IT Infrastructure Vulnerability Assessment Financial Firm

1. Executive Summary

This assessment provides an overview of the current vulnerabilities identified in the IT infrastructure of the financial firm. The assessment covers servers, networks, endpoints, cloud assets, and applications, with the intent to mitigate risks and enhance the organization's cyber resilience.

2. Scope of Assessment

- Firewall and Perimeter Devices
- Internal Networks (LAN/WAN)
- Servers (Windows, Linux)
- Workstations and Endpoints
- Databases
- Cloud Infrastructure
- Critical Web Applications

3. Methodology

- Automated vulnerability scanning
- Manual verification and analysis
- Configuration and policy review
- Interviews with IT personnel

4. Key Findings

Vulnerability	Affected Assets	Risk Level	Description
Unpatched Operating Systems	Servers, Workstations	High	CVE exposures due to missing security updates on critical systems.
Weak Authentication	VPN Gateway	High	Absence of multi-factor authentication.
Open Management Ports	Firewall, Database Server	Medium	Non-essential ports exposed to public networks.
Default Credentials	Network Devices	Medium	Default admin accounts detected on two routers.
Insecure Application Code	Web Portal	Medium	Input validation missing, risk of injection attacks.

5. Recommendations

- Implement strict patching procedures for all servers and workstations.
- Enforce multi-factor authentication on all remote access systems.
- Restrict management port access using firewalls and network segmentation.
- Change or remove default credentials from all network devices.
- Conduct secure code reviews and application penetration testing.

6. Conclusion

Addressing the identified vulnerabilities is crucial for protecting the firm's sensitive financial information. Regular vulnerability assessments and timely remediation efforts are recommended to maintain a robust security posture.