Executive Cyber Risk Assessment Summary

1. Overview

This assessment was conducted for a mid-sized healthcare services organization handling regulated patient data. The objective was to identify cybersecurity risks, evaluate their potential impact on business operations and compliance, and recommend remediation strategies. The assessment followed **NIST SP 800-30** methodology, with control alignment to **NIST SP 800-53** and **ISO/IEC 27001**.

2. Scope of Assessment

The assessment covered key organizational assets including:

- Electronic Health Record (EHR) system.
- Patient database.
- Cloud storage environment.
- Internal networks and endpoints.
- Third-party billing vendor.

The scope included evaluation of threats, vulnerabilities, existing controls, and compliance gaps.

3. Key Risk Findings

The assessment identified several high and medium risks that could significantly impact confidentiality, integrity, and availability of sensitive healthcare data. The most critical risks included phishing attacks targeting the EHR system, ransomware affecting patient databases, cloud access misconfigurations, insider threats, and third-party security gaps. High-risk findings were prioritized based on likelihood, impact, and regulatory exposure.

4. Business Impact

If exploited, these risks could result in:

- Regulatory non-compliance (HIPAA violations).
- Financial penalties and legal exposure.
- Operational disruptions to healthcare services.
- Reputational damage and loss of patient trust.

5. Recommendations

To reduce overall cyber risk, the following actions are recommended:

- Implement multi-factor authentication (MFA) for critical systems.
- Strengthen backup and disaster recovery testing procedures.
- Enforce least-privilege access and regular access reviews.
- Establish a formal third-party risk management (TPRM) program.
- These actions should be tracked through a formal risk treatment plan with defined ownership and timelines.

6. Conclusion

By addressing the identified control gaps and implementing the recommended remediation strategies, the organization can significantly improve its cybersecurity posture, reduce compliance risk, and better align security controls with business objectives. These findings enable leadership to make informed risk-based decisions aligned with regulatory and business objectives.