Cybersecurity Risk Assessment for Online Banking Platform

1. Overview

This report aimed to identify, assess, and prioritize cybersecurity risks associated with the launch of the institution's new online banking platform. The goal is to safeguard customer data, protect digital assets, and ensure compliance with financial industry regulations (e.g., GLBA, FFIEC, PCI DSS, NIST).

2. Risk Assessment Methodology

We applied the NIST Risk Management Framework (RMF) and used a qualitative risk matrix approach to rate risks based on:

Likelihood (Low, Medium, High)

Impact (Low, Medium, High)

The combined rating helps determine risk priority.

3. Identified Cybersecurity Risks

Risk ID	Risk Description	Threat Source	Asset Affected
R1	Unauthorized access via compromised credentials	External attacker	Customer accounts, sensitive data
R2	Exploitation of application vulnerabilities (e.g. injection attacks, XSS)	Hacker, script kiddie	Platform integrity, data confidentiality
R3	Distributed denial of service (DDoS) attack	Botnet	Platform availability
R4	Insecure API inetgration with third party services	Third party vendor	Data flow security, platform trust
R5	Phishing and social engineering attacks	Social engineer	Customer login credentials

	targeting customers		
R6	Insider threats (misuse or accidental breach)	Internal employee	Data leakage, fraud
R7	Inadequate encryption for data in transit or at rest	Technical flaw	Regulatory non-compliance, data theft

4. Risk Analysis & Prioritization

Risk ID	Likelihood	Impact	Risk level
R1	High	High	Critical
R2	Medium	High	High
R3	Medium	Medium	Medium
R4	Medium	High	High
R5	High	Medium	High
R6	Low	High	Medium
R7	Low	High	Medidum

Top Priority Risks: R1, R2, R4, R5

5. Mitigation Strategies

Based on FFIEC guidelines, NIST SP 800-53, and industry standards, here are the proposed mitigation strategies for the top risks:

R1: Unauthorized Access

Mitigation Measures:

- Enforce Multi-Factor Authentication (MFA) for all users
- Implement adaptive access controls (geo-fencing, device ID)
- Enable real-time fraud detection & account lockout thresholds
- Conduct regular credential stuffing simulations

R2: Application Vulnerabilities

Mitigation Measures:

- Adopt Secure SDLC practices with OWASP ASVS integration
- Perform regular code reviews and dynamic testing (DAST)
- Conduct quarterly penetration testing
- Enforce WAF (Web Application Firewall) with real-time threat intelligence

R4: Insecure APIs

Mitigation Measures:

- Apply OAuth 2.0 with strong API authentication
- Use API gateways to control and monitor access
- Encrypt API traffic using TLS 1.3
- Validate inputs and throttle requests

R5: Phishing Attacks

Mitigation Measures:

- Launch customer education campaigns on phishing
- Use DMARC, DKIM, and SPF to authenticate outbound emails
- Deploy email filtering and anomaly detection
- Add transaction verification alerts (SMS/Push)

6. Summary of Risk Management Process

Step	Activity
Identify	Reviewed platform architecture, integration points and past incident data
Assess	Used NIST based criteria to evaluate risk likelihood and impact
Prioritize	Mapped risks using a qualitative matrix
Respond	Proposed layered security controls aligned to regulatory guidance
Monitor	Recommended continuous monitoring using SIEM and automated compliance tools

7. Recommendations Summary

Priority	Action	Timeline
High	Implement MFA & anomaly detection	Immediate
High	Conduct full app & API security audit	Within 30 days
High	Launch phishing awareness program	Within 45 days
Medium	Evaluate insider access & logging	Ongoing
Medium	Update encryption policies	Within 60 days

Conclusion

The new online banking platform introduced powerful customer benefits, but it also expanded the institution's cyber risk surface. My assessment identified the most critical cybersecurity risks, and my recommendations ensure that confidentiality, integrity, and availability are maintained. These measures also support compliance with key financial regulations and reduce legal exposure.