NIST Cybersecurity Framework (CSF) Assessment Report – Finance Sector Organization

Executive Summary

This report presents the results of a comprehensive cybersecurity assessment for the organization, aligned with the NIST Cybersecurity Framework (CSF). The organization is a mid-sized finance sector company facing several critical security gaps despite having some security tools in place. Key findings include the absence of multi-factor authentication (MFA) for user access, a lack of internal network segmentation, and the presence of legacy Windows Server 2003 systems with unpatched critical vulnerabilities. These gaps significantly elevate cyber risk exposure. On a positive note, the organization has invested in a Splunk Security Information and Event Management (SIEM) for log monitoring and maintains Fortinet firewalls at its perimeter and branches, though these firewalls are outdated. Overall, the current security maturity level across the CSF categories is **low to moderate**, with many practices only partially implemented.

The organization's risk posture favors mitigation of risks by implementing controls, rather than accepting risk. High-risk issues are therefore expected to be addressed promptly, while risk acceptance is considered only for certain medium-risk items. This assessment identified several high-priority remediation areas. **Immediate actions are recommended** to address the most urgent gaps (implementing MFA, segmenting the network, and upgrading or isolating legacy systems) in order to reduce the likelihood of a severe security incident such as unauthorized access or data breach. Medium-term enhancements include upgrading firewall infrastructure, formalizing security processes (e.g. patch management, incident response planning), and improving staff security awareness. Long-term strategic improvements are outlined to continue raising the organization's security maturity in line with industry best practices and regulatory expectations for financial institutions.

By following the recommendations in this report, the organization can achieve a more robust security posture. The recommended improvements will strengthen the **Protect** and **Detect** capabilities (preventing common attack vectors and improving visibility), and establish formal **Respond** and **Recover** processes to minimize damage if an incident occurs. This report is intended for executive leadership, external auditors, and internal stakeholders to understand the current cybersecurity posture and to guide risk-informed decision-making for security investments. All findings and recommendations have been prioritized based on their impact on the organization's critical assets and services, with an emphasis on the organization's low risk tolerance.

Methodology

This assessment was conducted using the NIST Cybersecurity Framework (CSF) as a benchmark. The scope included all five core CSF Functions – Identify, Protect, Detect, Respond, and Recover – covering 23 associated security categories. Information was gathered through interviews with key IT and security personnel, review of documentation, technical configuration analysis, and vulnerability scanning. Key documents reviewed included security policies, network diagrams, asset inventories, and recent security reports (e.g., vulnerability scan results and SIEM logs). The assessment also considered governance aspects (leadership oversight and roles) as they influence CSF implementation.

Each CSF Category was evaluated and assigned an **implementation score from 0 to 3** based on the maturity of the organization's controls and processes:

- **0 = Not Implemented:** No meaningful implementation or capability in this area.
- **1 = Ad Hoc / Partially Implemented:** Some informal or reactive practices exist, but they are incomplete or not consistently applied.
- **2 = Defined / Risk Informed:** Controls or processes are in place and documented for the area, though they may not be fully effective or uniformly enforced across the organization.
- **3 = Managed / Adaptive:** Controls are fully implemented, regularly reviewed, and integrated into a continuous improvement process (reflecting a high level of maturity).

Assessment evidence was mapped to each category. For example, the presence of legacy unpatched systems was used to evaluate **Maintenance (PR.MA)**, and the lack of multi-factor authentication informed the **Access Control (PR.AC)** category score. Interviews with IT managers provided insight into risk management strategy and incident response preparedness. Where possible, technical controls were directly observed or tested (e.g., reviewing firewall configurations, checking for MFA enforcement in authentication systems).

All findings were validated with the organization's representatives to ensure accuracy. The results were then compiled into a detailed evaluation table (below), followed by a gap analysis and recommendations. The gap analysis prioritizes issues based on risk (with the organization's stated preference to mitigate rather than accept risk). Finally, an improvement plan was developed, outlining short-, medium-, and long-term actions with estimates of effort and required resources. This structured approach ensures that the assessment is both comprehensive and actionable, providing a clear roadmap for improving the organization's cybersecurity posture.

Detailed Evaluation of CSF Categories

The following table shows the assessment results for **all CSF categories** grouped by their function, with an implementation score (0–3) and relevant observations or examples from the organization's environment:

Function	Domain	Maturity Rating	Description
Identify	ID.AM: Asset Management	1	An inventory of IT assets exists but is incomplete and not regularly updated. For example, several legacy servers (Windows Server 2003) remain in production beyond their intended lifecycle. Critical assets and data (e.g. core financial databases) are known, but there is no centralized asset management system linking assets to business functions.
Identify	ID.BE: Business Environment	2	The organization has defined its business objectives and critical services (e.g. online banking, trading platform). Management recognizes the importance of these services for customers and regulatory obligations. However, this understanding is not formally used to prioritize cybersecurity activities. Security investments are not explicitly aligned to the most critical business processes (e.g., the lack of network segmentation around sensitive systems shows this misalignment).
Identify	ID.GV: Governance	1	There is no formal cybersecurity governance committee or comprehensive security policy enforcement. Some high-level IT security policies exist but executive oversight is limited. For instance, there is no mandate from leadership to implement MFA or update legacy systems, indicating a gap in governance and accountability for cybersecurity outcomes. Roles and responsibilities for security are informally assigned to IT personnel without formal documentation or regular governance reviews.
Identify	ID.RA: Risk Assessment	1	Risk assessment activities are performed on an ad hoc basis. The organization has conducted basic vulnerability scans (revealing critical issues like the Windows 2003 server vulnerabilities) and recognizes obvious risks (such as no MFA for remote access), but there is no formal risk assessment process or regular risk review cycle. Identified risks have not been fully evaluated for likelihood/impact in a consistent manner, and high risks have lingered without timely mitigation.
Identify	ID.RM: Risk Management Strategy	2	The organization exhibits an implicit risk management strategy: a preference for mitigating high risks by implementing controls, and only considering risk acceptance for medium-level risks. This indicates management has a general risk posture in mind. However, this strategy is not codified in a formal risk management program or policy. There is no documented risk appetite statement or structured process to decide when to accept, transfer, or mitigate risks beyond the basic principle observed.

Identify	ID.SC: Supply Chain Risk Management	1	Supply chain and third-party risks are weakly managed. The organization relies on several vendors and service providers (e.g., uses Fortinet for firewalls, possibly outsources some IT services), yet there is no formal vendor security assessment process. Security requirements are not consistently included in contracts. For example, the company has not assessed the security of software vendors or cloud providers from a cybersecurity standpoint. Any oversight of third-party risk is informal and limited to basic due diligence when selecting major vendors.
Protect	PR.AC: Identity Management & Access Control	1	User access controls are partially implemented. The company uses individual user accounts and passwords for systems (e.g., Active Directory for domain logins), but Multi-Factor Authentication (MFA) is not enforced on any critical systems or remote access VPNs. This means access is protected by single-factor authentication only, which is inadequate for a finance organization. Privileged accounts (administrators) also do not have MFA, heightening the risk of credential compromise. Physical access to offices and servers is controlled by keys and basic badges, but lacks integration with IT security monitoring.
Protect	PR.AT: Security Awareness & Training	1	A formal cybersecurity awareness program is largely missing. Employees receive minimal training – typically a brief orientation or annual policy acknowledgment – but there is no ongoing security awareness campaign. There is little to no phishing simulation or role-specific training for high-risk staff (e.g., finance managers handling wire transfers). This gap leaves the organization susceptible to social engineering attacks. IT staff do some self-directed security learning, but there is no structured training plan to keep technical teams updated on emerging threats.
Protect	PR.DS: Data Security	1	Data protection measures are only basic. While the organization uses standard protections like password controls and basic network firewalls, it lacks a formal data classification and protection program. Sensitive financial data (customer PII, transaction records) is not clearly classified or segregated. Encryption is used for data in transit (e.g., HTTPS for web services), but there is uncertainty about encryption of data at rest on servers and backups. No Data Loss Prevention (DLP) tools or database activity monitoring are in place to safeguard sensitive data. Overall, data security controls do not meet the expected rigor for a finance-sector entity handling confidential information.
Protect	PR.IP: Info Protection Processes & Procedures	1	Documented processes for information security exist in a limited capacity. For example, there are informal procedures for backing up data and basic change management, but no comprehensive written procedures for patch management, secure system configuration, or access provisioning. The security policies that do exist (such as an IT acceptable use policy) are outdated and not aligned with current threats. There is no formal schedule to review or update security procedures. The lack of standardized processes contributed to oversight of critical tasks – e.g., no procedure ensured legacy systems (Win 2003) were updated or decommissioned.

Protect	PR.MA: Maintenance	0	System maintenance practices are largely absent or ineffective. The clearest evidence is that multiple servers still run Windows Server 2003, an operating system that reached end-of-life and no longer receives security patches. This indicates a failure in patch management and technology lifecycle management. Regular updates and preventive maintenance are not consistently performed on systems and network devices. While hardware repairs or reactive fixes occur when something breaks, there is no proactive maintenance schedule. The outdated Fortinet firewall software (firmware) is another example of maintenance neglect, as it has not been upgraded to address known vulnerabilities.
Protect	PR.PT: Protective Technology	1	The organization has implemented some protective technologies, but they are insufficient or outdated. Firewalls are deployed at the network perimeter and branch offices (Fortinet appliances), providing a basic layer of defense. However, these firewalls run older firmware and may lack advanced threat prevention features seen in newer models. Moreover, there is no internal network segmentation – the internal network is flat, so once an attacker breaches the perimeter, they could move laterally without hindrance. Endpoint security is limited to standard antivirus on workstations, with no Next-Generation AV or endpoint detection and response (EDR) tools deployed. Overall, while baseline protective tools exist, critical enhancements (modern firewalls, network segmentation, up-to-date endpoint protection) are missing, reducing the effectiveness of the Protect function.
Detect	DE.AE: Anomalies and Events	1	The capability to detect anomalies and security events is rudimentary. There are basic logs from systems and the firewall, and the SIEM platform (Splunk) is aggregating some of this data. However, the organization has not established normal behavior baselines or advanced alert use-cases. Unusual network activity or user behavior may not be recognized in a timely manner. For example, there is no mechanism like User and Entity Behavior Analytics (UEBA) to flag if an employee account behaves abnormally (possibly indicating compromise). Detection largely relies on signature-based alerts (e.g., antivirus notifications or obvious firewall denies) rather than proactive anomaly detection.
Detect	DE.CM: Security Continuous Monitoring	2	The organization has implemented a SIEM (Splunk) which continuously collects and monitors logs from servers, the firewall, and other network devices. This is a strength, as it provides a central point to detect security events across the environment. Some alerts are configured in Splunk (e.g., alerts for multiple failed logins or firewall intrusion attempts). However, the effectiveness of monitoring is limited by the scope of logs and rules; since the internal network is not segmented, internal traffic is not well monitored for lateral movement. Additionally, the SIEM's use could be expanded (e.g., to include Windows event logs from all servers, VPN logs, etc., if not already ingested). Despite these limitations, the presence of a SIEM indicates moderate maturity in continuous monitoring.
Detect	DE.DP: Detection Processes	1	Formal processes for handling detected events are lacking. While the IT team investigates alerts that Splunk or antivirus generate, there are no written procedures or playbooks defining how to triage, escalate, or respond to various types of security incidents. The organization does not have a dedicated Security Operations Center (SOC); monitoring is done as a part-time responsibility by IT staff. There is no established threshold for when to involve management or external specialists based on an alert. In practice, detection and response are reactive: if something suspicious is noticed, IT will

			troubleshoot it, but this is not guided by a clear process or assignment of roles.
Respond	RS.RP: Response Planning	0	There is no formal incident response (IR) plan documented. The organization has not developed incident handling playbooks or defined an incident classification/severity scheme. In the event of a cybersecurity incident (e.g., malware outbreak or data breach), response actions would be improvised. This lack of planning means critical steps could be missed under pressure. The team does not have a clear assignment of incident roles (e.g., who acts as incident coordinator, communications lead, etc.), which would cause confusion during a crisis.
Respond	RS.CO: Communications	1	Communication pathways during incidents are informal. There is an understanding that IT staff would notify the IT manager and possibly executives if a major incident occurs, but no established communication plan exists for notifying internal stakeholders, customers, regulators, or law enforcement. For example, there are no pre-drafted incident notification templates or call trees. The organization would likely handle communications on the fly, which risks delays or inconsistent messaging in a fast-moving incident.
Respond	RS.AN: Analysis	1	The capability to analyze and investigate security incidents is limited. The IT team can perform basic analysis (e.g., checking logs in Splunk, isolating affected systems), but they do not have advanced forensic tools or training. There is no procedure for in-depth root cause analysis or preserving evidence for a potential legal investigation. Any analysis performed depends on the individual skills of the IT staff at the time and is not guided by an incident analysis framework. This could result in incomplete understanding of incidents and issues repeating.
Respond	RS.MI: Mitigation	1	When security events occur, the approach to mitigation is ad hoc. For minor incidents (e.g., a malware-infected PC), the IT staff will take steps like disconnecting the device and running antivirus scans. However, without an incident response plan, more complex incidents might not be handled effectively. There is no defined set of mitigation actions for different incident types (such as containment, eradication, and recovery steps). The organization's general philosophy is to fix issues as they arise (aligning with their risk posture to mitigate), but due to lack of preparation, this could be slow or flawed under real attack conditions.
Respond	RS.IM: Improvements	0	The organization does not conduct post-incident reviews or lessons-learned exercises formally. Since there is no structured incident management, there is likewise no process to document what went well or poorly after an incident and to update procedures accordingly. For example, if a phishing attack succeeded, the company might address the specific issue (mitigate it) but would not systematically analyze why it happened or update training and processes to prevent a recurrence. This lack of improvement mechanism means the incident response capability does not mature over time.

Recover	RC.RP: Recovery Planning	0	A disaster recovery (DR) or business continuity plan is not formally documented for IT systems. The company relies on regular data backups for critical applications (databases, transaction systems) and assumes that IT staff will be able to rebuild systems from backups if needed. However, there is no defined recovery time objective (RTO) or recovery priority for systems, and no step-by-step recovery procedures have been written. In a scenario such as a ransomware attack or major outage, the lack of a coordinated recovery plan could significantly delay restoration of services.
Recover	RC.IM: Improvements	0	There is no ongoing improvement process for recovery capabilities. Because formal recovery plans and testing are absent, the organization has not engaged in periodic drills or post-recovery analyses. As a result, they have not identified gaps (e.g., missing backup for a system, or time to recover being too long) in a structured way. Any improvements to backup or restoration processes happen in an ad hoc fashion (often after minor operational issues), rather than through lessons learned from simulated disasters.
Recover	RC.CO: Communications	1	Communication during recovery efforts is minimally planned. Internally, IT would inform management about system outages and progress in restoring systems, but this is not guided by a communication plan. Externally, there is no predefined process to update customers or partners if a cyber incident causes a prolonged service disruption. For example, if online services were down for several days, the team would scramble to craft notices or regulatory reports at that time. The lack of a prepared communication strategy for recovery can lead to stakeholder frustration and reputational damage during a crisis.

(Note: Each category score is based on observed controls relative to NIST CSF best practices. Scores of 0–1 indicate areas with significant gaps or minimal implementation, 2 indicates moderate implementation, and 3 would indicate a high level of maturity. No category in this assessment scored a 3, reflecting that there are no areas fully meeting top-tier cybersecurity practices at this time.)

Gap Analysis and Prioritized Recommendations

Based on the detailed results above, the assessment identified several critical gaps in the organization's cybersecurity controls. This section highlights the most significant gaps, their implications, and recommended actions to address them. The gaps are prioritized by risk level (impact and likelihood), with an understanding that the organization intends to mitigate high risks as a priority (consistent with its risk posture).

1. Lack of Multi-Factor Authentication (MFA) – *High Risk*: The absence of MFA for user and administrator logins is a serious gap. Without MFA, user accounts (especially those with privileged access or remote access) are vulnerable to compromise through phishing or password brute-force attacks. In the finance sector, account compromise can lead to unauthorized transactions or data breaches.

Recommendation:*Implement MFA on all critical systems and remote access immediately.*Priority: Very High (urgent mitigation). This should cover VPN access, core financial applications, email, and administrative access to servers and network devices.

MFA significantly reduces the risk of stolen credentials being used to breach systems. There are low-cost, quick-deployment options (e.g. integrating with an existing directory or cloud-based MFA services) that make this a feasible short-term project.

2. No Network Segmentation – *High Risk*: The internal network is flat with no segmentation, meaning that once inside the network, an attacker could freely reach most systems. In a finance environment, sensitive systems (e.g., databases with customer data or payment systems) should be isolated on separate network segments with strict access controls. The current architecture increases the potential impact of any breach (allowing threats to spread laterally, such as malware or an intruder moving between servers).

Recommendation:*Design and implement network segmentation.*Priority: High. Create VLANs or subnetworks to separate critical servers, user workstations, and guest/third-party networks. For example, isolate the core banking/database servers from the corporate office network and restrict access to only authorized services. This may involve reconfiguring switches and existing firewalls to enforce internal access controls. Starting with high-value assets, introduce segmentation gradually. Network segmentation will contain attacks and is a fundamental security best practice. (This may be a multi-phase project, but initial segmentation of the most critical assets should be done as soon as possible.)

3. Legacy Unsupported Systems (Windows Server 2003 with Critical Vulnerabilities) – *High Risk*: Running end-of-life systems with known vulnerabilities poses a direct threat. Windows Server 2003 has not received security patches for many years; any known exploit could be used by an attacker to gain control of these servers. Given these servers likely host important applications (since they haven't been decommissioned), their compromise could lead to data loss, service downtime, or entry into the broader network.

Recommendation:*Retire or upgrade legacy systems as a top priority.*Priority: High. Develop a plan to replace Windows Server 2003 instances with supported operating systems (such as Windows Server 2019/2022 or a hardened Linux alternative if applicable). If an immediate upgrade is not possible (due to application compatibility), implement compensating controls: isolate these legacy servers on their own network segment with strict firewall rules, minimize user access, and apply any available third-party security patches or virtual patching solutions. Additionally, expedite procurement or development of updated software to migrate off these legacy platforms.

4. Outdated Perimeter Firewalls – *Medium-High Risk*: While firewalls are in place, the Fortinet devices are running outdated software (and possibly older hardware models). This can result in missed detection of newer threats and potential unpatched vulnerabilities in the firewall itself. For a financial organization, perimeter defense is critical and should be up-to-date to withstand modern attack techniques. An outdated firewall might also lack features like deep packet inspection or up-to-date threat intelligence feeds.

Recommendation:*Update or replace firewall infrastructure*.Priority: High (for updates), Medium (for longer-term replacement if needed). In the short term, update the Fortinet firewall firmware to the latest stable version to patch known vulnerabilities. In the medium term, consider replacing or upgrading the firewall appliances to newer models that support advanced security features (such as intrusion prevention systems, application control, and SSL inspection). Ensure the firewall ruleset is reviewed and tightened during this process (e.g., only required ports are open, and logging is enabled for allowed traffic). Given that the firewalls are a key security layer, maintaining them is essential.

5. Weak Incident Response Preparedness – *Medium Risk*: The organization lacks a formal incident response plan and defined procedures for security incidents. This gap means that if a serious incident occurs (e.g., a data breach or malware outbreak), the response may be chaotic or slow, potentially exacerbating damage. Regulators in the finance industry expect documented incident response capabilities and timely incident reporting.

Recommendation:*Develop and implement an Incident Response Plan*.Priority: Medium. This should include creating a written incident response policy and playbooks for common incident types (malware infection, unauthorized access, data breach, etc.). Define roles (incident commander, technical lead, communications lead, etc.) and escalation pathways (when to involve executives or external partners such as forensic consultants or legal counsel). Training the IT staff and conducting a tabletop exercise to practice the incident response plan are also recommended once the plan is in place. While this is not as immediately urgent as plugging technical vulnerabilities, it is important for compliance and will significantly improve readiness.

6. Inadequate Data Protection and Backup/Recovery Processes – *Medium Risk*: There is no formal data classification or data loss prevention program, and recovery planning is not documented. Although backups exist, the lack of a documented recovery strategy means the organization might struggle to restore operations after a severe incident. Additionally, absence of data classification could lead to inconsistent protection (some sensitive data might not be encrypted or backed up properly). In finance, failure to recover data or services quickly can have regulatory and reputational consequences.

Recommendation:*Enhance data protection and recovery planning*.Priority: Medium. Implement a data classification scheme to identify which data is most sensitive or mission-critical (e.g., customer financial data vs. internal documents) and apply appropriate controls (encryption, access restrictions, monitoring) to each category. Concurrently, develop a Disaster Recovery (DR) and Business Continuity Plan that outlines how critical systems would be restored in various scenarios (cyberattack, hardware failure, etc.). This plan should define RTOs/RPOs (Recovery Time/Objectives) for key services. Also, regularly test backups and recovery procedures (e.g., annual DR drills) to ensure data integrity and team preparedness.

7. Security Awareness Deficiencies – *Medium Risk*: Employees are not receiving adequate cybersecurity training, which increases the risk of social engineering attacks (phishing, fraud). In a finance organization handling sensitive transactions, users need to be vigilant. The lack of ongoing training and phishing awareness can lead to incidents that technical controls might not prevent.

Recommendation:*Implement a comprehensive security awareness training program*.Priority: Medium. This program should include regular (e.g., quarterly) training sessions or online modules for all staff, covering topics like phishing detection, safe use of company systems, and data protection responsibilities. Include periodic phishing email simulations to test and reinforce awareness. Also, provide specialized training for high-risk roles (IT administrators on advanced security, finance staff on fraud schemes, etc.). Improving user awareness is a low-cost, high-impact way to prevent incidents.

8. Gaps in Formal Security Processes and Policies – *Medium Risk*: Many security processes (asset management, patch management, change control, vendor risk management) are informal. Policies are outdated and not comprehensive. This lack of structure can lead to important tasks being neglected and inconsistent security practices. For instance, without a patch management policy and schedule, critical updates may be missed (as happened with the legacy systems).

Recommendation:*Establish and update security policies and procedures*.Information Security PolicyPriority: Medium-Low Develop a formal that outlines the organization's approach to each major area of security (access control, maintenance, incident response, acceptable use, etc.). From that, derive specific procedures/runbooks for IT staff – e.g., a Patch Management Procedure (monthly review of patches, testing, deployment priority for critical patches), Change Management Procedure (ensuring security review for any IT changes), and Third-Party Risk Management Procedure (assessing vendors annually or during onboarding for their security controls). Also assign clear responsibilities for these processes (who is the owner of asset inventory, who reviews firewall rules quarterly, etc.). Over time, these formal processes will improve consistency and accountability. (important for long-term maturity, but after critical technical gaps are addressed).

Other identified issues (such as lack of advanced endpoint protection, missing network intrusion detection internally, etc.) are noted but are considered lower priority or naturally addressed by the above recommendations. For example, once network segmentation and firewall upgrades are in place, implementing internal intrusion detection systems or sensors can be considered to further improve detection (a possible future project). Similarly, while supply chain risk management is currently minimal, as a medium-risk area the organization can accept it in the short term but should plan to formalize vendor security assessments in the longer term.

In summary, the highest priority items are those that directly close avenues for attackers (MFA, segmentation, patching legacy systems, firewall updates). These should be tackled first to **reduce immediate risk exposure**. Subsequently, improving organizational preparedness (incident response planning, disaster recovery capability, training, and policies) will build resilience. The recommendations align with the company's intent to mitigate risks – by acting on these, the organization will address all high-risk gaps rather than accepting them. Each recommendation is mapped to relevant CSF categories and will raise the scores in those areas as implemented. The next section provides a phased improvement plan to execute these recommendations in a manageable sequence.

Improvement Plan (Roadmap with Timeline and Effort Estimates)

To achieve the target security posture, we propose a phased improvement plan. The plan breaks down the recommended remediation actions into short-term, medium-term, and long-term initiatives. This scheduling takes into account the urgency of risks, the complexity of implementation, and resource requirements. Each action is annotated with an estimate of the effort and resources needed (low, medium, high), and is linked to the CSF category it strengthens. The organization's strategy is to **mitigate high risks immediately** and address medium risks in a planned manner; low-risk items and refinements are scheduled for the long term.

Short-Term Actions (0–3 months, Quick Wins)

These initiatives address the most critical gaps and can be started right away. They typically require modest resources or are extensions of existing capabilities:

- **Implement Multi-Factor Authentication (MFA)** *(CSF: PR.AC)* – **Effort:** Moderate. Enable/configure MFA for all users, especially for VPN, email, and administrative accounts. This may involve using existing identity management systems (e.g., enabling MFA in Office 365/Azure AD or VPN appliance). **Resources:** Will require an MFA service or software (subscription or on-premise), and IT staff time for integration and user rollout. Expected to significantly improve Access Control security with minimal cost (many solutions are pay-per-user and affordable) and manageable user training (communication and support for initial setup).
- **Urgent Patching and Isolation of Critical Vulnerabilities** *(CSF: PR.MA & PR.PT)* – **Effort:** Moderate. Immediately apply available security updates to any systems and network devices that are behind on patches (especially internet-facing systems like the firewall). For the Windows Server 2003 machines, since they cannot be patched, isolate them as a temporary containment: restrict network access to only what is absolutely necessary for operations (using firewall rules or VLAN ACLs). **Resources:** IT staff time to perform updates during maintenance windows,

possibly support from a vendor for legacy system isolation. This action quickly reduces the exposure of known vulnerabilities while longer-term fixes (system upgrades) are in progress.

- **Initial Network Segmentation for High-Value Assets** *(CSF: PR.PT & PR.AC)* – **Effort:** Moderate. As a quick first step, segment the most critical server (or group of servers) from the rest of the network. For example, place the core financial database server in a separate VLAN with a firewall rule restricting access to only the application server that needs to communicate with it. **Resources:** Network engineer time to create VLANs and adjust firewall rules. Existing network hardware likely supports VLANs, so no significant cost. This provides immediate risk reduction by protecting key assets while a more comprehensive segmentation plan is developed.
- **Develop Basic Incident Response Procedure** *(CSF: RS.RP & RS.CO)* – **Effort:** Low. In the immediate term, create a simple incident response cheat-sheet or call tree. Identify who should be contacted in common incident scenarios (IT manager, CTO, external security partner) and what initial steps to take (e.g., isolate affected system, gather logs). **Resources:** Minimal – this is largely documentation effort by the IT/security manager. While a full IR plan takes longer (see medium-term actions), having a basic procedure now ensures the team isn't completely unprepared if an incident occurs tomorrow. This will slightly improve Respond capabilities and is aligned with the mitigation-oriented strategy (being prepared to act reduces impact).
- **Security Awareness Communication** *(CSF: PR.AT)* – **Effort:** Low. Kick off a basic security awareness initiative: for example, send out an organization-wide email or short training video about the importance of strong passwords and identifying phishing emails (especially since MFA is being rolled out). **Resources:** Low, can use free materials or internally developed content. This sets the stage for a more formal training program later and begins to address the human element of security immediately.

Medium-Term Actions (3–12 months, **Planned Improvements**)

Medium-term initiatives require more planning, resources, or possible procurement of solutions. They aim to fully remediate high-risk issues and tackle important medium-risk gaps:

- **Replace/Upgrade Legacy Systems and Software** *(CSF: PR.MA & ID.RA)* – **Effort:** High. Execute the project to **migrate off Windows Server 2003**. This involves procuring new server hardware or VMs and installing a supported OS (Windows Server 2019/2022). Also, migrate or upgrade the applications running on those legacy servers. Testing is needed to ensure compatibility. **Resources:** Significant – will require capital expense for new licenses/hardware and substantial IT staff or contractor time to perform migration and testing. May involve vendor support if a third-party application runs on those servers. This action eliminates a high risk and moves maintenance practices into a managed state.

- **Comprehensive Network Segmentation Project** *(CSF: PR.PT & PR.AC)* – **Effort:** High. Building on the initial segmentation, design a **network architecture overhaul** that segments the entire network by trust zones (e.g., Workstations, Servers, DMZ, Guest network, Development environment, etc.). Implement internal firewalls or use existing firewall with internal interfaces to enforce access controls between segments. **Resources:** High – possibly need to purchase additional firewall modules or licenses for internal segmentation, consulting support for network redesign, and significant effort by network engineers. User testing and careful roll-out will be required to avoid disrupting business processes. This project, while resource-intensive, will greatly enhance the organization's defensive posture and is crucial for a finance firm handling sensitive data.
- **Upgrade Firewall and Perimeter Security** *(CSF: PR.PT & DE.CM)* – **Effort:** Medium. Evaluate the current Fortinet firewall appliances for replacement or enhancement. If the hardware is old or underpowered, budget for new next-generation firewall appliances that include modern threat protection features. If replacing, plan for deployment, configuration migration, and testing. If the decision is to keep current hardware longer, ensure the firmware is now up-to-date (from short-term action) and maybe augment with an intrusion detection/prevention system (IDS/IPS) on the network. **Resources:** Medium to High (depending on replace vs. upgrade). New firewalls involve capital expense and possibly training IT staff on the new platform. If remaining on current hardware, perhaps just a moderate cost for an IDS appliance or subscribing to threat intel feeds. Upgraded perimeter security will help detect and block threats and is expected by regulators for financial institutions.
- **Formalize the Incident Response Plan** *(CSF: RS.RP, RS.MI, RS.CO)* – **Effort:** Moderate. Expand the basic procedures created earlier into a **full Incident Response Plan** document. This includes incident severity levels, detailed steps for analysis and containment, and notification procedures (who contacts legal/regulatory, how to communicate to media or clients if needed). Conduct an incident response training session with the IT team and a simulated incident drill to test the plan within this timeframe. **Resources:** Moderate – primarily staff time; may involve engaging a security consultant to help draft the plan or run a workshop. Improves compliance and readiness significantly with a relatively contained effort.
- **Implement Security Awareness Training Program** *(CSF: PR.AT)* – **Effort:** Moderate. Adopt a more structured training regimen. This could involve licensing an online security awareness training platform or incorporating it into existing HR training systems. Roll out an initial comprehensive training to all employees, then schedule periodic refreshers and phishing simulation exercises throughout the year. **Resources:** Moderate – some budget for a training service, and coordination by HR/IT. Possibly leverage industry offerings specifically for financial sector threats (like

social engineering scenarios related to finance). This will cultivate a security-aware culture and reduce the likelihood of human errors leading to incidents.

- **Enhance Monitoring and Detection Capabilities** *(CSF: DE.AE, DE.CM)* – **Effort:** Moderate. Tune and expand the use of the **Splunk SIEM**. Now that network segmentation is being implemented, ensure new segments' logs/alerts are integrated. Create more advanced correlation rules or use-case alarms (e.g., alert on a high volume of data leaving a sensitive segment, or an admin account login at an odd hour). If budget permits, consider adding endpoint detection and response (EDR) software on critical servers and workstations, feeding events into the SIEM for better anomaly detection. **Resources:** Moderate – may require professional services to develop SIEM content or additional license costs for more log sources or an EDR tool. This step will increase the Detect function maturity, helping catch any issues that slip past preventive controls.
- **Update and Create Key Security Policies** *(CSF: ID.GV, PR.IP)* – **Effort:** Low. By the mid-point of the year, draft and formalize the various security policies and procedures that were lacking. Prioritize policies such as: Access Control Policy (with the new MFA requirements), Acceptable Use Policy, Change Management Policy, Patch Management Policy (covering how updates like those on servers and firewalls are handled regularly), and a Data Protection Policy (covering classification and handling requirements). Also introduce a Third-Party Security Policy outlining how vendor risk is assessed. **Resources:** Low to Moderate – largely documentation work by the security officer/IT manager, possibly reviewed by legal or compliance staff to ensure alignment with any regulatory requirements. These policies will provide governance structure to maintain all implemented improvements long-term.

Long-Term Actions (12+ months, **Sustaining and Maturing**)

Long-term initiatives focus on sustaining the improvements and tackling remaining areas once the critical issues are resolved. These may also align with strategic goals or compliance mandates:

- **Business Continuity/Disaster Recovery (BC/DR) Program Enhancement** *(CSF: RC.RP, RC.CO)* – **Effort:** Moderate. Develop a comprehensive BC/DR plan for the organization if not already initiated. This involves business impact analysis to identify critical business functions, establishing redundancy or failover for key systems (perhaps utilizing cloud services or offsite backups), and defining procedures to recover operations within acceptable timeframes. Conduct annual DR tests (simulating, for example, a data center outage or ransomware scenario) to validate the recovery plan and make improvements (RC.IM). **Resources:** Moderate – will require cross-department effort (not just IT, but business units, management) and possibly investment in backup infrastructure or contracts with disaster recovery service

providers. In the long run, this ensures the company can withstand and quickly recover from major incidents, reducing downtime and financial losses.

- **Continuous Security Improvement and Auditing** *(CSF: RS.IM, ID.RA)* – **Effort:** Low to Moderate. Establish a cycle of periodic reviews and audits to keep the security program up to date. For example, conduct **annual NIST CSF assessments** or audits against regulatory standards to measure progress (improving the scores documented in this report). Perform routine vulnerability assessments quarterly to catch new issues early. Have management review risk acceptance decisions for any medium risks that were left (ensuring they remain acceptable or are eventually mitigated). **Resources:** Low to Moderate – could be handled internally for vulnerability scans, but an external auditor or security consultant might be engaged annually for an unbiased review. This ensures that security improvements are not one-time, but rather continuously evolving (the organization moves toward NIST CSF Tier 3: Repeatable).
- **Advanced Security Implementations** *(CSF: PR.PT, DE.CM)* – **Effort:** Moderate to High (depending on the solution). After shoring up the basics, consider deploying more advanced controls common in the finance industry for higher security assurance. Examples include: **Data Loss Prevention (DLP) solutions** to monitor and prevent unauthorized transfer of sensitive data; **Database encryption** and/or tokenization for sensitive financial data at rest; **Network Access Control (NAC)** to enforce device authentication and health checks when connecting to the network; **Threat intelligence integration** into the SIEM for early warning of relevant threats; and possibly **Zero Trust Architecture** principles (continuously verifying user/device identity for access to resources). These initiatives require careful planning and investment, so they are slated for long-term. **Resources:** High – each advanced solution might require new software, hardware, and training. These will further align the security posture with industry-leading practices and may become necessary as the company grows or faces stricter regulatory environments.
- **Formal Governance and Risk Management Integration** *(CSF: ID.GV, ID.RM)* – **Effort:** Low. Over the long term, management should integrate cybersecurity into corporate governance. This could mean regular board reporting on cybersecurity, assigning a senior executive (CISO or similar) responsibility for security oversight, and maintaining a risk register that includes cybersecurity risks with defined owners and mitigation plans. **Resources:** Low – mainly a shift in management process and oversight. This ensures that the security program remains aligned with business objectives and that there is accountability at the highest levels for managing cyber risk, which is especially important in the finance sector where regulatory scrutiny is high.

For each of the above actions, it is recommended to assign an owner, define a timeline, and secure necessary budget early. The short-term actions are either already underway or should begin immediately to address glaring vulnerabilities. Medium-term actions should be planned in the upcoming budgeting cycle and initiated as projects with clear milestones. Long-term

actions may span multiple budget cycles and should be revisited as the threat landscape and business context evolve.

By following this improvement plan, the organization is expected to considerably raise its NIST CSF category scores (with most categories reaching a 2 or 3 within 1-2 years, from the 0-1 in many areas currently). This phased approach balances quick risk reduction with sustainable program development, aligning with the organization's mitigation-centric risk strategy. Progress should be monitored, and this plan adjusted as needed based on any incidents, new risks, or changes in business strategy.

Attachments

The following attachments provide supporting evidence and detailed information collected during the assessment:

- **NIST CSF Assessment Checklist (Completed):** The filled evaluation checklist detailing scores for all CSF sub-categories, along with evaluator notes. This is the working document that supports the summary ratings in the Detailed Evaluation section.
- **Technical Evidence Artifacts:** Relevant technical data gathered from the environment, including:
    - Network diagrams and configuration snippets (illustrating the current flat network topology and firewall setup).
    - Vulnerability scan reports (highlighting critical findings such as the Windows Server 2003 vulnerabilities and outdated firewall firmware versions).
    - System screenshots and logs (e.g., screenshots from the Active Directory showing lack of MFA enforcement, SIEM log summary showing types of events captured).
    - Inventory extracts (listing hardware/software assets and their details, used for assessing asset management).
- **Policies and Documentation Reviewed:** Copies of or excerpts from existing organizational documents that were analyzed during the assessment, such as:
    - Any current IT security policies or employee handbook sections related to security (to check for coverage of MFA, acceptable use, etc.).
    - IT operational procedures (backup schedules, patch logs, if available).
    - Incident handling or business continuity documents (if any existed in draft or partial form).

- Vendor contracts or security addenda (to evaluate supply chain risk management practices, if available).