***Cybersecurity Risk Faced by the Financial Sector and Risk Assessment Analysis. Using NIST (CSF 2.0)***

**1. Data Breach:**

**Identify**: It was discovered that the financial institution has an inadequate asset inventory of sensitive financial data and no comprehensive risk assessment for external threats. This lack of identification leaves critical assets vulnerable to potential breaches.

**Protect**: The current encryption methods for protecting data both at rest and in transit are weak, and access controls, especially around critical financial systems, are insufficient. These protective measures are inadequate to prevent unauthorized access or data breaches.

**Detect**: There is an absence of real-time monitoring systems designed to detect data exfiltration, and the institution has limited capabilities to detect anomalies in data activity, which makes early detection of breaches challenging.

**Respond**: The institution does not have a clearly defined incident response plan for addressing data breaches. In case of a breach, there is a delay in communicating with stakeholders, which can exacerbate the impact of the breach.

**Recover**: There is no defined recovery plan in place to restore compromised systems and data following a breach. The backup and recovery strategies currently employed are limited, further jeopardizing data integrity in the event of a breach.

**Govern**: The cybersecurity policies in place do not align with the overall business strategy. Additionally, third-party risk management practices are insufficient, increasing the institution's exposure to external risks.

**2. Insider Threat**:

**Identify**: The financial institution lacks effective monitoring of employee activities related to sensitive data. There is also insufficient assessment of insider risks, which increases the vulnerability to insider threats.

**Protect**: The access control policies for privileged users are inadequate, allowing for potential misuse of access by insiders. Additionally, there is a lack of proper security awareness training focused on insider threats, leaving employees ill-prepared to recognize or prevent such risks.

**Detect**: The institution lacks monitoring mechanisms to detect unusual or unauthorized activities by employees. There is no system in place to detect privilege escalation or abuse by insiders, making it difficult to identify insider threats early.

**Respond**: There is no specific response plan tailored to addressing insider threats. Furthermore, the institution lacks clear protocols for handling insider incidents, including appropriate disciplinary actions.

**Recover**: The procedures for reassigning or revoking access after an insider incident are insufficient. Additionally, there is no communication strategy in place to address post-incident concerns, which may affect the institution's ability to recover effectively from an insider threat.

**Govern**: The institution has not clearly defined roles and responsibilities for managing insider threats. Moreover, there is no continuous improvement process in place for managing insider threats, leaving the institution vulnerable to repeated incidents.

**Detailed Findings:**

***1. Data Breach:***

Issue: During the assessment, it was discovered that the encryption methods currently in use for protecting sensitive financial data are outdated and insufficient. Additionally, there are weak access controls around critical financial systems, making them vulnerable to external attacks. The absence of real-time monitoring systems for data exfiltration further exacerbates the risk.

Impact:  A successful data breach could lead to the exposure of sensitive customer information, financial losses, and damage to the institution's reputation. Regulatory penalties are also a potential consequence due to non-compliance with data protection standards.

Recommendation: Implement strong encryption protocols for data at rest and in transit. Strengthen access controls by enforcing multi-factor authentication (MFA) and regularly reviewing permissions. Deploy real-time monitoring systems to detect and respond to data exfiltration attempts.

**2. Insider Threat:**

Issue: There is a lack of proper access control policies for privileged users, making it easier for insiders to misuse their access. Additionally, no system is in place to monitor unusual activities by employees, and there is no defined response plan for dealing with insider incidents.

Impact: Insider threats, whether malicious or accidental, can lead to data breaches, financial fraud, and other damaging outcomes. The lack of detection and response mechanisms makes it difficult to mitigate these risks effectively.

Recommendation: Implement stricter access controls, including role-based access management and regular audits of privileged accounts. Enhance employee monitoring systems to detect

unusual behavior. Develop a specific incident response plan for insider threats, including clear protocols for investigation and disciplinary actions.

***Recommendations Overview:***

1. Identify:
   - Conduct a comprehensive asset inventory and risk assessment for both external and internal threats.
   - Regularly update the assessment to reflect the current threat landscape.

2. Protect:
   - Implement advanced encryption methods and strengthen access controls.
   - Provide regular cybersecurity training focusing on both external threats and insider risks.

3. Detect:
   - Deploy continuous monitoring systems and improve anomaly detection.
   - Implement tools for monitoring employee activities, particularly those with privileged access.

4. Respond:
   - Develop and maintain a detailed incident response plan, covering both data breaches and insider threats.
   - Establish communication protocols for timely and transparent reporting of incidents.

5. Recover:
   - Create and test recovery plans for restoring systems and data after an incident.
   - Develop clear procedures for reassessing access after an insider threat incident.

6. Govern:
   - Align cybersecurity governance with the institution's business strategy.
   - Enhance third-party risk management practices and establish continuous improvement processes for insider threat management.