**Date:** [Insert Date]

**To:** [Name of Entity/Executive Management]
**From:** [Name of Supervisory Authority/Internal Audit]
**Subject:** Supervisory Letter regarding Incident Response Preparedness

Dear [Recipient Name],

This letter follows the recent review of [Organization Name]'s cybersecurity and operational resilience framework, specifically focusing on Incident Response (IR) preparedness.

The objective of this assessment was to evaluate the organization's ability to detect, respond to, and recover from security incidents that could impact the confidentiality, integrity, or availability of critical systems and data.

**Summary of Findings:**

- [Finding 1: e.g., Incident Response Plan requires updating to reflect current infrastructure.]
- [Finding 2: e.g., Evidence of regular tabletop exercises is insufficient.]
- [Finding 3: e.g., Communication protocols with external vendors need clarification.]

**Required Actions:**

1. **Update IR Plan:** Revise the existing Incident Response Plan to include [Specific Requirement] by [Date].
2. **Training and Testing:** Conduct a simulated cybersecurity exercise involving senior management and provide a post-action report by [Date].
3. **Reporting Protocols:** Enhance the internal escalation matrix to ensure timely notification of material incidents to the Board and regulatory bodies.

**Next Steps:**

Management is requested to provide a written response and a detailed remediation plan addressing the findings above by [Date]. Failure to address these gaps may result in further supervisory action or increased risk ratings.

We appreciate your cooperation in strengthening the organization's security posture.

Sincerely,

[Your Name/Signature]
[Title]
[Department/Organization]