# Project Risk Management Plan

|  |  |
| --- | --- |
| Project ID | 20210901 |
| Project Name | Switch of third-party vendor for SMS sending to customers |
| Document Version | V1.0 |
| Authors (Project Business Analysts) | Nakonechnyy Pavel |
| Project Sponsor | Digital Customer Experience |

# Introduction

The function of SMS sending to customers is a critical process that supports several Operational and Regulatory processes. For Continuity of Business and Legal&Compliance reasons it is necessary to ensure that the process will continue uninterrupted (within approved SLA of 4 hours to switch communications to a backup vendor).

Due to announced plans of existing SMS vendor XYZ to shut down its operations in market of the bank, it is necessary to perform a timely switch of SMS sending to a new vendor that will be selected by 10th of December by the recently formed committee.

Goal of this document is to highlight to the committee and future project team members the risks that have to be taken in account when implementing the project.

# Risk Identification

To identify all the risks rising from such a switch an extensive surveying of Legal, Compliance, Corporate Governance, Corporate Risks, Fraud, Information Security, Data and Analytics, and Digital Customer Experience departments has been done. In two workshop sessions ran by the Project Business Analyst and overseen by Project Sponsor repeated risks have been grouped.

*All the identified Risks are listed in the Unified Table (Table 1) together with results of further analysis.*

# Risk Assessment

Impact of identified risks has been evaluated in 4 workshop sessions where all participants have been asked to categorize risks as high, medium, or low in terms of their probability of occurrence and potential impact on the bank with additional field for description of specific impact. These results have been aggregated into a common table in a workshop ran by the Project Business Analyst and overseen by Project Sponsor.

The numeric probability of occurrence of risk events during development has been evaluated by the Local Technology team and confirmed by APAC&EMEA Technology Head.

*All the assessed Risks are listed in the Unified Table (Table 1) together with results of further analysis.*

# Risk Response Strategies

Potential Risk Response Strategies for every risk have been collected by surveying and later aggregated in a single approach during two workshops ran by the Project Business Analyst and overseen by Project Sponsor.

Four Risk Mitigation approaches used in the project have been agreed to be commonly named Risk Avoidance, Risk Reduction, Risk Sharing, and Risk Acceptance.

*Chosen strategies are listed in the Unified Table (Table 1) together with results of other analysis.*

# Unified Risk Management Table

Results of Risk Identification, Risk Assessment, Risk Response Strategies have been gathered in a Risk Register. Full version of the Risk Register including Risk Owners and teams responsible for Risk Monitoring is available in the project repository. A simplified overview is presented below:

*Table 1 – Overview of the Risk Register as of 24th of November*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Risk Event** | **Severity** | **Impact** | **Mitigation steps** |
| 1 | **Data Security**  Sensitive customer data is exposed. | Critical | Regulatory penalties | **Risk Reduction**   1. Conduct thorough due diligence on the new vendor's security measures. 2. Implement end-to-end encryption for data in transit. 3. Check vendor’s compliance with relevant regulations (e.g., GDPR, PCI DSS). 4. Execute annual Security Audits and penetration testing; |
| 2 | **Continuity of Business**  The switch causes interruptions in SMS services. | Critical | Regulatory penalties  Monetary loss | **Risk Avoidance**   1. The transition must be done on Friday night. 2. A rollback plan must be prepared in case of issues during deployment and service failure. 3. Backup SMS vendor must be available for use under 4 hours after identification of an issue. 4. Extensive testing must be done in a test environment prior to production deployment. |
| 3 | **Compliance and Regulatory Risks**  The new vendor does not fully comply with banking regulations. | Critical | Regulatory penalties  Monetary loss | **Risk Sharing**   1. Include compliance requirements in the vendor contract and ensure that the vendor has a proven track record of adhering to regulations. 2. Consider obtaining legal counsel to review the vendor's compliance measures and practices. |
| 4 | **Customer Trust and Reputation Risks**  There are issues with receiving important service and marketing communications during deployment. | High | Loss of trust  Reputation damage | **Risk Acceptance**   1. Acknowledge that some level of risk is inherent in the transition. 2. Customers will be informed prematurely about the works on the SMS delivery through a Push notification. Customer support will be available on the phone during whole period of deployment with increased capacity. |
| 5 | **Integration Challenges**  The new SMS system may not integrate seamlessly with existing banking systems, leading to operational inefficiencies. | High | Necessity of further developments and monetary loss | **Risk Reduction**   1. Local Tech is to conduct a comprehensive integration assessment and planning for potential issues to reduce the likelihood of integration challenges. |
| 6 | **Vendor Reliability**  New vendor may have service outages or performance issues. | High | Reputational damage | **Risk Sharing**   1. Bank is to establish performance metrics and SLAs to share the risk of vendor reliability, holding the vendor accountable for service quality. |
| 7 | **Cost Overruns**  Transitioning to a new vendor incurs unexpected expenses on SMS delivery | High | Monetary loss | **Risk Acceptance**   1. Creating a detailed budget and contingency plan, the bank acknowledges the possibility of cost overruns while preparing to manage them if they occur. |
| 8 | **Loss of Historical Data**  Important historical SMS data may be lost when previous vendor is which can affect regulatory and business reporting & analytics. | Critical | Regulatory penalties | **Risk Reduction**   1. Local Technology to execute a project of data migration for existing vendor data; |
| 9 | **Regulatory Reporting Issues**  Reporting features for compliance of the new vendor are having issues | Critical | Regulatory penalties | **Risk Sharing**   1. Bank is to incorporate compliance checks into the vendor selection process and agreement with the vendor to share the responsibility of meeting regulatory requirements between the bank and the vendor. |
| 10 | **Inadequate Support from Vendor**  The new vendor fails to provide sufficient technical support during and after the transition, causing downtime or unresolved issues. | High | Technical issues  Reputational damage | **Risk Sharing**   1. Bank is to incorporate support terms in the contract to ensure that the vendor is responsible for providing adequate support. |

# Monitoring and Review

To effectively manage risks during the transition, the following monitoring activities will be implemented:

1. Monthly Risk Assessments: The project team will conduct weekly risk assessments to evaluate the current risk landscape. These assessments will focus on identifying any emerging risks related to the new vendor selection process, technical integration, and operational readiness.

2. Status Updates from the Vendor Selection Committee: The recently formed committee responsible for selecting the new SMS vendor will provide regular status updates on their progress and any potential risks they identify during the selection process. This ensures that all stakeholders are aware of developments and can address concerns promptly.

The risk register will be updated by Project Manager to reflect any new risks identified during monitoring activities.

# Communication Plan

During the execution of the project, Project Manager will be presenting updates on the project weekly highlighting key accomplishments, and probable risk events.

If Project Manager identifies that any of the outlined risk events has happened, he must reach out to the Project Sponsor to initiate a meeting confirming the steps planned for Risk Mitigation and initiating these tasks.