Date: [Insert Date]

To: Board of Directors and Executive Management

From: [Insert Supervisory Authority/Internal Audit Department]

Subject: SUPERVISORY LETTER: Ransomware Threat Mitigation and Cybersecurity Preparedness

Dear Management Team,

This letter serves to formally address the increasing prevalence of ransomware attacks and to outline mandatory expectations for the institution's cybersecurity posture and threat mitigation strategies.

The supervisory authority has identified specific areas where the institution must demonstrate robust controls to ensure operational resilience and the protection of sensitive data. Please review and address the following requirements:

- **Risk Assessment:** Conduct a comprehensive assessment of internal and external vulnerabilities specifically related to ransomware delivery vectors (e.g., phishing, RDP vulnerabilities).
- **Backup Management:** Ensure the implementation of immutable, encrypted, and offline backups. Regularly test restoration procedures to ensure data integrity.
- **Access Control:** Enforce the Principle of Least Privilege (PoLP) and mandate Multi-Factor Authentication (MFA) across all administrative and remote access points.
- **Incident Response:** Maintain a documented Ransomware Incident Response Plan. This plan must include specific communication protocols, legal notification requirements, and recovery priorities.
- **Employee Training:** Execute ongoing security awareness training focused on social engineering and threat reporting procedures.

The institution is required to submit a written response by [Insert Date] detailing the current status of these controls and a timeline for remediating any identified gaps.

Failure to adequately address these risks may result in further supervisory action or increased capital requirements due to operational risk exposure.

Sincerely,

[Insert Name]
[Insert Title]
[Insert Organization]