Business Continuity Cybersecurity Assessment

Sector: Financial Services

1. Executive Summary

This assessment provides a high-level overview of the organization's preparedness to maintain business operations and protect critical information assets during and after cybersecurity incidents.

2. Scope

- Core banking and payment systems
- Client data storage and access controls
- Remote and hybrid work infrastructure
- Third-party service providers

3. Risk Assessment

Threat	Likelihood	Impact	Current Controls
Ransomware Attack	Medium	High	Regular backups, endpoint protection
Data Breach	Medium	High	Access management, monitoring
Insider Threat	Low	Medium	Audit logs, least privilege
Third-Party Compromise	Low	High	Vendor risk assessment

4. Business Continuity Controls

- Documented and tested incident response and disaster recovery plans
- Multi-site data replication and failover
- Employee cybersecurity training and awareness
- Regular penetration testing and vulnerability management

5. Assessment Findings

1. Incident response plans are in place but not tested annually.
2. Critical data is backed up daily; backup testing occurs quarterly.
3. Limited vendor risk assessments for smaller third-parties.
4. Remote work security controls need strengthening.

6. Recommendations

- Conduct annual tests of business continuity and disaster recovery plans.
- Increase frequency of backup restoration testing.
- Expand risk assessments to cover all third-party vendors.
- Enhance security training for remote and hybrid employees.

7. Conclusion

The organization demonstrates solid foundational controls, but improvements are recommended to ensure future resilience against evolving cyber threats. Regular review and testing of plans are critical for continued

operational continuity.