**FDIC VPN and RA Controls**

**Multi-Factor Authentication (MFA):** Implementing robust MFA is crucial for securing remote access. This goes beyond simple two-factor authentication and may include enhanced MFA (EMFA) or hardware tokens for business/commercial banking

**Strong Password Policies:** Enforcing complex, unique passwords and regular password changes helps prevent credential compromise. This is especially important given that 50% of IT professionals reuse passwords across work accounts

**Encryption:** Ensuring all remote connections and data transmissions are encrypted using strong protocols to protect sensitive financial information

**Network Segmentation:** Implementing proper network segmentation to limit access to only necessary resources for remote workers

**Endpoint Security:** Requiring up-to-date antivirus, anti-malware, and personal firewall software on all devices used for remote access

**Secure VPN Configuration:** Properly configuring VPNs with strong encryption, authentication, and access controls

**Continuous Monitoring and Logging:** Implementing systems to monitor and log all remote access activities for detecting and responding to potential security incidents

**Regular Security Assessments:** Conducting periodic vulnerability assessments and penetration testing of remote access systems

**User Education and Training:** Providing comprehensive security awareness training for employees on safe remote working practices, including recognizing phishing attempts and proper handling of sensitive data

**Access Control and Least Privilege:** Implementing strict access controls and following the principle of least privilege to ensure users only have access to resources necessary for their roles

**Secure Communication Channels:** Establishing reliable and secure communication channels for remote teams to collaborate effectively

**Incident Response Plan:** Developing and maintaining a robust incident response plan specifically tailored for remote access scenarios