Cybersecurity Gap Analysis Report for Banks

1. Executive Summary

[Provide a summary of the key findings, identified gaps, and a high-level overview of recommendations.]

2. Scope and Objectives

- **Scope:** [List the systems, processes, departments, or branches covered.]
- **Objectives:** [Define the purpose and expected outcomes of the gap analysis.]

3. Methodology

[Briefly describe the approach, frameworks (e.g., NIST, ISO 27001), tools, and data sources used for the analysis.]

4. Current State Assessment

- [Summary of existing cybersecurity controls, tools, and processes in place]
- [Outline of organization structure regarding cybersecurity]

5. Gap Analysis

Control Area	Industry Standard	Current State	Gap	Risk Level
Access Control	Role-based access enforced	Partial	No periodic review	High
Incident Response	Documented and tested annually	Documented, not tested	Testing missing	Medium
Network Security	Segmented and monitored	Segmented only	Limited monitoring	Medium

6. Recommendations

- [Prioritized recommendations to address each identified gap]
- [Quick wins and long-term strategies]

7. Action Plan

Action Item	Responsible	Timeline	Status
Implement access reviews	IT Security Team	Q3 2024	Pending
Test incident response plan	CISO	Q4 2024	Pending

8. Conclusion

[Summarize key points, acknowledge limitations, and present final remarks.]

Appendix

- [Supporting documents, reference frameworks, additional data]