# RISK AND CONTROL SELF-ASSESSMENT (RCSA) TEMPLATE FOR XX BANKING COMPANY

## INTRODUCTION

This document provides a detailed Risk and Control Self-Assessment (RCSA) template specifically tailored for XX Banking Company. The RCSA process is integral to our risk management framework, enabling us to proactively identify, assess, and mitigate risks in our banking operations.

## RISK IDENTIFICATION

1. **Risk Category**: Operational Risk
    - **Specific Risk**: Cybersecurity Threats
    - **Risk Description**: Risk of data breaches and cyber-attacks impacting customer data and banking operations.
2. **Risk Category**: Compliance Risk
    - **Specific Risk**: Regulatory Non-Compliance
    - **Risk Description**: Risk of failing to comply with evolving banking regulations leading to legal penalties and reputational damage.
3. **Risk Category**: Credit Risk
    - **Specific Risk**: Loan Defaults
    - **Risk Description**: Risk of borrowers failing to repay loans, impacting the bank's financial stability.

## RISK ASSESSMENT

1. **Likelihood of Occurrence**: High for cybersecurity threats, Medium for regulatory non-compliance, and Low for loan defaults.
2. **Severity of Impact**: Severe for all identified risks.
3. **Inherent Risk Rating**: High for cybersecurity threats and regulatory non-compliance, Medium for loan defaults.

## RISK CONTROL AND MITIGATION

1. **Control Measure**: Implementation of advanced cybersecurity measures, regular compliance audits, and stringent credit assessment procedures.
2. **Control Effectiveness**: Cybersecurity measures are highly effective, compliance audits are moderately effective, and credit assessments are effective.
3. **Residual Risk Rating**: Medium for cybersecurity threats and regulatory non-compliance, Low for loan defaults.
4. **Mitigation Strategies**: Enhance cybersecurity training, update compliance policies regularly, and refine credit risk assessment models.

## MONITORING AND REVIEW

1. **Responsible Party**: Chief Information Security Officer for cybersecurity, Compliance Officer for regulatory compliance, and Chief Credit Officer for credit risk.
2. **Monitoring Frequency**: Cybersecurity risks to be monitored daily, compliance risks quarterly, and credit risks annually.
3. **Review Date**: Set specific dates for the next review of each risk category.

## APPENDICES

- Detailed cybersecurity risk analysis report.
- Latest regulatory compliance requirements and audit results.
- Credit risk assessment model and historical loan repayment data.