# NIST CSF 2.0 GAP ASSESSMENT

*Meridian Wealth Partners | Cybersecurity Risk Management & Maturity Assessment*

| | |
|---|---|
| **Prepared By:** Carolina Pinto, GRC Analyst | **Assessment Date:** August 2026 |
| **Framework:** NIST CSF 2.0 (NIST CSWP 29) | **Classification:** Internal Use / Portfolio Demonstration |

## 1. Executive Summary

This evaluation reviews Meridian Wealth Partners' ("Meridian") cybersecurity risk management structure against the six core functions of the NIST Cybersecurity Framework 2.0 (Govern, Identify, Protect, Detect, Respond, Recover).

Meridian exhibits localized maturity in Protect (PR) controls, reflecting existing regulatory compliance efforts (GLBA Safeguards Rule, KYC/AML safeguards). However, critical deficiencies exist within Govern (GV) and Detect (DE). The firm currently operates without formal board-level cyber oversight, lacks a structured Supply Chain Risk Management (SCRM) policy, and maintains zero continuous monitoring capabilities. These gaps represent immediate regulatory and operational exposure given Meridian's Custody/UHNW client profile.

Remediation requires a 12-month phased risk mitigation plan prioritizing governance designation, vendor oversight formalization, and detection capability deployment.

## 2. Scope & Assessment Methodology

**Scope:** Covers Meridian's core corporate technology stack, hybrid network infrastructure, and critical SaaS provider environments (detailed in Section 3). Excludes active technical penetration testing and vulnerability scanning; conclusions derive from control design review, documentation analysis, and stakeholder interviews.

**Evaluation Framework:** Each of the 22 NIST CSF 2.0 categories is evaluated on a 1–4 Implementation Tier scale:

- **Tier 1 (Partial):** Ad hoc, reactive, unformalized.
- **Tier 2 (Risk-Informed):** Management-approved practices; lack of enterprise-wide policy/integration.
- **Tier 3 (Repeatable):** Formally defined, policy-driven, routinely updated.
- **Tier 4 (Adaptive):** Continuous, predictive, real-time posture adjustments based on threat intelligence.

Target profiles reflect appropriate baseline requirements for a registered wealth management firm of Meridian's size and asset complexity.

## 3. Critical Asset Inventory

| Asset / System | Operational Owner | Criticality | Sensitivity / Data Type |
|---|---|---|---|
| ClientVantage CRM (SaaS) | Compliance / Ops | High | High — PII, Financials, KYC/AML |
| Portfolio Management System (SaaS) | Investment Ops | High | High — Account & Transaction Data |
| Email & Collaboration Platform (SaaS) | IT | Medium | Medium — Non-public Personal Info (NPI) |
| Document Mgmt / KYC Repository | Compliance | High | High — Regulated Records, Identity Docs |
| Employee Endpoints (~45) | IT | Medium | Medium — Network Access, Cached Files |
| Corporate Network / VPN | IT | High | N/A — Transit Infrastructure |
| Backup & DR Environment | IT | High | High — Full System & Data Mirror |

## 4. Maturity Profile & Gap Matrix

*Priority Gaps (2-Tier Deficiencies) flagged for immediate remediation.*

| NIST CSF 2.0 Category | Current | Target | Gap | Status |
|---|---|---|---|---|
| **GOVERN (GV)** | | | | |
| GV.OC Organizational Context | 2 | 3 | +1 | Baseline |
| GV.RM Risk Management Strategy | 2 | 3 | +1 | Baseline |
| GV.RR Roles, Responsibilities & Authorities | 2 | 3 | +1 | Baseline |
| GV.PO Policy | 2 | 3 | +1 | Baseline |
| **GV.OV Oversight** | **1** | **3** | **+2** | **Priority** |
| **GV.SC Supply Chain Risk Management** | **1** | **3** | **+2** | **Priority** |

| | | | | |
|---|---|---|---|---|
| **IDENTIFY (ID)** | | | | |
| ID.AM Asset Management | 2 | 3 | +1 | Baseline |
| ID.RA Risk Assessment | 2 | 3 | +1 | Baseline |
| **ID.IM Improvement** | **1** | **3** | **+2** | **Priority** |
| **PROTECT (PR)** | | | | |
| PR.AA Access Control & Identity Mgmt | 3 | 4 | +1 | Baseline |
| PR.AT Awareness & Training | 2 | 3 | +1 | Baseline |
| PR.DS Data Security | 3 | 4 | +1 | Baseline |
| PR.PS Platform Security | 2 | 3 | +1 | Baseline |
| PR.IR Infrastructure Resilience | 2 | 3 | +1 | Baseline |
| **DETECT (DE)** | | | | |
| **DE.CM Continuous Monitoring** | **1** | **3** | **+2** | **Priority** |
| **DE.AE Adverse Event Analysis** | **1** | **3** | **+2** | **Priority** |
| **RESPOND (RS)** | | | | |
| RS.MA Incident Management | 2 | 3 | +1 | Baseline |
| **RS.AN Incident Analysis** | **1** | **3** | **+2** | **Priority** |
| RS.CO Response Communications | 2 | 3 | +1 | Baseline |
| RS.MI Incident Mitigation | 2 | 3 | +1 | Baseline |
| **RECOVER (RC)** | | | | |
| RC.RP Recovery Plan Execution | 2 | 3 | +1 | Baseline |
| **RC.CO Recovery Communication** | **1** | **3** | **+2** | **Priority** |

## 5. Primary Deficiencies & Risk Exposure

- **Oversight Deficiencies (GV.OV):** Absence of designated executive ownership and structured board reporting. Leaves the firm vulnerable to governance-level scrutiny under SEC cybersecurity disclosure and management mandates.
- **Vendor Risk Exposure (GV.SC):** Third-party risk reviews occur ad hoc without standardized evaluation frameworks, creating concentration risk across critical SaaS infrastructure (e.g., ClientVantage CRM).
- **Monitoring Deficits (DE.CM / DE.AE):** Absence of active logging/SIEM aggregation prevents real-time threat detection, increasing dwell time and leaving the firm reliant on vendor notifications or post-facto breach discovery.
- **Forensic & Forensic Response Gaps (RS.AN):** Lack of standardized incident investigation protocols impairs root-cause analysis, regulatory notifications, and evidence preservation.
- **Crisis Communication Planning (RC.CO):** Absence of pre-approved incident notification workflows for clients, legal counsel, and regulatory bodies during a security event.

## 6. Risk Register

| Risk Event | Category Ref. | Likelihood | Impact | Severity | Primary Mitigation | Residual Risk |
|---|---|---|---|---|---|---|
| Unmonitored Intrusion / Breach | DE.CM, DE.AE | High | High | **Critical** | Deploy Managed Detection & Response (MDR/SIEM) | Medium |
| Third-Party Vendor Compromise | GV.SC | Medium | High | **High** | Institute mandatory vendor risk assessment workflows | Medium |
| Governance Regulatory Non-compliance | GV.OV | Medium | High | **High** | Establish quarterly executive cyber risk reporting | Low |
| Inadequate Post-Incident Analysis | RS.AN | Medium | Medium | Medium | Standardize investigation/escalation SOPs | Low |
| Uncontrolled Incident Disclosure | RC.CO | Low | High | Medium | Formalize regulatory & client breach disclosure plans | Low |
| Asset Drift / Untracked Systems | ID.AM | Medium | Medium | Medium | Enforce quarterly inventory review cadences | Low |
| Credential Loss | PR.AT | Medium | Medium | Medium | Mandate | Low |

| | |
|---|---|
| via Phishing | ongoing security awareness & testing |

## 7. Remediation Roadmap

### Phase 1: Governance & Third-Party Risk Foundation (Months 0–3)

- Appoint an executive risk owner; institute mandatory quarterly board reporting on risk metrics.
- Enforce a standardized Vendor Risk Policy for all critical software vendors.
- Operationalize quarterly asset reconciliation procedures.

### Phase 2: Technical Detection & Incident Escalation (Months 3–6)

- Procure and deploy an integrated MDR/SIEM solution across endpoints and cloud environments.
- Codify technical Incident Response SOPs (root cause, triage, preservation).
- Execute an executive tabletop exercise simulating a vendor breach scenario.

### Phase 3: Crisis Preparedness & Program Maturity (Months 6–12)

- Finalize client and regulatory communication playbooks for incident disclosures.
- Institutionalize mandatory security awareness training and phishing simulations.
- Conduct a formal 12-month NIST CSF reassessment to validate tier progression.

## 8. Recommendation

**Approved Action:** Formal adoption of the 12-Month Remediation Roadmap.

Initial focus must center on Phase 1 governance structures and Phase 2 detection capabilities. Establishing clear governance accountability and vendor oversight addresses immediate compliance vulnerabilities with minimal capital expenditure, while MDR deployment resolves the firm's primary technical risk exposure.