Suretas

SAMPLE REPORT

CYBERSECURITY RISK ASSESSMENT REPORT

Prepared for

Meridian Harbor Advisors LLC

July 15, 2026

Point-in-time advisory assessment

ABOUT THIS SAMPLE

This is an illustrative sample produced by the Suretas report engine.
The firm named here is fictional and every response was invented for demonstration.
It does not describe a real client, and nothing in it is legal, compliance, or security advice.

Executive Summary

61%

Overall posture: Developing

Severity outlook: Critical · 18 findings across 20 domains

Coverage: all 199 questions answered.

This report presents the results of a questionnaire-based cybersecurity risk assessment of Meridian Harbor Advisors LLC, completed on July 15, 2026 using the Suretas assessment framework. Responses were evaluated against a control baseline drawn from NIST CSF 2.0 and the regulatory requirements applicable to financial firms.

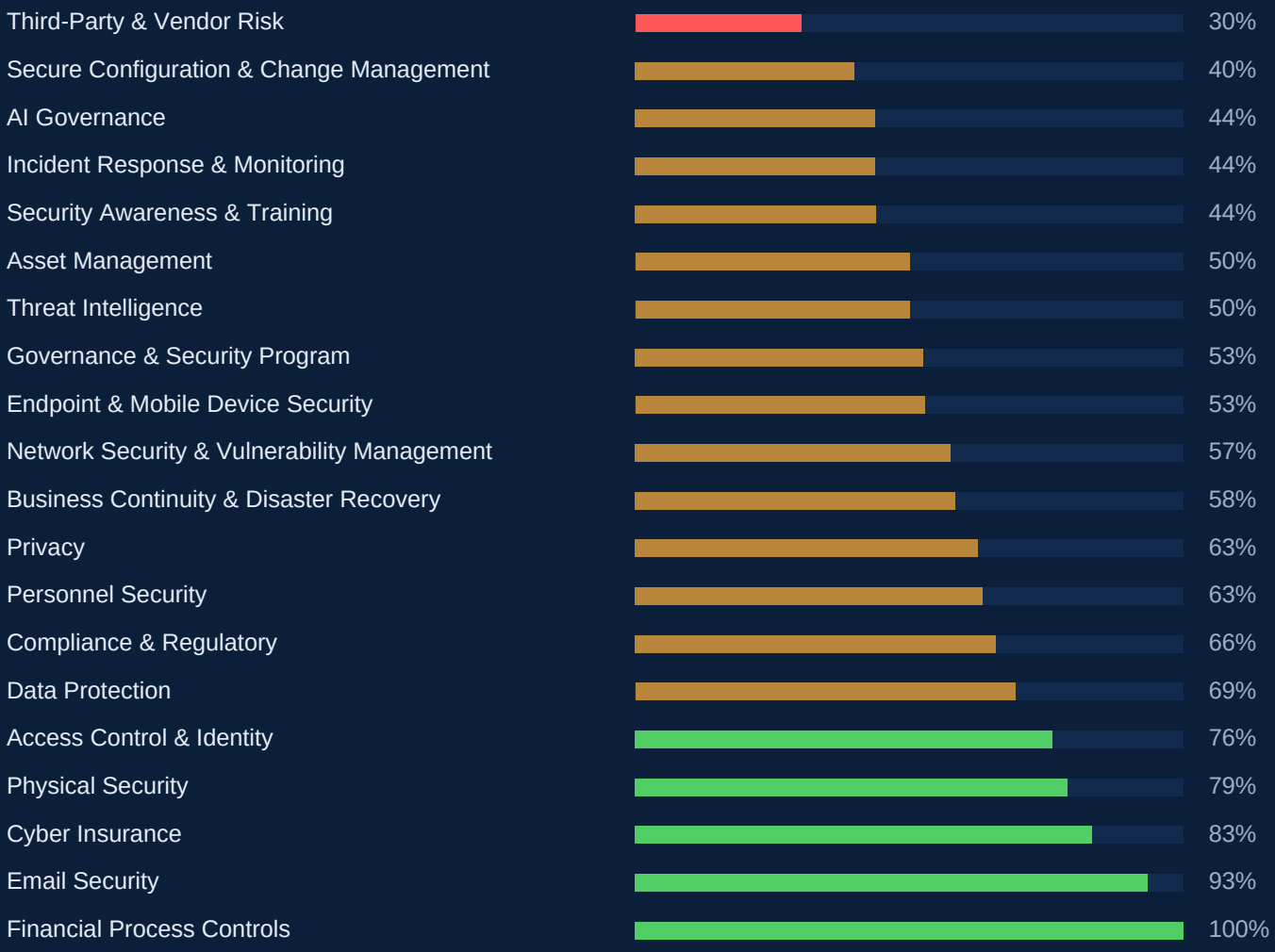
Meridian Harbor Advisors LLC achieved an overall control-coverage score of 61%, placing the firm's posture in the "Developing" range. The assessment produced 18 findings (1 Critical, 10 High, 4 Medium, 3 Low), detailed in the Findings section of this report.

The strongest coverage was observed in Financial Process Controls (100%) and Email Security (93%). The most significant exposure is concentrated in Third-Party & Vendor Risk (30%) and Secure Configuration & Change Management (40%).

Remediation attention should be directed first to: Third-Party Vendor Risk Exposure, Security Program Governance Gaps and Ungoverned AI Usage Exposure. Each is described with a concrete recommendation in the Findings section.

Results by Domain

Sorted weakest-first. Control-coverage percentage per domain.



Scope & Methodology

The assessment covered 20 security domains: Governance & Security Program; Compliance & Regulatory; AI Governance; Asset Management; Access Control & Identity; Data Protection; Email Security; Endpoint & Mobile Device Security; Network Security & Vulnerability Management; Secure Configuration & Change Management; Third-Party & Vendor Risk; Security Awareness & Training; Personnel Security; Incident Response & Monitoring; Business Continuity & Disaster Recovery; Threat Intelligence; Financial Process Controls; Cyber Insurance; Privacy; Physical Security.

Information was gathered through Suretas's structured questionnaire of 199 control questions, completed by Meridian Harbor Advisors LLC personnel. Responses are self-attested. Suretas did not perform technical testing, vulnerability scanning, penetration testing, or independent verification of responses as part of this assessment. Findings and scores reflect the control environment as represented by the firm on July 15, 2026.

Scoring is deterministic: each response is scored against a fixed rubric, weighted by control importance, and aggregated into domain scores and an overall control-coverage score (0 to 100%). Findings are generated for domains and controls scoring below fixed thresholds, with severity assigned by score band; a gap on a highest-weight control escalates the finding's severity by one tier. No element of scoring or finding generation involves generative AI or human discretion; identical responses always produce an identical report.

Opinion & Limitations

On the basis of the responses provided and the methodology described above, it is our opinion that Meridian Harbor Advisors LLC's cybersecurity control environment is developing: core safeguards are present, but meaningful gaps remain in specific areas. The Critical findings identified in this report warrant remediation on a priority basis. This opinion is a point-in-time advisory assessment of the control environment as represented in the firm's questionnaire responses.

Limitations. This report is not an audit, attestation, or certification, and does not establish or imply compliance with any law, regulation, or framework. It relies on self-attested responses that were not independently verified, reflects a single point in time, and does not guarantee security or the absence of compromise. Regulatory excerpts and citations are provided for reference and do not constitute legal advice. Meridian Harbor Advisors LLC should consult qualified counsel on legal and regulatory obligations.

Findings

Third-Party Vendor Risk Exposure

CRITICAL

Third-Party & Vendor Risk · 30% control coverage

Third-Party & Vendor Risk controls are at 30% coverage. The following specific controls have gaps that require attention: • Do you maintain a current inventory of all third-party vendors and service providers that handle, store, or access your firm's or clients' data? • How mature is your process for assessing the security posture of vendors before onboarding them and on a recurring basis afterward? • Have you identified which vendors are critical to operations or hold the most sensitive data, and prioritized oversight of those vendors accordingly? • Has a formal third-party risk management (TPRM) program been established, with information security always included in vendor evaluations? • Do your vendor contracts include security and breach-notification clauses that obligate the vendor to protect data and report incidents to you?

RECOMMENDATION

Build and maintain a current inventory of all vendors with access to firm or client data. Require SOC 2 Type II reports or completed security questionnaires before onboarding data-handling vendors. Ensure all vendor contracts include a breach notification clause (48 to 72 hours is standard). Identify your top 3 to 5 critical vendors and review their security posture annually. Audit vendor access rights at least once per year and revoke stale access promptly.

NIST CSF 2.0: GV.SC-04 · GV.SC-07 · GV.SC-01 · GV.SC-05 · GV.SC-10

Regulations: FTC Safeguards §314.4(f) · NYDFS §500.11 · SEC Reg S-P

Security Program Governance Gaps

HIGH

Governance & Security Program · 53% control coverage

Governance & Security Program controls are at 53% coverage. The following specific controls have gaps that require attention: • Does the firm have a designated internal person responsible for information security, rather than relying solely on an external provider such as a managed service provider (MSP)? • How well is security funded as a distinct line, driven by the risk program rather than absorbed into general IT spend? • Are cybersecurity program metrics generated in a repeatable way and reported to C-level management on an established cadence? • Is a formal process in place to review, approve, and document exceptions to security policies? • Has a cyber/risk committee with key stakeholders from across the business been established, meeting at least annually?

RECOMMENDATION

Formally define and document who owns cybersecurity: a named internal individual, even if dual-hatted, with documented responsibilities and a designated backup. Establish a dedicated security budget tied to the firm's risk strategy rather than blended IT spend. Report program metrics to leadership on a set cadence and manage policy exceptions through a documented review-and-approve process. For GLBA-covered firms, these map directly to the Safeguards Rule's Qualified Individual requirement; for NYDFS-covered entities, to the §500.04 CISO obligations.

NIST CSF 2.0: GV.RR-02 · GV.RR-03 · GV.OV-01 · GV.PO-02 · GV.RR-01 · GV.OV-02 · GV.OC-03

Regulations: FTC Safeguards §314.4(a) · NYDFS §500.04 · NYDFS §500.02 · FTC Safeguards §314.4(i) · NYDFS §500.03 · FTC Safeguards §314.4(b) · SEC Cyber Disclosure

Ungoverned AI Usage Exposure

HIGH

AI Governance · 44% control coverage

AI Governance controls are at 44% coverage. The following specific controls have gaps that require attention: • Is entering client personal data, portfolio holdings, or material nonpublic information into public AI assistants prohibited by policy AND prevented or monitored by a technical control? • Does an AI acceptable-use policy exist that clearly defines approved AI use cases? • Is AI usage at the firm formally scoped and controlled, rather than left to individual staff discretion? • Is a specific person or committee formally responsible for overseeing the firm's use of AI? • Are processes in place to ensure compliance with applicable AI laws and regulations in all jurisdictions where the firm operates?

RECOMMENDATION

Assign a named owner or committee for AI oversight. Publish an AI acceptable-use policy that lists approved tools and use cases, and explicitly prohibits pasting client or firm-sensitive data into unapproved AI services. Move from staff-discretion usage to an approved-tools model, enforced by technical controls (web filtering or DLP) where feasible. Track emerging AI regulations in every jurisdiction where the firm operates.

NIST CSF 2.0: GV.PO-02 · GV.PO-01 · GV.RR-02 · GV.OC-03 · GV.SC-07

Regulations: SEC Reg S-P · FTC Safeguards §314.4(f)

Incomplete Asset Visibility

HIGH

Asset Management · 50% control coverage

Asset Management controls are at 50% coverage. The following specific controls have gaps that require attention: • Is a centralized, complete inventory of hardware assets maintained under formal asset-management procedures? • Is a centralized, complete inventory of software assets maintained under formal asset-management procedures? • Are all critical business systems free of end-of-life or unsupported hardware, operating systems, and applications? • Are the cloud services used by the firm centrally inventoried and formally managed? • Are databases holding firm or client data inventoried and formally managed?

RECOMMENDATION

Build centralized inventories of hardware, software, cloud services, and databases. You cannot protect what you haven't inventoried, and regulators (NYDFS §500.13, FTC Safeguards) now expect documented asset inventories. Move update cadence from ad-hoc toward automated discovery. Identify and retire end-of-life systems on critical paths, or isolate them with compensating controls and a documented exception.

NIST CSF 2.0: ID.AM-01 · ID.AM-02 · PR.PS-02 · ID.AM-07

Regulations: FTC Safeguards §314.4(c)(2) · NYDFS §500.13 · NYDFS §500.05

Endpoint and Mobile Device Control Gaps

HIGH

Endpoint & Mobile Device Security · 53% control coverage

Endpoint & Mobile Device Security controls are at 53% coverage. The following specific controls have gaps that require attention: • Is mobile device access to company data managed through a mobile device management (MDM) or mobile application management (MAM) tool, such as Microsoft Intune or Jamf, or blocked entirely? • Are Office macros blocked from executing automatically on endpoints? • Is acceptable use of personally-owned devices for firm business formally defined? • Do mobile device policies enforce PIN or biometrics, a minimum OS version, and blocking of jailbroken or rooted devices? • Is corporate data on mobile devices confined to an encrypted container with copy/paste restrictions?

RECOMMENDATION

Block Office macros by default, enforce a 10-minute-or-less screen lock, and define acceptable use for personal devices. Manage mobile access to firm data through MDM/MAM tooling (enforce PIN/biometrics, minimum OS versions, jailbreak blocking, and encrypted containers for corporate data), or block mobile access entirely. Review device policies at least annually.

NIST CSF 2.0: PR.PS-01 · PR.PS-05 · GV.PO-01 · PR.DS-01

Network Security and Vulnerability Management Gaps

HIGH

Network Security & Vulnerability Management · 57% control coverage

Network Security & Vulnerability Management controls are at 57% coverage. The following specific controls have gaps that require attention: • How mature is your patch management program? Are critical patches applied within 30 days and emergency patches within 72 hours across servers, endpoints, and network devices? • Do you run authenticated vulnerability scans against your internal network and your external attack surface at least quarterly? • Is your network segmented so that systems holding client financial data are isolated from general office traffic, and is that segmentation enforced at the network layer? • Are identified vulnerabilities formally tracked, prioritized, and remediated under documented procedures? • Do you engage an independent third party to perform penetration testing of your external perimeter and internal network at least annually?

RECOMMENDATION

Establish a formal patch management program targeting critical patches within 30 days and emergency patches within 72 hours, tracking compliance by asset. Deploy endpoint detection and response (EDR) on all workstations and servers with 24/7 alert coverage. Run authenticated vulnerability scans quarterly and remediate high/critical findings within 30 days. Segment networks so client financial data systems are isolated from general office traffic at the network layer. Commission an annual penetration test from an independent third party and track all findings to closure. Enable DNS filtering to block known-malicious domains before they reach endpoints.

NIST CSF 2.0: PR.PS-02 · ID.RA-01 · PR.IR-01 · DE.CM-01

Regulations: NYDFS §500.05 · FTC Safeguards §314.4(d)(2) · FTC Safeguards §314.4(d)

Configuration and Change Management Deficiencies

HIGH

Secure Configuration & Change Management · 40% control coverage

Secure Configuration & Change Management controls are at 40% coverage. The following specific controls have gaps that require attention: • Do formal technical configuration standards (hardening baselines) exist for IT systems, with security consistently addressed? • Are changes to production systems managed through a formal change-management process? • Are configuration standards actively enforced, either manually on a cadence or continuously via configuration-management tooling? • Are production changes tested and verified not to introduce security vulnerabilities before release? • Are technical configuration standards reviewed on a defined cadence or when systems change?

RECOMMENDATION

Adopt hardening baselines (CIS Benchmarks are the standard starting point) for servers, workstations, and cloud services, review them on a defined cadence, and enforce them, ideally via configuration-management tooling. Route all production changes through a formal process with security testing, rollback plans, and documented tracking. The FTC Safeguards Rule (§314.4(c)(7)) explicitly requires change-management procedures.

NIST CSF 2.0: PR.PS-01

Regulations: FTC Safeguards §314.4(c)(7)

Security Awareness and Human Risk Exposure

HIGH

Security Awareness & Training · 44% control coverage

Security Awareness & Training controls are at 44% coverage. The following specific controls have gaps that require attention: • Do you run simulated phishing campaigns against employees on a recurring basis, and provide targeted training to employees who click or report simulations? • Are new employees required to complete security awareness training before or immediately upon gaining access to firm systems and client data? • Do senior leaders and board members receive tailored cybersecurity briefings covering threats relevant to the firm, such as business email compromise and wire fraud? • How well-prepared are your staff to recognize and report social engineering attempts including vishing (voice phishing), pretexting, and impersonation of leadership? • Does training cover AI-generated voice and video impersonation, so staff understand that a familiar voice or face on a call is not authorization to move money or change payment details?

RECOMMENDATION

Require all employees to complete security awareness training annually, with completion tracked. Run phishing simulations at least quarterly and route clickers to targeted training, and track click rates over time to measure improvement. Require security training for new hires before granting system access. Brief senior leadership and the board on threats specific to financial firms: business email compromise (BEC), wire fraud, and executive impersonation are the top social-engineering vectors in this sector. Require annual written acknowledgment of security policies for all staff. Consider a security awareness platform (KnowBe4, Proofpoint) to systematize and evidence the program.

NIST CSF 2.0: PR.AT-01 · PR.AT-02 · GV.RR-01

Regulations: NYDFS §500.14 · FTC Safeguards §314.4(e)

Incident Response Readiness Gaps

HIGH

Incident Response & Monitoring · 44% control coverage

Incident Response & Monitoring controls are at 44% coverage. The following specific controls have gaps that require attention: • Do you have a written incident response plan that defines roles, decision authority, and step-by-step actions for a suspected security incident? • Is there a specific playbook for business email compromise and fraudulent payment requests, covering immediate bank recall steps and the window in which funds can still be recovered? • How mature is your security monitoring, including endpoint detection, alerting, and the ability to detect suspicious activity in a timely manner? • Is there a documented decision policy for ransom demands that names who can authorize payment and requires sanctions screening before any payment is considered? • How mature is your practice of running tabletop exercises or drills to rehearse the incident response plan with the people who would execute it?

RECOMMENDATION

Develop a written incident response plan that names who is responsible, how decisions are escalated, and the step-by-step process from detection through recovery. Define breach notification timelines: GLBA-covered entities typically have a 30-day obligation; SEC registrants 4 business days for material incidents. Run at least one tabletop exercise per year. Centralize log collection and retain logs for a minimum of 90 days. Define a recovery time objective (RTO) for each critical system.

NIST CSF 2.0: ID.IM-04 · RS.MA-02 · DE.CM-09 · ID.IM-02 · RC.RP-02 · DE.AE-03 · PR.PS-04 · DE.CM-03

Regulations: NYDFS §500.16 · FTC Safeguards §314.4(h) · SEC Reg S-P · NYDFS §500.14 · FTC Safeguards §314.4(c)(8) · FTC Safeguards §314.4(d) · NYDFS §500.06 · SEC 17a-4/204-2

Business Continuity and Recovery Readiness Gaps

HIGH

Business Continuity & Disaster Recovery · 58% control coverage

Business Continuity & Disaster Recovery controls are at 58% coverage. The following specific controls have gaps that require attention: • Has a business impact analysis been conducted in the last 24 months, with results used to shape resilience and recovery planning? • Is the business continuity plan exercised at least annually with the people who would actually execute it? • Is the disaster recovery plan tested at least annually? • Is the business continuity plan reviewed at least annually? • Is the disaster recovery plan reviewed at least annually?

RECOMMENDATION

Conduct a business impact analysis and let it drive documented business continuity and disaster recovery plans, then test both at least annually, including key-person and emergency-communication scenarios. Apply the 3-2-1 backup rule with at least one immutable or WORM-protected offsite copy so ransomware cannot encrypt the backups too. NYDFS §500.16 requires documented, tested BCDR plans and protected backups.

NIST CSF 2.0: ID.RA-04 · ID.IM-02 · ID.IM-04 · PR.DS-11

Regulations: NYDFS §500.16 · SEC 17a-4/204-2

Limited Threat Visibility

HIGH

Threat Intelligence · 50% control coverage

Threat Intelligence controls are at 50% coverage. The following specific controls have gaps that require attention: • Are documented procedures in place for receiving and analyzing threat intelligence? • Does the firm receive sector threat intelligence through an industry information-sharing body such as FS-ISAC? • Is dark-web and brand monitoring in place, through manual checks or an automated service scanning for leaked firm credentials and impersonation?

RECOMMENDATION

Subscribe to threat feeds and vulnerability notices covering your actual technology stack, and document a lightweight process for reviewing and acting on them. Join FS-ISAC or a comparable financial-sector sharing community. Consider dark-web monitoring for exposed firm credentials: compromised-credential resale is a leading precursor to financial-firm intrusions.

NIST CSF 2.0: ID.RA-02

Regulatory Compliance and Governance Deficiencies

MEDIUM

Compliance & Regulatory · 66% control coverage

Compliance & Regulatory controls are at 66% coverage. The following specific controls have gaps that require attention: • Do you have a formal GLBA Safeguards Rule compliance program in place, including a designated qualified individual, written information security plan, and annual reporting to the board? • Do you maintain a written Identity Theft Prevention Program under SEC Regulation S-ID, approved by the board or senior management, with periodic reporting on how well it is working? • Do you conduct a formal, documented cybersecurity risk assessment at least annually that identifies threats, vulnerabilities, and risk treatment decisions? • Do you have documented procedures for notifying regulators of a cybersecurity incident within required timeframes, including the SEC, FINRA, or state regulators as applicable? • Does the board or senior leadership receive regular cybersecurity status reports at least annually, covering risk posture, incidents, and program updates?

RECOMMENDATION

If subject to GLBA (most RIAs, broker-dealers, and community banks are): designate a Qualified Individual to oversee your information security program and deliver an annual written report to the board. Maintain a written information security plan (WISP) updated at least annually. Conduct a formal documented risk assessment annually: this is required by GLBA, NY DFS Part 500, and is a standard exam request for FINRA and SEC examinations. Document your regulatory incident notification procedures: SEC registrants must notify within 4 business days for material incidents; GLBA-covered entities within 30 days to affected customers. Ensure the board receives at least annual cybersecurity reports. Review cyber liability coverage limits annually; many firms are underinsured relative to the client data they hold.

NIST CSF 2.0: GV.OC-03 · ID.RA-01 · RS.CO-02 · GV.OV-01

Regulations: FTC Safeguards §314.4(a) · GLBA · SEC Reg S-ID · FTC Safeguards §314.4(b) · NYDFS §500.09 · SEC Reg S-P · NYDFS §500.17 · SEC Cyber Disclosure · FTC Safeguards §314.4(j) · FTC Safeguards §314.4(i) · NYDFS §500.04 · SEC 17a-4/204-2 · NYDFS §500.06

Data Protection and Encryption Deficiencies

MEDIUM

Data Protection · 69% control coverage

Data Protection controls are at 69% coverage. The following specific controls have gaps that require attention: • Do you periodically test restoring from backups to confirm the data is recoverable and meets your recovery objectives? • Do you have a written data classification policy that labels data by sensitivity and defines handling rules for each level? • Do you maintain an inventory of where sensitive client and financial data is stored, processed, and transmitted across your environment? • Are data loss prevention (DLP) tools, such as Microsoft Purview or Forcepoint, in place to monitor and alert on the movement of sensitive data? • Is sending firm data to personal email prevented, with personal email access blocked or controlled on firm systems?

RECOMMENDATION

Enable full-disk encryption on all laptops and endpoints. Apply database-level encryption for systems storing client or financial data. Develop a written data classification policy that defines handling rules for sensitive information. Test backup restoration at least quarterly and maintain an offsite or immutable copy. Build and maintain a data inventory that tracks where sensitive data is stored, processed, and transmitted.

NIST CSF 2.0: PR.DS-11 · ID.AM-07 · DE.CM-09

Regulations: NYDFS §500.16 · FTC Safeguards §314.4(c)(2) · NYDFS §500.13 · SEC Reg S-P · FTC Safeguards §314.4(c)(8) · NYDFS §500.14

Personnel Security Control Gaps

MEDIUM

Personnel Security · 63% control coverage

Personnel Security controls are at 63% coverage. The following specific controls have gaps that require attention: • Are HR documents containing personal data (resumes, Social Security numbers, I-9s, bank details) collected and stored securely? • Are alerting and verification processes in place for changes to HR data such as payroll bank details? • Is unusual data access or bulk download by employees who are serving notice, or in dispute, monitored during their final weeks? • Are background checks re-performed periodically for employees in key-person roles?

RECOMMENDATION

Conduct background checks before hire for all roles, adding criminal and credit history for roles that touch client data or move money (where legally permitted). Require signed acknowledgment of the security policy at onboarding. Store HR records containing SSNs and bank details in access-controlled, encrypted locations, and add verification steps for payroll detail changes, a growing payroll-diversion fraud vector.

NIST CSF 2.0: PR.DS-01 · DE.CM-03 · GV.RR-04

Regulations: SEC Reg S-P · FTC Safeguards §314.4(c)(3) · SEC Reg S-ID · FTC Safeguards §314.4(c)(8)

MEDIUM

Privacy Program Deficiencies

Privacy · 63% control coverage

Privacy controls are at 63% coverage. The following specific controls have gaps that require attention: • Are roles and responsibilities for the firm's privacy program formally defined and assigned? • Are formal procedures in place to respond to individuals exercising personal-data rights requests? • Are privacy impact assessments (PIA) or data protection impact assessments (DPIA) conducted at least annually or when data processing changes?

RECOMMENDATION

Assign formal ownership of the privacy program. Maintain a privacy policy and deliver the consumer privacy notices Regulation S-P and GLBA require. Establish documented procedures for responding to personal-data rights requests within statutory windows, and run a privacy impact assessment when data processing changes materially.

NIST CSF 2.0: GV.RR-02 · GV.OC-03

Regulations: SEC Reg S-P · GLBA

LOW

Access Control and Identity Management Gaps

Access Control & Identity · 76% control coverage

Access Control & Identity controls are at 76% coverage. The following specific controls have gaps that require attention: • Is phishing-resistant multi-factor authentication (passkeys, FIDO2 security keys, or certificate-based login) required for administrator accounts and for any system that moves money, rather than SMS codes or simple approve or deny push prompts? • Are local administrator rights on workstations restricted to designated IT personnel, with a formal exception process for anyone else? • Are emergency break-glass administrator accounts formally defined, held in a sealed credential store, excluded from single sign-on, and alerted on every time they are used? • Are authenticated sessions protected against stolen session tokens, through bounded session lifetimes and forced re-authentication when device, location, or risk signals change? • Is privileged access reviewed on a separate, more frequent cycle than standard user access?

RECOMMENDATION

Enforce multi-factor authentication (MFA) on all business systems, email, and VPN. Create dedicated administrator accounts separate from daily-use accounts and log all privileged activity. Conduct quarterly access reviews and tie employee offboarding to a same-day deprovisioning checklist. Apply least-privilege principles: users should only have access to the systems their role requires.

NIST CSF 2.0: PR.AA-03 · PR.AA-05 · PR.AA-01

Regulations: FTC Safeguards §314.4(c)(5) · NYDFS §500.12 · NYDFS §500.07 · FTC Safeguards §314.4(c)(1)

Cyber Insurance Coverage Gaps

LOW

Cyber Insurance · 83% control coverage

Cyber Insurance controls are at 83% coverage. The following specific controls have gaps that require attention:
• Does coverage include funds-transfer fraud, business email compromise, ransomware, and extortion events?

RECOMMENDATION

Review the policy against the incidents most likely to hit a financial firm: funds-transfer fraud and business email compromise (frequently sub-limited or excluded), ransomware and extortion, third-party breach, incident response costs (forensics, legal, PR, notification), and business interruption. Involve executive leadership in coverage decisions and re-evaluate limits annually against the volume of client data held.

NIST CSF 2.0: GV.RM-04

Physical Security Control Weaknesses

LOW

Physical Security · 79% control coverage

Physical Security controls are at 79% coverage. The following specific controls have gaps that require attention:
• Do you have a removable-media policy that controls or blocks the use of USB drives and other portable media on systems handling sensitive data? • Are visitors to the office signed in, escorted in sensitive areas, and logged so there is a record of who was on-site and when? • Do you enforce a clean-desk policy so that printed client data and credentials are not left exposed when workstations are unattended? • How mature is your practice of periodically reviewing physical security controls and updating them as facilities, staffing, or threats change? • Do physical controls include individual badging, surveillance of entry and exit points, visitor management, and alerts for potential intrusions?

RECOMMENDATION

Restrict access to server rooms, network closets, and wiring panels to authorized personnel using badge readers or keyed locks, and document who has access. Log all visitor entries and require escort in sensitive areas. Enforce full-disk encryption on all laptops and mobile devices so a lost device does not expose client data. Establish a documented media disposal procedure: shred paper records, use certified wiping software or physical destruction for hard drives.

NIST CSF 2.0: PR.PS-01 · PR.AA-06 · PR.DS-01