C. Action Plan for Recommendations

The following action plan outlines the steps IBC Bank should take to implement the **short-term** and **long-term** recommendations from the report. Each recommendation is accompanied by a timeline and the responsible team.

1. Phishing Prevention and Employee Training

Action: Implement **advanced email filtering** and conduct **employee phishing awareness training**.

Timeline: Within **30 days**.

Responsible Team: IT Security and HR.

2. Network Segmentation

Action: Implement **network segmentation** to isolate critical systems from general workstations.

Timeline: Within **60 days**.

Responsible Team: Network Operations and IT Infrastructure.

3. Backup System Overhaul

Action: Deploy **immutable, off-site, and cloud-based backups** to ensure data integrity.

Timeline: Within **90 days**.

Responsible Team: IT Backup and Recovery, Cloud Infrastructure Team.

4. Incident Response Drills

Action: Conduct **regular incident response drills** to ensure preparedness for future attacks.

Timeline: Every **6 months**.

Responsible Team: IT Security, Crisis Management Team.

5. Advanced Threat Detection Deployment

Action: Deploy **Intrusion Detection and Prevention Systems (IDPS)** to monitor network traffic and detect anomalies.

Timeline: Within **120 days**.

Responsible Team: IT Security, SIEM Operations.

6. Governance Framework Implementation

Action: Establish a **cybersecurity governance team** to oversee security initiatives and compliance.

Timeline: Within **6 months**.

Responsible Team: Executive Leadership, IT Security, Compliance Office.

D. Incident Response Checklists

The following checklists are provided to guide the **incident response team** in future ransomware attacks or similar incidents:

Incident Identification Checklist

Review **email security logs** for phishing attempts.

Monitor **file encryption** activity across critical systems.

Analyze **network traffic** for unusual outbound connections.

Containment and Recovery Checklist

Isolate infected machines from the network immediately.

Disable compromised accounts and change administrator credentials.

Engage forensic experts to assist with recovery and data integrity assessments.

Restore systems from immutable backups where possible.