Assignment 1: Overview and application

Robert Salter

Stockholm University

Risk Management (RIMA)

Love Ekenberg

HT 2021

1. Introduction

The assignment will outline the application of a risk management process implemented during the development and launch of a new mobile payment solution provided by a Nordic commercial bank.

The bank focuses on financing solutions within the motor industry for private, business and fleet customers whilst also offering credit card services, savings accounts and point of sale payment solutions for industry partners. Banking customers access the bank's products through their website, mobile app or a network of car dealerships throughout the country.

Part of the bank's strategy is to provide frictionless payment methods for private credit card customers. In conjunction with this strategy was the launch of a mobile contactless payment solution. The payment solution works within Apple Wallet, Samsung Pay or Google Pay, allowing customers to make payments with their mobile phones.

According to Deloitte's 2019 report on the rise of mobile wallets in the Nordics, the traditional payment methods are under pressure from new technology, changing consumer behaviour and new regulations. The European Union's Payment Services Directive (PSD2) has accelerated change within the payments sector allowing retailers, tech companies and new FinTechs to disrupt a significant part of the traditional payment industry. The launch of the new payment solution offered an opportunity whereby the company was investing in additional payment options for customers to increase credit account usage and benefit from the rise in mobile payments in Scandinavian countries.

2. Risk Management Framework

Risk management activities are central to all aspects of the bank's operations and are strictly regulated internally through risk and compliance departments and externally through regulators and auditors. The company implements a risk management framework from ISO 31000 at both the project and company levels.

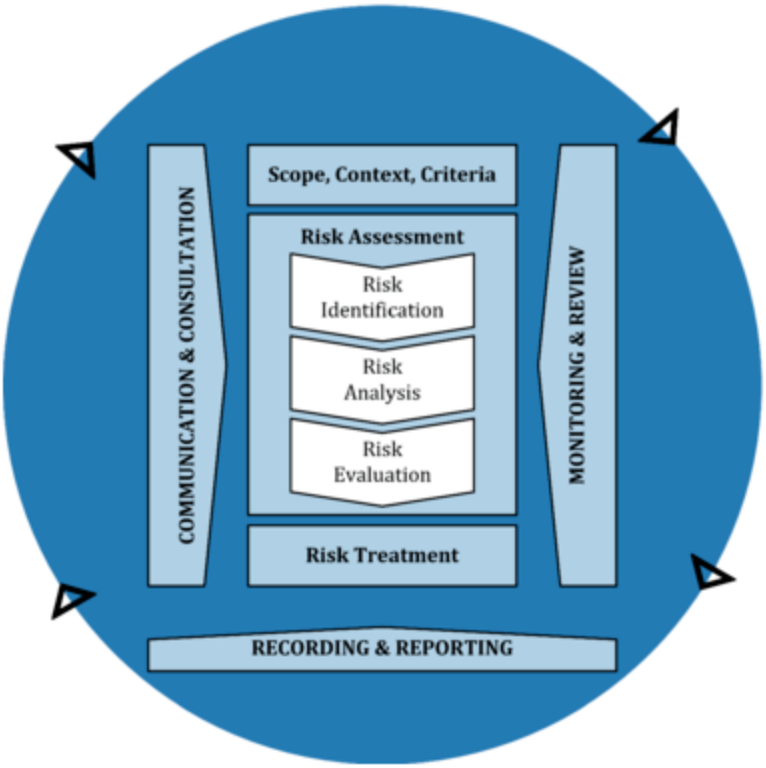

Figure 2.1: Risk management process from ISO 31000 (ISO, 2018)

3. Risk Management Context

3.1 External Context

The bank operates in a highly competitive market where there are many credit card products available to customers. The bank's strategy is to offer technological solutions to provide a competitive edge over competitors and guard against the risk of losing market share to new Fintech entrants.

The project's success is crucial to the bank's reputation and the customer's perception of their banking products. The introduction of a mobile payment solution aims to attract younger demographics to complement the bank's traditional customers who are between 40-65 years old.

3.2 Internal Context

The internal stakeholders include senior managers, project managers and IT specialists. The board of directors expects the project implementation to align with the bank's internal control requirements. These are consistent with COSOs definition, which states, "A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations."

(Hopkin, 2018, p.388)

The organisation also identifies an ability to identify, measure, monitor, and manage their risks in addition to this definition. The internal control requirements provide a foundation for the company's risk management process and are outlined in the internal company handbook. The handbook covers all business areas and states the policies and procedures to which the organisation adheres.

4. Risk Assessment

4.1 Identification

According to Hopkin (2018, p.141), the bank's risk classification areas can be broadly divided into:

- Market risk: concerning fluctuations in the financial markets (e.g. interest rates, foreign exchange rates).
- Credit risk: concerning the ability of customers to repay their loans
- Operational risk: relating to "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events."

The bank has specialist treasury and credit departments whose primary focus is the management of market and credit risk. The mobile payments project primarily affects the company's operational risk, and the risk management process will focus on this area.

Company-wide operational risks are identified annually by the risk and compliance department and compiled in a risk register. Risks are rated based on impact and likelihood on 1-10 scales and then combined to form an overall rating. The operational risks are also quantified, allowing the risk department to allocate capital to cover

operational risks consistent with Basel III requirements. Risks rated above the company's tolerance threshold are treated throughout the year by the risk department as departmental objectives. This benchmark for risk tolerance is otherwise referred to as the company's risk appetite.

In terms of the mobile payments project, the project management team was in charge of the identification, analysis and treatment/mitigation of operational risks. The team implemented risk workshops in collaboration with risk managers, which allowed them to highlight several risks documented in a project risk register.

Risk Index	**Risk Description**	**Current level of risk**			**Action to be taken**
		Likelihood	**Magnitude**	**Overall Rating**	
1	Data leakage through the sharing of sensitive customer data with external suppliers.	Low	High	Medium	● Implementation of the company handbook/framework regarding outsourcing of operations, in partnership with the legal department.

2	IT system failure/crashes during the product launch.	Medium	Medium	Medium	● Staggered launch schedule. ● Beta testing. ● Soft launch product with no marketing preceding the full launch.
3	Poor customer service knowledge of new products.	Low	Medium	Medium	● Implement workshops and training for customer service. ● Customer service included in beta testing.
4	Project delayed due to a lack of specialist IT knowledge.	Low	Low	Low	● Assessment of IT competencies ● Recruit specialist consultants
5	Project over budget.	Medium	Medium	Medium	● Scrum teams. ● Project management team oversees the budget.
6	Delayed approval of outsourcing by the Financial Regulator (FR).	Low	High	Medium	● Partner with the compliance department to expedite application to

					FR.
7	Risk of IT issue between banking app and Samsung/Google /Apple app.	High	High	High	● Members of the banking app team to work on the project. ● Increased testing before launch.

Table 4.1: Selected risks from the project risk register

4.2 Analysis And Evaluation

The identified risks involve departments throughout the bank including, legal, customer service, IT and compliance. These identified risks require analysis and evaluation by the relevant departments, which given the number of stakeholders, can be a challenging process to manage.

The bank, therefore, implements a documented New Product Approval Process (NPAP) which stated by the financial regulator, usually includes the following components:

- Checking that the product can be managed by all parts of the organisation;
- Documentation of the process or a procedural description for the new product;
- Checking that there are evaluation and risk measurement models for the product,
- All relevant managers should approve the product.

(FI, 2006, p.10).

The NPAP is the framework used to analyse and evaluate risk in new projects and products and applies to changes regarding existing products. The document provides a record for risk assessment and the approval of processes and procedures used in the

project implementation. It also allows department managers to provide insight into the challenges faced by the project with suitable solutions.

The project was analysed using the NPAP document to assess the impacts on all business areas, e.g. treasury, cyber security, money-laundering, external partners. Identified risks were included in the document, and workshops were arranged for department managers to address the operational risks concerning their department. Appropriate processes were developed and implemented with appropriate resources allocated. This approach developed a robust risk management culture whereby departments successfully implemented action points, taking ownership of risks affecting their operations.

5. Monitoring & Review

The project management team monitored the operational risks throughout the development and implementation stages, updating the project risk register as risk assessments changed and new risks were identified. Risks with a high overall rating were evaluated with risk managers with appropriate controls implemented. The process was ongoing and included in the project managers weekly updates to department managers.

The company has an internal ecosystem for reporting, documenting and addressing operational risks. The system allows any department to report operational risks, which are then analysed by the risk department and actioned by the relevant managers. The approach allowed issues relating to the project to be effectively managed on a case by case basis, and the implementation of risk controls arrested the development of risk severity.

On a longer-term basis, project risks were monitored through the reporting of an operational risk heatmap. The heatmap contained key risk indicators agreed upon by the board of directors with numerical ranges applied to the risk categories; acceptable, tolerated and unacceptable. The project's key risk indicators were: reported project-related IT issues, negative media attention, credit-card fraud, and customer uptake.

Operational Risk	Risk Scale			Month 1	Month 2	Month 3
	Acceptable	Tolerated	Unacceptable			
Project related IT issues	1	2-3	>4	2	0	0
Project related customer complaints	0-5	6-9	>10	2	3	1
Mobile payment fraud cases	0-1	2-3	> 4	0	0	0
Negative media attention			> 0	0	0	0

Table 5.1 Project Operational Risk Heatmap

6. Conclusion

The company has a long and successful track record with the implementation of technical projects and considerable resources dedicated to risk management as expected in a bank. The project risks identified were appropriately controlled and contributed to a successful project. A particular success was mitigation of risks concerning the product launch, whereby a staggered release schedule with appropriately timed marketing resulted in a low IT incidence rate and high customer uptake. The successful implementation of the project positively impacted several risks relating to the broader company risk register, in particular creating safer payment transactions through the implementation of digital credit card numbers and biometric identification, thereby positively impacting the company's operational risk regarding credit card fraud.

7. References

Deloitte., (2019). *Nordic Mobile Payment Report 2019 – Chasing Cashless* [online]. Deloitte [Viewed 1 September 2021]. Available from: https://info.deloitte.no/lg-finance-nordic-payment-report.html

Finansinspektion., (2006). *Firm's management of operational risk and FI's recommendations* [online]. Finansinspektion [viewed 1 september 2021]. Available from: https://www.fi.se/en/published/reports/reports/2006/firms-management-of-operational-risk-and-fis-recommendations-200618/

Hopkin, P. (2018). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*. 5th ed. New York: Kogan Page.

ISO., (2018). ISO 31000:2018(en) Risk management — Guidelines [online]. ISO [Viewed 1 September 2021]. Available from: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en