Remote Access Risk Assessment Template – Community Bank

1. Purpose and Scope

This risk assessment evaluates the security, regulatory, and operational risks associated with remote access to the bank's internal systems, including access by employees, contractors, and third-party service providers. This assessment supports compliance with FFIEC guidance and GLBA Section 501(b).

2. Remote Access Inventory

Remote Access Method	Description	Users	Systems Accessed
VPN (SSL/IPSec)	Secure tunnel for employee access	Internal staff	Core banking apps, file shares
RDP over VPN	Remote desktop via VPN tunnel	IT staff	Admin interfaces, servers
Vendor VPN Access	Restricted VPN access for vendors	MSP, core processor	Specific systems
Mobile App Access	iOS/Android app connectivity	Relationship staff	CRM, scheduling

3. Threats and Vulnerabilities

Entry Point	Threats	Vulnerabilities
VPN	Credential theft, MITM	Weak MFA, stale accounts
RDP	Brute force attacks	Open ports, weak passwords
Vendor VPN	Over-privileged access	Lack of network segmentation
Mobile	Device theft, data leakage	No MDM, lack of encryption

4. Risk Evaluation

Risk Description	Likelihood	Impact	Risk Level
VPN access lacks session timeout	Medium	High	High
Vendor access uses shared credentials	High	High	Critical
Mobile devices lack encryption	Medium	Medium	Medium

5. Control Review

Control	Description	In Place?	Effective?
MFA for remote access	Required for all VPN logins	Yes	Yes
Vendor access policy	Contractual + IP restrictions	Yes	Partial
Mobile device policy	MDM enforced with wipe-on-failure	No	N/A

6. Recommendations

Issue	Recommended Action	Priority
Shared vendor accounts	Issue named accounts with access logs	High
Lacking mobile MDM	Deploy MDM for all corporate devices	High
VPN firmware outdated	Apply latest vendor security patches	Medium

7. Residual Risk Analysis

Residual risk remains for vendor VPN abuse. Short-term mitigations include logging and alerting. Full mitigation requires contract updates and network segmentation.

8. Review and Approval

Prepared by: [ISO Name]

Date: [Date]

Reviewed by: [IT Director Name]

Approved by: [Senior Management or Board]

Appendices

- Appendix A: VPN Connection Logs Summary

- Appendix B: Remote Access Policy Excerpts

- Appendix C: Vendor List with Access Levels