**Note to Candidate:**  
To protect confidentiality, we have not included actual control descriptions from a bank. Instead, the controls provided in this case study are hypothetical and crafted to reflect the structure and content commonly used in banking practices.

**Sample Internal Controls for Cyber Risk**

1. **Control-ID: CYR-001**  
   **Control Name:** Multi-Factor Authentication (MFA) Implementation  
   **Description:** Ensure that all critical systems and applications require multi-factor authentication for user access. This includes implementing MFA for internal employees, external contractors, and third-party vendors with system access.
2. **Control-ID: CYR-002**  
   **Control Name:** Regular Vulnerability Assessments  
   **Description:** Conduct monthly vulnerability scans on all internal and external systems to identify and address potential security weaknesses. Document and track remediation efforts through a centralized ticketing system.
3. **Control-ID: CYR-003**  
   **Control Name:** Endpoint Protection and Monitoring  
   **Description:** Deploy endpoint detection and response (EDR) tools across all user devices and servers to monitor and block malicious activity. Ensure that antivirus software is installed, updated, and configured to run real-time scans.
4. **Control-ID: CYR-004**  
   **Control Name:** Cyber Incident Response Plan (CIRP)  
   **Description:** Maintain and periodically test a Cyber Incident Response Plan to ensure prompt and effective response to cyber incidents, including ransomware, data breaches, and phishing attacks. Document results and lessons learned from all incident response exercises.
5. **Control-ID: CYR-005**  
   **Control Name:** Secure Configuration Baselines  
   **Description:** Establish and enforce secure configuration baselines for all servers, network devices, and applications. Periodically review baselines to align with evolving cybersecurity standards (e.g., CIS Benchmarks).
6. **Control-ID: CYR-006**  
   **Control Name:** Data Encryption and Key Management  
   **Description:** Ensure that all sensitive data is encrypted both at rest and in transit using industry-standard encryption protocols. Implement a centralized key management solution to securely store and rotate encryption keys.
7. **Control-ID: CYR-007**  
   **Control Name:** Access Privilege Reviews  
   **Description:** Conduct quarterly reviews of user access privileges to critical systems. Remove access for terminated employees and adjust access rights based on changes in job roles or responsibilities.
8. **Control-ID: CYR-008**  
   **Control Name:** Cybersecurity Awareness Training  
   **Description:** Provide mandatory cybersecurity awareness training for all employees at least annually. Include modules on phishing prevention, password security, and reporting suspicious activities.
9. **Control-ID: CYR-009**  
   **Control Name:** Network Segmentation  
   **Description:** Implement network segmentation to isolate critical systems and limit lateral movement of potential attackers. Enforce strict access controls between network segments using firewalls and access control lists (ACLs).
10. **Control-ID: CYR-010**  
    **Control Name:** Third-Party Cyber Risk Management  
    **Description:** Require all third-party vendors with access to bank systems or data to adhere to the bank's cybersecurity policies. Conduct annual assessments of vendor cybersecurity controls and address any identified gaps.
11. **Control-ID: CYR-011**  
    **Control Name:** Continuous Security Monitoring  
    **Description:** Deploy a Security Information and Event Management (SIEM) system to collect and analyze logs from critical systems in real time. Investigate and respond to alerts generated by the SIEM system within defined Service Level Agreements (SLAs).
12. **Control-ID: CYR-012**  
    **Control Name:** Patch Management Process  
    **Description:** Implement a structured patch management process to ensure timely application of security patches for all systems and applications. Prioritize patches for high-risk vulnerabilities based on severity and criticality.