnected Risks; Basel Committee on Banking Supervision (2018). Corporate Governance Principles for Banks.
[4] NIST (2024). Cybersecurity Framework 2.0. National Institute of Standards and Technology; COSO (2017). Enterprise Risk Management: Integrating with Strategy and Performance.

• Address high-priority gaps in Govern, Identify, and Protect:

• Identity and access management

• Crown-jewel data protection

• Critical vendor controls

• Enhanced detection and response capabilities

Phase 3 — 12–18 Months

Conduct annual board tabletop exercises, maintain recurring risk metrics, commission annual cyber resilience reviews, and track all results through ERM.

Decisions Requested

For the Board meeting, please agree to:

• Define cyber as an enterprise risk in our ERM framework

• Approve NIST CSF 2.0 adoption and a 6-month gap assessment

• Endorse a Board agenda item for cyber risk and annual resilience review.

Your endorsement will align us with regulatory expectations and reduce the risk of severe cyber incidents that could affect our operations.[5]

[5] SEC (2023). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. 17 CFR Parts 229, 232, 239, 249, and 274; OCC (2023). Sound Practices to Strengthen Operational Resilience. OCC Bulletin 2023-17.