Financial Supply Chain Dynamics – Operational Risk Management and RFID Technologies

by

Harry Reddy

S.M. in Management of Technology, Massachusetts Institute of Technology, 2004
M.S. in Computer Science, Central University of Hyderabad, 1988
B.S. in Electronics, Osmania University, 1986

Submitted to the Engineering Systems Division in Partial Fulfillment of the

Requirements for the Degree of

Master of Engineering in Logistics

at the

Massachusetts Institute of Technology

May 2005

© 2005 Harry Reddy, All Rights Reserved

The author hereby grants to MIT permission to reproduce and distribute copies of this thesis document in whole or in part.

Signature of Author ..................................................

[(Signature)]

Engineering Systems Division
Master of Engineering in Logistics Program (MLOG)

Certified by .................................................................

Prof. Chris Caplice
Executive Director of MLOG Program
Thesis Supervisor

Accepted by .................................................................

Prof. Yossi Sheffi
Professor of Civil and Environmental Engineering
Professor of Engineering Systems

BARKER
Abstract

The banking industry is consolidating to streamline its operations through mergers and acquisitions, and is adopting new technologies to develop innovative products and services, thereby achieving both economies of scale and scope. Operational risk management has become a serious issue in the banking industry. Some reputed banks are either forced to close down their operations (e.g., Citibank Private Bank in Japan) or faced cost overruns (e.g., Barings Bank in England) due to poor operational risk management. In the supply chain industry, businesses are engaged in devising effective solutions using RFID technologies to locate and track the goods. We present the dynamics of banking industry in terms of operational risk management, innovation and business strategies. We also present the process mapping of RFID technology use in banking business areas to minimize operational risks. We further come-up with an effective operational risk management framework for banks to follow in improving their operational risk management.
Acknowledgements

In every phase of this study, many people supported me with many suggestions and words of encouragement. I would never be able to accomplish this task without these people.

First and foremost, I would like to specially thank my thesis advisor and mentor, Chris Caplice, for giving me the opportunity to work with him on such a wonderful and important research project. I would like to express my sincere gratitude to the Prof. Caplice for his helpful advice and comments throughout the course of the program at MIT. I’d also like to thank Prof. Yossi Sheffi for his advice during the program. I’d further extend my thanks to Prof. Arnoldo Hax for his valuable advice on strategy development.

I would like to thank Mr. Shinori Chibu for sharing with me his insights of Japanese banking industry and Citibank in particular. I would also like to thank Mr. John Reed for his insights on technology critical role in banking, which inspired me to use technology for creating a better value to customers. I’d like to thank Prof. John Carroll for his valuable advice on statistics.

I’d like to thank numerous people who helped me directly or indirectly either through the interview or through collecting the data and material, such as Tetsuya Yuge from Suruga Bank in Japan, Mr. Yasushi from MTB bank and Roy from Citigroup.

Last but not least, I’d like to thank my wife Yoshiko, and my daughter Emma, without them my days in Cambridge could never be so substantial and memorable.
# Table of Contents

Abstract 2  
Acknowledgements 3  
1. Introduction 5  
2. Motivation 12  
3. Financial Industry Dynamics 14  
   3.1 US Banking 14  
   3.2 Banking Innovation 19  
   3.3 Financial Supply Chain 24  
   3.4 RFID Technologies and Banking 37  
   3.5 Delta Model Strategy Framework 52  
4. Survey, Analysis and Results 57  
   4.1 Introduction 57  
   4.2 Data Gathering 57  
   4.3 Analysis and Results 59  
   4.4 Recommendations - OR Business Areas for RFID Technologies 77  
   4.5 Recommendations - ORM Framework 78  
5. Conclusion and Further Research 80  
References 81  
Appendix 84
Financial Supply Chain – Operational Risk Management and RFID Technologies

1. Introduction

The banking industry is facing increasing competition from several new fronts such as emerging technology companies like PayPal (a payments company acquired by eBay) and EBay (an e-commerce marketplace company with credit card transactions). These new technology based companies are successfully integrating their supply chains by offering financial services. The banking industry is also facing serious challenges emanating from operational risk management due to lack of effective mechanisms to control and track issues such as fraud, non compliance, system failure, physical asset damage, process management failure, business practice failure, and external business disruptions.

Due to lack of effective operational risk management, even reputed banks are either forced to close down their operations (e.g., Citibank Private Bank in Japan) or face cost overruns (e.g., Barings Bank in England). Recently, new technologies such as RFID (Radio Frequency Identification) are helping solve operational issues (e.g., product theft and product location identification) associated with supply chain management by better tracking and control of products. These technologies could offer potential help to minimize some operational risks in the financial industry as these risks are also related to better tracking and control of assets, processes, etc.
If we could develop effective process mapping solutions for the financial industry based on RFID technologies, it would provide both a platform for innovation and a mechanism to manage operational risks effectively.

The BIS (Bank of International Settlement) defines operational risk management in its Basle II accord as “the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events”. In other words, operational risk management consists of three stages: 1) cause of operational risk event, 2) type of operational risk event, and 3) loss of operational event occurrence. This can be depicted as shown below in Figure 1.

Source: Adapted from Basle description of operational risk management

Figure 1. Operational Risk Management Stages
As shown in Figure 1, the first stage of operational risk management is “causes of operational risk events” which is classified as internal processes, people, systems, and external event. These are defined below.

**Internal processes**

These are business processes that are adopted by a bank and failure of any of these processes could trigger an operational risk event to occur. The examples include customer credit profiling, loan application review, cash management, etc.

**People**

These are bank’s employees whose failure to follow policies and procedures of the bank could trigger an operational risk event to occur. Examples include fulltime employees, part-time employees and management.

**System**

These are banking systems and failure of any of these systems could trigger an operational risk event to occur. Examples include order taking system, credit scoring system, data exchange system, etc.

**External Event**

These are events that are external to a bank and they would force an operational risk event to occur. Examples include client bankruptcy, market drop, regulations, deregulations, etc.
As shown in Figure 1, the second stage of operational risk management is “type of operational risk event” which is classified as “internal fraud”, “external fraud”, “employment practices and work place safety”, “clients, products and business practices”, “damages to physical assets”, “business disruption and system failure”, and “execution, delivery and process management”. These are defined below.

*Internal fraud*

Internal fraud is an illegal act that causes financial harm to a bank and is conducted by an employee of the bank. Examples include intentional misreporting of positions, employee theft, and insider trading on an employee’s own account.

*External fraud*

External fraud is an illegal act that causes financial harm to a bank and is conducted by external party, not by an employee of the bank. Examples include robbery, forgery, check kiting, and damage from computer hacking.

*Employment practices and workplace safety*

These are certain practices and policies that have to be followed by a bank according to various safety and labor laws of state and federal governments. Examples include workers compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims, child labor regulations, and general liability.
Clients, products and business practices

These are unauthorized and illegal business conduct involving clients, products or business itself. Examples include fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank’s account, money laundering, and sale of unauthorized products.

Damage to physical assets

These are natural or intentional destructive acts that cause damages to physical assets of a bank resulting financial harm to the bank. Examples include terrorism, vandalism, earthquakes, fires and floods.

Business disruption and system failures

These are disruptions caused to banking business or banking infrastructure. Examples include hardware and software failures, telecommunication problems, and utility outages.

Execution, delivery and process management

These are areas of a bank in which failures or disputes could arise, causing financial harm to the bank. Examples include data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty nonperformance, and vendor disputes.

Each of these risk events could result in losses such as write-downs, loss of
recourse, restitution, legal liability, regulatory/compliance, or asset damage. These losses are depicted as stage third of operational risk management shown in Figure 1. A detailed analysis of operational risk management is presented in section 4.

In addition to enforcing controls, policies, procedures and regulations, we tend to think that there is a good opportunity for banks to significantly improve operational risk management in the following business areas.

- Cash Management
- Custodian and Promissory Notes Management
- Document and Workflow Management
- Customer Profiling (banks have to be sensitive for customer privacy concerns in this business area)
- Physical Assets Management
- Check Verification
- Payments
- Access Data Trail to Cash, Custodian, Promissory Notes and Documents

There are some benchmark frameworks or reports being developed by a well known banking industry consortium, BIS, and its benchmark report is called Basle II. However, we believe that the Basle II is not sufficient to mitigate operational risks as it doesn't provide a linkage with the business strategy of a bank. Business strategies differ
from one bank to another, thus we need to explore the relationship between operational risk management and business strategy. To do this, we conducted a survey of banks (regional, national and global) to find out business areas are affected by operational risks and to relate this to their underlying business strategy. After analyzing responses from the survey, we demonstrate how RFID technologies may be used in the banking business to minimize certain operational risks.

The remainder of the thesis is organized as follows. Chapter two explains the motivation to do current research. Chapter three describes the financial industry dynamics including an overview of banking industry, banking innovation, financial supply chain, RFID technologies in banking and Delta Strategy framework. Chapter four explains the survey, analysis, results and recommendations including list of business areas that could be used to implement RFID technologies and an effective operational risk management framework to minimize operational risks. Chapter five gives conclusions and further research that could be done.
2. Motivation

The motivation to do research on operational risk management in the banking industry comes from several factors.

First, operational risk management has significant financial impact. The annual exposure to operational risks in the banking industry is estimated to be $1.8 trillion in the settlement business alone (SIA 2003). The annual exposure to operational risks is $800 million due to poor cash management (Celent 2004). Banks including other organizations that are involved in financial business are penalized for having inadequate operational risk management (e.g., Orange County Crisis $1.6 billion, Baring Securities $750 million, Citibank Private Bank in Japan was forced to close down in October of 2004.

Second, there is a global recognition for importance of operation risk management. The introduction of regulations such as the Patriot Act and Sarbanes Oxley in general and BASEL II in particular as it is specifically applied to banking industry has raised the awareness of risk mitigation.

Third, RFID technologies are promising as they are already being adopted in supply chain industry by well known companies and organizations such as Wal-Mart, Gillette and US Department of Defense. In the banking industry too, RFID technologies are being
implemented. For example, Bank of Nagoya in Japan has started implementing RFID technologies in its document management. The bank’s spokesman said the savings due to RFID implementations would be in millions of dollars (NDG News Letter 2004).

Fourth, it is often crucial that we need to align new operational initiative of a bank with the bank’s business strategy. However, the banking industry consortium (BIS) offered a benchmark practice, Basle II, which is same for all banks, although business strategies are not necessarily same for all banks. Hence, we need to conduct a research to see whether or not aligning the operational risk management to business strategy is irrelevant and if customized best practice is a better solution for each bank.

In summary, operational risk management has huge financial impact, is being recognized as critical by governmental regulations, might be mitigated through the use of new technologies and should be aligned with a bank’s overall strategy. This thesis specifically looks to explore the latter two points.
3. Financial Industry Dynamics

3.1 Banking Industry Background

The banking industry in the US is consolidating due to intense competition and pressure to reduce bad debt. The US Federal Reserve Bank requires all banks to maintain a certain capital adequacy ratio (defined as existing assets divided by outstanding loans) by having a sufficient amount of assets in the bank. This regulation is spurring consolidation among banks in order to increase their asset value relative to outstanding loans and thus maintain the required capital adequacy ratio.

Although, one could think that the cash is needed all year round, financial transaction activities are actually cyclical in nature. Therefore, the banking profits follow a cyclical economic pattern (BCG 2003). The banking industry also experiences significant losses in different periods of time. For example, shareholders lost about $350 billion in market capitalization of the banking industry in 2001. Total returns for shareholders were minus 11 percent of investment on average during 1998-2002 as shown in the Figure 2.

For example, Germany and Switzerland were hit very hard. Among segments, asset management, investment banking, and transaction banking were the worst performers during 1998-2002 (BCG, 2003). It is the general perception in the industry
that banks in these nations are exposed to high operational risks, which are rare to occur but when it occurs the losses would be huge.

![Shareholder Returns Are Low but Above the Overall Market](image)

Source: (BCG 2003)

**Figure 2. US Banks Shareholder Returns**

The ten largest banks in the world raised their share in global market capitalization from 19 percent in 1998 to 24 percent in 2002, mainly through mergers and acquisitions. Today’s largest three banks (Citigroup, Bank of America, and HSBC Holdings) have increased their market capitalization on average by 25 percent per year since 1998, reaching a total market capitalization of more than $100 billion each (BCG 2003).

The bank’s average return on equity (ROE) after tax improved from 14.3 percent in 2001 to 16.5 percent in 2002. However, the cost of equity increased too, leaving the economic spread between ROE and the cost of equity unchanged since 2002. Only a few countries experienced a real profitability squeeze in 2002 (such as Germany with an average ROE below 1 percent for listed banks). Globally, 76 percent of equity capital earned profits above its cost of equity. Equity growth declined further from 7 percent in
2001 to 5 percent in 2002 (BCG 2003). When banks experience a profitability squeeze, they tend to loosen up their operational controls which can result in serious operational risks if not managed well.

The performance charts of the World ten largest bank holding companies (BHCs) and all other banks are shown below in Figure 3.

![Average Total Capital Ratios](chart)

*Source: Tower Group*

**Figure 3. Total Capital Ratios**

The above Figure 3 shows that the average capital ratio of larger banks is still lower than that of all other banks, which indicates that larger banks will most likely continue to pursue consolidation by acquiring other banks to increase their capital ratio (also known as capital adequacy ratio).
Shareholder value is measured by Return-On-Equity (ROE), as shown in the following Figure 4. The graph shows that the largest banks have much more variability in their performance than the smaller banks. This is counter intuitive since larger banks have larger asset bases and should withstand the cyclical nature of economic profits. However, it can be explained in terms of operational risk management. The larger banks are exposed to large operational risks due to the fact that a large asset base would be at risk if an operational risk event occurs.

![ Quarterly Return on Equity (Annualized, percent - 1997Q1 - 2003Q4) ]

Source: Tower Group

**Figure 4. Quarterly ROE**

To identify the drivers behind such operational risks we have to closely look into operational risk management and its associated business strategies.

In many cases, large banks and other institutions involved in financial
transactions are failing to manage their operational risks and are losing huge amounts of money. For example, Orange County Crisis lost $1.6B, Baring Securities lost $750M, and Citigroup had to close Citibank Private Japan operations in late 2004 for failure to meet the regulation. In each case, operational risk managements were not identified, managed, or mitigated properly.

In the next section, we explore the way innovation happens in the banking industry and if it needs any special consideration to manage operational risks effectively.
3.2 Banking Innovation

In this section we examine the effect of innovation on operational risk management. In order to consider a general overview of how innovation activities are performed in banking, we focus on three aspects of innovation performance: (1) generating new ideas and screening them, (2) understanding customers’ needs, and (3) conducting trials and experimentation to determine the utility and effectiveness of potential new innovations.

The first step in innovation activities in banking, or any industry, is to generate new ideas and make use of new technologies. After starting with a broad range of possibilities, the list should be gradually refined. Wheelwright and Clark (1992) describe the use of a “Development Funnel”; a graphical structure for thinking about the generation and screening of alternative development options. It also aids in combining some subset of these into a product concept. A variety of different product and process ideas enter the funnel for investigation, but only a small fraction become part of a full-fledged development project. Those are examined carefully before entering the narrow neck of the funnel, where significant resources are expended to transform the selected ideas into a commercial product and process.

The nature of the funnel is defined by the way an organization identifies, screens, reviews, and converges on the content of a development project as it moves from idea to reality. The funnel establishes the overall framework for development: the generation
and review of alternatives, the sequence of critical decisions, and the nature of decision making.

According to Wheelwright and Clark (1992), managing the development funnel involves three different tasks or challenges. The first is to widen the funnel's mouth. To be effective, the organization must expand its knowledge base and access to information in order to increase the number of new product and new process ideas.

The second challenge is to narrow the funnel's neck. After generating a variety of alternative concepts and ideas, management must screen them and focus resources on only the most attractive opportunities. Wheelwright and Clark (1992) note that the narrowing process must be based on a set of screening criteria that fit the company's technological opportunities while making effective use of its development resources in meeting strategic and financial needs. The goal is not just to apply limited resources to selected projects with the highest expected payoffs, but to create a portfolio of projects that will meet the business objectives of the firm while enhancing the firm's strategic ability to carry out future projects.

The third challenge is to ensure that the selected projects deliver on the objectives that were anticipated when the project was originally approved.

As Wheelwright and Clark depict in the development funnel, it is crucial to inject great ideas into innovative projects and to carefully screen them for creating
innovative products. However, these innovations in banking are no different from any IT-intensive organization where software products and projects are often innovated in a similar way.

The second aspect of innovation is to pay attention to customer needs. Most research emphasizes the importance of the role of the customer in the development process for generating innovative or breakthrough new products. Von Hippel (1988) indicates that involving customers in the early stages of the product development process could contribute to the development of products which meet customer needs. This is, however, a ‘lead user innovation’. Moreover, he noted that only ‘lead user innovation’ forms the basis for new products and services to any manufacturer. At this point, he defined ‘lead users’ as users who have needs that foreshadow general demand in the marketplace and expect to obtain high benefit from a solution to their needs, separating from ‘target customers’ used by the marketing method. In other words, all lead users are target customers but not vice versa because target customers are the ones who enjoy the use of products, whereas lead users are the ones who not only enjoy the use of products but also involve themselves in creating such products. Thomke and Von Hippel (2002), illustrated the ‘Customers as Innovators’ (CAI) method which means shifting parts of the development process to customers, and also showed that ‘toolkit’ translating manufacturer’s language (solution information) into customer’s one (needs information) is crucial for innovation.

The third aspect of innovation is to conduct trials to determine the utility and
effectiveness of potential new innovations. Thomke (2001) points out that a major
development project can require literally thousands of experiments, all with the same
objective—to learn whether the product concept or proposed technical solution holds
promise for addressing a need or problem, then incorporating that information into the
next round of tests so the best product ultimately results. He also noted that in the past the
testing process was relatively expensive, so firms were frugal about the number of
experimental iterations. Today, however, new technologies such as computer simulation
and rapid prototyping enable companies to create learning more rapidly, and that
knowledge can be incorporated in more experiments at less expense. Moreover, new
technologies affect everything, from the development process itself (including the
innovative organization), to how new knowledge (learning) is created. Thus, Thomke
suggests, for companies to be more innovative, they must overcome both managerial as
well as technical challenges.

Many of these innovation methods seem applicable to the service world such as
banking industry. The challenge in applying those successful innovation methods to
services might be accompanied with some difficulty in contrast with manufactured goods.
The most different point from manufactured goods is that a service is intangible. For
sake of clarity, we use service to refer to both product and service offered by bank.
Since some services exist only in the moment of its delivery to a customer, and are
tailored to individual buyers at the point of purchase, it is difficult to isolate them in a
‘laboratory’ and perform ‘trial-and-error’ process enough to examine if they really meet
with customer needs or not – primarily due to the complexity involved with millions of
individual customers and hundreds of transactions each by many business customers. However, we could segment the customers to perform the experimentation.

For more than 60 years, in many countries, governments have been prohibiting financial institutions from entering new business fields to maintain their country’s financial condition stability (ABA 2002). This prohibition drove financial institutions to adopt business structuring practices such as subsidiaries in banking, security, and insurance. As a result, those regulations have made the financial industry anticompetitive due to loss of scale and discouraged it to create innovative services at a centralized location.

In summary, the innovation in banking industry is no different from product based industry or service based industry. In banking industry, generating new ideas, understanding customer needs and conducting experimentation are important and so do they in other innovation based (product or service) industry where in operational risk management is minimal. Therefore, we argue that the banking innovation has no effect on the operational risk management.

In the next section, we present the intricacies of financial supply chain, effect of deregulation, historical forecast and actual of operational risks, and best practices of operational risk management.
3.3 Financial Supply Chain

Deregulation in the banking industry spurred technology-based centralized innovations such as online payments and contact-less payments. These innovations in financial institutions created opportunities for designing effective financial supply chains to meet the increasing customer demand in scale and scope of automated products and services. For example, previously, every time a foreign company issued a purchase order to one of its suppliers in China, it had to open a letter of credit with its bank, a process that required presenting a stack of documents. The bank would then courier the letter of credit to the manufacturer's bank, a journey that could often take a week. The Chinese bank would then review the documents and inform the factory it could receive payment as soon as it shipped the order. The entire transaction could take as much as two weeks, during which time the company's money had left its accounts but had not yet paid for the goods (Kahn and Gabriel 2004)

Kahn and Gabriel (2004) raise the following important points with regards to the financial supply chain.

1. In a world of just-in-time inventories, common systems for paying suppliers remain slow and complex.

2. Cost of processing trade documentation is more than 5% of the total annual value of world trade.

3. Cost of processing a simple international business transaction is about $400.

4. Up to 24 forms must be completed for each transaction for a case study involving purchase order and letter of credit.

5. Half of all letter-of-credit transactions are rejected or asked for revised
ones by banks because of incorrect information from the buyer or seller.

All the above points are referred to as payment problems, document problems, automation problems, or incorrect information problems, which all could be fixed by RFID enabled solutions. We will explain each of these in the next section.

According to Procter (2003), JP Morgan is aiming to enhance the value from supply chain financing, and is launching an Internet-based payables discounting service for corporate clients. The solution brings increased efficiency through the benefits of extended Days Payable Outstanding for its corporate clients, and reduced Days Sales Outstanding (DSO) for their suppliers. The result is increased predictability of cash flow. JP Morgan clients will transmit approved invoices via a newly developed web-based Internet platform. The supplier can receive early payment from JP Morgan, while the client repays JP Morgan on maturity. By leveraging the Internet for supplier connectivity, buyers and suppliers gain a valuable tool for managing cash and information flow along the entire financial value chain.

Bruce Proctor, head of global trade services for JP Morgan in New York says "Our customers' growing requirement to move away from letters of credit and other traditional trade methods is stimulating new opportunities for the automation of receivables and payables management". He continues: "As one of the few banks currently operating in the open account market, JP Morgan is able to meet this demand and offer the right technology for integrated trade and cash management solutions that
enable clients to more effectively manage their balance sheets." This automation related and cash management related problems could be fixed by an RFID enabled solution.

Stetter (2003) discusses the recent regulations in the financial industry. A number of recent events have accelerated the transformation of bank’ Treasury department, forcing banks to change their corporate strategies and reorder priorities. This is having a profound effect on corporate Treasury personnel and causing a significant increase in the scope of their responsibilities. Probably the most significant development stems from Sarbanes-Oxley (created after several accounting scandals surfaced in public corporations in the US) and the USA Patriot Act (created after September 11, 2001 terrorist activities occurred in the US). Market conditions are forcing companies to take a much more aggressive approach to self-financing by minimizing the cash required for working capital. Treasury personnel are being asked to do more with less. Yet, the number of developments that they must deal with and understand has grown significantly. Treasury departments are making working capital management an integral part of their strategy and responsibilities. The traditional role of Treasury focused on cash forecasting, and balance and liquidity management. In its new role, Treasury must embrace the full cash conversion cycle. These regulations are another dimension of driving the need for designing effective financial supply chain with adequate operational risk management.

The regulations also include paper to electronic payments (Stetter 2003). Until recently, companies could afford and see what payment trends would eventually gain widespread acceptance and then adopt them. The delayed adoption is not an option.
anymore due to recent payment legislations. Companies are now forced to make conscious decisions as to what is the effective way to deal with the new legislation (Check 21), new industry practices (check conversion and/or truncation), new and more sophisticated forms of fraud, and technology (systems integration and imaging).

According to Killen & Associates (2004), market analysts predicted that the cash management market will be $80 billion for the year end of 2004. Financial institutions that are currently offering services via the Internet will be in the best position to lead this market because of the huge number of customers available via the web, the researchers noted. This rush to the Internet will leave their less-prepared competitors behind and will enable Internet-savvy institutions to pick up an additional 40-50 million small and medium-sized commercial customers worldwide.

According to Killen & Associates (2004), the technology will become a vital application and will change the economics of banking product delivery. The technology will provide real-time information that will enable companies to make decisions on where and how much money to invest, what to pay, and where to transfer funds.

The American Bankers Association (2002) says new cash management systems equipped with technologies will keep banks competitive in the industry. Several powerful personal computer-based cash management systems have entered the market
recently. First National Bank of Waconia has offered cash management services to its corporate customers since 1984. In 1992, the bank installed Business Express/PC, a PC-based cash management system from Automatic Data Processing (ADP) Network Services Division. The latest release of the software, Version 2.1, offers small business users direct deposit of payroll and automated account reconciliation. About 20 First National clients are now connected to the system. Several of the earliest users are looking for the ability to make electronic vendor payments with Business Express/PC. Columbus Bank & Trust Co. uses Banc-COM, an online cash management system from Southern Business Technologies. In mid-January 1993, nineteen corporate accounts were linked to the Banc-COM system, including the American Family Life Assurance Corp. and municipal accounts.

According to Swann (2004), cash management is becoming more common among community banks as well. These banks have closer relationships with buyers and suppliers of small scale supply chain industries.

If banking operations such as cash management can be improved with the use of new technologies, we now present the urgency of implementation of such services considering the issue of operational risk management as presented below.

According to McKinsey Report (2004), there is little correlation between the actual failure of banks with either forecast or naïve methods such as historical figures. The graph of these figures is depicted in the following Figure 5.
Figure 5. Bank Failure Rates – Actual Vs. Forecast

The above graph, Figure 5, is plotted with year on x-axis and failure rate as percentage of banks that fail on y-axis. The graph contains three lines: first one is for banks’ failure forecast, second one is for naïve method of 2-year historical failure rate as forecast, and third one is for actual failure rate. When we compare banks’ actual failure rate with the failure forecast, there is a huge difference, except in mid 1999 and late 2000. This forecast is gathered from banks every quarter by Financial Risk Committee of US Federal Reserve Board. However, when we compare the banks’ actual failure rate with the naïve method of two immediate preceding years’ figures as a forecast, the difference
still exists but is smaller than the earlier one. The reason for such difference might be due to poor operational risk management that this thesis focuses on.

In light of recent failures of several banks, the international body, Banking International Settlement (BIS), has come-up with the Basle II accord. A voluntary accord, Basle II, was created to improve bank's operational risk management.

According to the Basle II Report (2003) the risks are described as a catch-all name for a set of very different risk types, including those the related to staff, processes, systems, and acts of God, that are inherent to the practice of doing business. These risks can range from such extreme events as the 2001 New York World Trade Center bombing to simple execution failures, such as a missed deadline that resulted in revenue loss.

The Basle II Accord, as shown in the following Figure 6, describes three pillars to be followed in order to protect a bank from failing due to operational risk management. These are Minimum Capital Requirements, Supervisory Process, and Market Discipline.

The first pillar, Minimum Capital Requirements, mandates banks to maintain a certain deposit to loan ratio and links credit risk to credit ratings. The second pillar, Supervisory Process Review, mandates banks to do risk assessment and review capital adequacy ratio (i.e., assets-to-loan ratio). The third pillar, Market Discipline, mandates banks to disclose capital adequacy information, risk profiles and capital structure information.
New Basle Capital Accord

**Figure 6. Basle Capital Accord**

BIS issued notification to banks around the world to follow these guidelines and implement them fully by January 2007. Although, there is no mandatory requirement for a bank to follow these guidelines, it is expected that most banks would implement these guidelines by 2007 to satisfy the respective country’s central banks in terms of following the best practices.

Before getting into details of risk types and risk priorities, we first explain the distribution and severity of losses. According to Crouhy, Galai and Mark (2001), the distribution of losses within banks is characterized as shown in the following Figure 7. The graph illustrates likely hood of loss on x-axis and severity of loss on y-axis. The severity of loss is categorized into three segments – 1) business plan and reserves, 2)
operational risk capital, 3) insurable risk. The banking business plan risk has a high probability of occurring but small loss potential, and these risks can be mitigated by following proper credit and market screening procedures. On the other hand, the transferable risk such as insurance has a small probability of occurrence but has potential for high loss, and this risk can be hedged since it is transferable. Whereas, the middle risk has medium-to-small probability of facing risk but the effect on loss is medium-to-high, which is depicted in the middle of the curve as shown in the following Figure 7.


Figure 7. Loss vs. Severity
These operational risks cannot be eliminated either by adopting risk screening procedures or by hedging the risk. This thesis focuses on these operational risks shown in the middle of the curve, where the probability of loss occurrence is medium-or-low but has potential for high losses.

Deloitte and Tomatsu (2003) describes bank’s risk management priorities as varying from low to high as shown in the following Figure 8. The risks are depicted on y-axis and the percentage of banks is on x-axis.

For example, the operational risk measurement system is high priority for about 25% of banks, is moderate priority for about 45% of banks, and is already implemented by about 5% of banks only. Whereas, advanced market risk systems are already
implemented by about 25% of banks and advanced credit risk systems are already implemented by about 20% of banks. This clearly shows that banks are upgrading their priorities in operational risk management.

According to Celent (2004), the operational risks are encompassing all areas of the banking business. The most notable fact is that banks have further work to do in all nine operational risks, as shown below in Figure 9. However, banks have done better so far in market risk and credit risk. This shows the urgency of a need to address operational risk management within banks.

Source: Celent Communication

Figure 9. Risk Types vs. Work To Be Done
The financial supply chains (Celent 2003) are depicted as shown below in Figure 10.

![Figure 10. Financial Supply Chains](image)

The dark-shaded blocks in Figure 10 are newly focused areas and the light-shaded blocks are traditionally focused areas. By merging these two focus areas, the banks have to devise the resilient operational risk management framework in the context of increasing complexity of financial operations both in scale and scope. The scale (i.e., wide reach into customer base) and scope (i.e., wide rich of offerings to customers) of financial operations are increasing because of handling ability of automation using technologies such as electronic settlement of payments. Lack of effective operational controls such as document management can result in operational risks. The cash management, electronic payments and document management can be RFID-enabled to tag the audit trail and locate the cash or document whenever necessary.

In summary, deregulation in the banking industry spurred the innovation with centralized funding to offer distributed products and services at point of locations, which while offering great services to customers are creating problems from the standpoint of
operational control. Further, financial operations such as check processing and cash management have tremendous scope to improve using automation technologies. These improvements are needed because of lack of accurate forecast of bank’s failure rate and because of the fact that the severity of loss is high when an operational risk is occurred.

To address the problem associated with poor operational risk management, Banking International Settlement (BIS) has offered a best practice framework for any bank to follow. We view that this best practice framework is only first order solution for a bank to mitigate or minimize operational risks. The second order solution would be utilizing RFID technologies to automate certain processes and to have a better audit trail. The third order solution would be to customize the best practice to meet the particular business strategy of a bank. The background of second order and third solutions are explained in the following sections, and the actual analysis of these solutions is offered in the following chapter.

In the following section, we examine the current prototypes and potential future use of RFID technologies in various products and services of banking. RFID technologies can help mitigate operational risks. In essence, RFID eliminates the problems associated with locating an asset, tracking access data, automating the process and auditing the access trail.
3.4 RFID Technologies and Banking

We first give an overview of RFID technologies before getting into specifics of banking applications. Radio Frequency Identification (RFID) is a technology that refers to the use of radio waves to transmit data for identification purposes. Among the many uses of this RFID technology are identification and tracking of livestock, library books, airline baggage, remote locks, and contact-less payment systems (Sullivan and Happek 2004). All these applications benefit from RFID’s ability to track and identify unique physical entities remotely. Recently, more attention has been placed on the applications of RFID in Supply Chain Management. RFID offers many improvements over existing barcode technology including the automatic data capture without a physical scan, omni-directional data capture (line of sight scanning is not required), and increased data capabilities.

An RFID system, as shown in the following Figure 11, consists of the following four components. The definitions below detail each component of an RFID system and how they interact to make the RFID system work.

- **RFID Reader**: Device used to query/read and possibly write data to RFID tags – also known as a RFID transceiver or interrogator.
- **RFID Tag**: A device responsible for the transmission of data to RFID readers containing an antenna consisting of a microchip and a transponder. The tag stores a code that unique identifies this RFID tag known as an Electronic

- **Communication:** A predefined common radio frequency and protocol used by both reader and tag for data transmissions (Chiesa et al 2002).

- **Savants:** Local data repositories that contain EPCs and associated data. They are essentially middleware that connects RFID collection devices with enterprise applications (Sullivan and Happek 2004).

![Figure 11. RFID System Diagram](image)

*Source: WebMethods, 2004*

There are two general types of RFID tags - active tags and passive tags - which could be used depending on type of application. However, inventory related applications need just passive RFID tags.

Active Tags are self-powered by a built-in battery which also powers an
embedded radio transceiver. Active tags have a larger read range of about 300 feet due to the powered transceiver but also have a higher cost due to the batteries, which periodically need replacement.

Passive Tags usually do not have batteries and operate by receiving an incoming interrogation signal, modulating it to add identification data and finally reflecting the signal back to the reader. Passive tags have a much smaller read range than Active tags. However, one important benefit of Passive tags without batteries is their significantly lower costs (Chiesa et al 2002).

RFID tags not only vary in their read range but also in their ability to have stored data rewritten as well but for normal applications such in Supply Chain Management and banking we don’t need the ability to rewrite the data.

RFID technology has been around since World War II, but its commercial applications have not been considered until recently. Applications for RFID in supply chain management have been limited in the past by the costs of the tags. Niemeyer, Pak and Ramaswamy (2003) shows, as in the following Figure 12, the decreasing costs of tags from around 1 dollar per tag in 2000 to a projected cost of around 5 cents per tag in the next few years. The cost of the reader technology is reducing as well. However, the cost of 10 or 15 cents for protecting a valuable document in banking industry may not be as serious issue as in supply chain industry.
With the costs of RFID reducing, the return-on-investment and potential of the technology are increasing. Therefore, an increasing number of companies are developing initiatives to enable RFID in their supply chains. Wal-Mart and the Department of Defense (DOD) mandated that their top suppliers should tag all supplies with RFID tags by 2006. In addition, Target and Tesco have already informed their suppliers that they will be issuing mandates on RFID compliance soon as well. The calls for RFID compliance by the world’s largest retailer and military has not only boosted the credibility of RFID technology but has also put it in the spotlight as suppliers scramble to find the requirements, (Sullivan & Happek, 2004).
RFID technologies are creating new opportunities for the banking industry to effectively manage their operational risks and increase their efficiency. The banking industry has been successfully utilizing the information, computers and telecommunications for creating an automation using digitization (e.g., scanning the document). However, the digitization of certain assets such as custodian promissory notes comes with operational risk management issues because of customer privacy and security concerns. Up until now, the dilemma is how to automate certain assets or processes without digitization. Now, the solution to this dilemma is to utilize RFID technologies that make automation possible without actually digitizing the underlying asset. The RFID solution provides tracking mechanism to physical assets and the data generated from tracking can be stored for future review.

Operational risk management in the banking industry can be effectively addressed in the following areas.

- Cash Management
- Custodian and Promissory Notes Management
- Document and Workflow Management
- Customer Profiling
- Physical Assets Management
- Check Verification
- Payments
- Access Data Trail of assets and processes.

These areas are studied in detail in the following sections.
Cash Management

As illustrated in the following Figure 13, the cash settlement transactions continue throughout the whole day.

Further, there are ATM and counter transactions that need to be considered when

Source: Adapted from Suruga Bank

Figure 13. Typical Cash Management Cycle in Bank
managing the right amount of cash. Too much excess cash in inventory leads to losing the opportunity cost of interest for the bank while insufficient cash in inventory leads to losing a customer. In other words, cash is inventory for banks, just like products for a company. The cash in a bank is physically stored in a special room and bankers are typically hesitant to take charge of managing the physical cash as there is a lot at stake for errors, and an error by an employee may easily be considered as an intentional theft thus leading to mistrust among employees.

Moreover, it is not productive to spend hours simply counting the cash over and over again each time the cash is used. We suggest that banks use RFID for each bundle of cash so that a banker should count only if the bundle is tampered with and moreover the access to this bundle is logged for each event. Further, there is no privacy concern here since the associated RFID tag will automatically be deleted when the bundle is opened or when it is handed in to a customer. This mechanism of RFID enabled cash bundles would help mitigate operational risks in terms of cash management and access data trail to physical cash. Celent (2003) says the annual estimate of cash management loss as $800 million.

*Custodian and Promissory Notes Management*

These are safe-keep items that are sensitive business or customer material. Banks store in safe places custodian material such share certificates, gold, promissory notes and bond notes. Since the access to these highly valuable custodian materials is
handled physically by people, it is prone for mishandling thus leading to exposure to operational risks. We suggest that banks use RFID enabled tags for such custodian files and metals including promissory notes so that these valuable items are not only protected but also logged the access data to such items. The logged access data can be analyzed periodically to find out a particular abnormal pattern of usage by an employee, and knowing these abnormal patterns proactively can alert the management to control the activities of the employee before the bank is actually exposed to the associated operational risk. That way, operational risks can be effectively managed with RFID enabled tags. IDG (2004) says the annual estimate of loss of custodian securities management as $2.3 billion dollars.

Document & Workflow Management

Document and work flow management is one of the most tedious things in a banking environment. Currently, though, banks have no effective way of storing, locating and accessing documents as frequently as needed without digitizing them. Digitizing may pose problems for certain documents due to customer confidentiality and privacy issues. We suggest that banks incorporate RFID in such documents to effectively manage the document handling and access tracking. IDG (2004) says the annual estimated savings of RFID enabled document management for Bank of Nagoya, a small local bank in Japan, runs into millions of dollars. IDG (2004) notes that this RFID based document management implementation is first of its kind in Japan and many other banks started showing significant interest in this initiative.
Physical Assets Management

Physical assets such as computers, servers, telecom equipment and customer data storage tapes can be RFID tagged to help locate and possibly avoid theft. These physical assets are just like inventory items in a supply chain company.

Because of the fact that supply chain companies like Wal-Mart, Gillette and P&G started implemented RFID initiatives, the banking industry that spends about 20% of their expenses on IT (Information Technology) can easily implement these technologies to minimize operational risks arising out of missing and stealing of assets. Furthermore, banks can potentially reduce insurance premium for putting in place such operational risk management.

Check Processing and Auto-payments

The banks have started providing the contact-less check payment system by embedding the RFID chip in a check. This payment system not only helps automate the process but also minimize the counterfeiting. The attempted check counterfeiting at US banks was $5.5 billion in 2003 (WCB Journal 2004). This serious check fraud can be reduced by using RFID technologies.

For example, check fraud could be minimized by re-designing the check with built-in RFID chips as shown in the following Figure 14 (Celent 2004).
The cost of few cents per check is not an issue considering the fact that a potential check fraud involves thousands of dollars. The RFID-integrated checks could be used at the point of sale system as well (Celent 2003).

The auto-payments involving with cards can be implemented utilizing RFID technologies at point of sale system as shown in the following Figure 15. This system contains tag equipped card, reader and host computer. The host computer collects the data each time card is passed through without having a need to physically swipe through and this data could be utilized for analyzing to reduce operational risks such as fraud while improving the customer service.
American Express has already started developing the RFID-integrated express payment system, (Amex 2004) as shown below in Figure 16. These technologies are already installed in places such eZpass (Road Tools), Octopus card (Hong Kong subway system), and gas stations.

These RFID enabled small and easy payment systems help a bank offer service to millions of people without exposing the bank’s operational risk. In addition, banks can use this system as internal credit or marketing tool to analyze the customer risk and behavior.
Similarly, the Bank of America (BOA 2004) also started developing quick-wave transaction system using RFID-integrated payments mechanism, as shown in Figure 17.

Source: American Express

Figure 16. RFID Credit Card Payment

Figure 17. RFID Credit Card Payment - BOA
These RFID-enabled payment systems can avoid the current fraud. ABA (2002) reports the breakdown of loss by fraud type as shown in the following Figure 18. The major loss of 24% is reportedly coming from signature forgery which could be eliminated by implementing RFID technologies. The other major loss of 24% is due to NSF (Non-Sufficient Funds) which could be reduced by implementing RFID technologies because there is no much manual work involved in processing NSF checks.

<table>
<thead>
<tr>
<th>Type of Fraud</th>
<th>% of Cases</th>
<th>US$ Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forged Makers' Signatures</td>
<td>24%</td>
<td>24%</td>
</tr>
<tr>
<td>NSFs</td>
<td>24%</td>
<td>19%</td>
</tr>
<tr>
<td>Closed Accounts</td>
<td>10%</td>
<td>9%</td>
</tr>
<tr>
<td>Counterfeit Checks</td>
<td>9%</td>
<td>12%</td>
</tr>
<tr>
<td>Forged Endorsements</td>
<td>6%</td>
<td>10%</td>
</tr>
<tr>
<td>Reclamation</td>
<td>4%</td>
<td>3%</td>
</tr>
<tr>
<td>Kiting</td>
<td>2%</td>
<td>4%</td>
</tr>
<tr>
<td>Alterations</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td>20%</td>
<td>17%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Figure 18. Payment Fraud and Losses**

These check frauds can be eliminated or reduced by implementing RFID enabled check system and introducing RFID based auto payment system, thus these technology based solutions can help a bank to minimize its operational risk.

A treasury’s risk survey of over 500 CFOs and treasurers (TR 2003) found that threats posed by the mismanagement of cash position and opportunities of proper cash management systems are significant. The statistics of this survey show that one in every four companies expected to have a consolidated cash management and almost half of
companies said they were approached by banks to consider their cash management solutions. Almost four out five (79%) customers said they would get better service with enhanced cash managed system, and almost half of customers (48%) said they would offer a bank with more business if the bank provides a better cash management solution that is integrated to company's business applications.

Their data suggest that there is tremendous need to come-up with a better solution for managing the cash. Treasury and Risk magazine has gathered responses through survey from CFOs and Treasurers representing corporate customers of banks. The survey asked primarily what kind of threats they have in terms of cash management service and what are the opportunities exist for proper cash management systems. As 79% of customers feel that they are not happy with cash management service provided by their banks and 44% of customers are ready to give more business to a bank that can offer better cash management service, banks have tremendous opportunity to improve their cash management solutions.

*Access Data Trail to Documents, Custodian Assets and Physical Assets*

Most importantly, the RFID enablements will create an opportunity to log the access trail to each and every asset and document, and analyzing this access data trail can become a valuable tool to find out the abnormal patterns of use. These abnormal patterns can proactively alert the management of a bank to take right action and to implement right policies before the bank is actually faced with the exposed operational
Thus, RFID technologies can help minimize operational risks of banks.

In the next section, we present the Delta Model strategy framework, to understand different business strategies of a bank, which would help later to analyze if operational risk management should be tied to bank’s business strategy. The Delta Model is selected to study different strategies because it is an integrated model of Porter’s strategy frameworks, Porter (1991), and resource based strategy frameworks. The Delta Model further offers a framework that is based on customer bonding and it considers current technology and e-commerce businesses.
3.5 Delta Model Strategy Framework

This section presents strategy framework to identify sources and alignment of operational risks in the context of business and its competitive positioning.

Hax and Majluf (1996) presents Delta Model framework, as shown in the following Figure 19, which describes the strategic positioning as one of three distinctive bases: Best Product (BP), Total Customer Solution (TCS), and System Lock-in (SLI). Hax and Wilde (2001) further describes that the BP position could be attained by following Cost strategy (e.g., South West Airlines) or Differentiation strategy (e.g., Sony Wega), the TCS position can be attained by following Customer Integration strategy (e.g., EDS), Redefining Customer Relations strategy (e.g., Saturn), or Horizontal Breadth strategy (e.g., Fidelity), and the SLI position can be attained by following Proprietary Standards (e.g., Microsoft), Dominant Exchange (e.g., eBay), or Exclusive Channel (e.g., Wal-Mart).

The “Cost” strategy is to compete in the market by offering low price product or service and companies that employ this strategy enjoy the cost advantage in the market. The “Differentiation” strategy is to compete in the market based on offering differentiated product or service in terms of new products, new features or good quality. The “Customer Integration Strategy” is to compete in the market by integrating its customers through systems or processes so that these customers will be unlikely to switch.
the vendor. The “Redefining the Customer Relationship” strategy is to compete in the market by transforming the relationship with its customers to a higher level so that these customers will be unlikely to switch the vendor. The “Horizontal Breadth” strategy is to compete in the market by offering a large scope of products or services. The “Exclusive Channel” strategy is to compete in the market by having an exclusive distribution channel that is dominant and is not accessible by competitors. The “Dominant Exchange” strategy is to compete in the market by establishing a large exchange of commerce. The “Proprietary Standards” strategy is to compete in the market by innovating proprietary technologies and having these technologies turned into industry standards.

Source: Hax and Majluf (1996)

Figure 19. Delta Model Strategic Positioning

The Delta Model further says that different strategies can be enabled through effective
Achieving a particular strategic positioning (BP, TCS or SLI) is difficult for a bank unless the bank undergoes the strategy making process in an integrated approach. Delta Model also presents an integrated strategy making process framework, as shown below in Figure 20, the strategy process is used to identify the key elements of the strategic plan, to outline action plans, and to define appropriate performance measures. There are twelve steps in total to explain the strategy process, however, the thesis focus is on operational risk management, and hence the importance of relevant elements of this strategy framework will be gathered by the survey.
The strategy making process framework has a total of twelve steps. Step 1 is the overview of the business, the Step 2 is the positioning which identifies the basis upon which its strategy will be defined and implemented. The Step 3 defines the customer segmentation to be used by the business, and the mission of the business is defined as a result of the analysis and documentation provided in Step 4.

The Step 5 is an analysis of the industry structure. Step 6 is an analysis of company’s competitive positioning, which identifies the strengths, weaknesses, opportunities and threats of the business in the market.

Based upon the analyses of Step 5 and 6, the Strategic Agenda for the company as a business is explored in detail in Step 7. The specific “adaptive processes”, Customer Targeting (Step 8), Operational Effectiveness (Step 9) and Innovation (Step 10), follow on naturally from the Strategic Agenda to further clarify and focus the strategic activities of the business.

Once the appropriate strategic thrusts for the business and adaptive processes have been defined, a budget can be developed which includes both strategic funding and allocated operational revenues and expenses, as provided in Step 11.

Aggregate and granular measures will be used to gauge the performance of a company and is examined in Step 12.
In the next chapter, the survey will be explained and analyzed to shed insights on what strategies need to be aligned with operational risk management and what business areas can be mapped with RFID technologies to minimize operational risks. This analysis is very crucial to know if a bank should adopt a customized best practice to effectively manage operational risks and if RFID technologies can be helpful in minimizing operational risks.
4. Survey and Analysis

4.1 Introduction

A survey is conducted with several national and global banks to gather data on operational risks and associated business strategies. The survey is designed to help understand the dynamics of operational risk management and its linkage with the business strategy and underlying business areas that need to be improved. After analyzing the survey data, recommendations are made on business areas to implement RFID technologies and a new operational risk management framework is presented.

The survey has a total of six questions that are categorized as causes of operational risks, types of operational risks, losses as a result of operational risks, other banking risks, business strategies, operational risk processes, and these questions are divided into total of 46 responses, as shown in Appendix 1.

4.2 Data Gathering

The questionnaire was designed to help analyze operational risk management, business strategy, business areas, and linkages among them. The survey was sent out to 30 banks, of which 16 banks responded. The data sample was made based on geography (US, Europe, and Asia) and size (small, medium, large) and included sixteen banks from various categories such as national banks, international banks and regional
banks. The selection of banks is based on subjective opinions and we, however, think that it is a good representative of the banking industry.

The questions are separated into six categories as follows:

- Causes of operational risks
- Events of operational risks
- Losses as a result of operational risks
- Risk types
- Business strategy
- Operational processes

These six categories are further divided into 46 items which we refer as questions, here onwards, for sake of simplicity. The complete questionnaire is shown in Appendix 1.

In the next section, we present the analysis of survey data.
4.3 Analysis

In this section, the tabulated data is analyzed in the context of several financial operational risks. We analyze the use of RFID technologies to support the better management of operational risk. Gaps are identified with respect to best practice, and finally recommendations are presented along with construction of operational risk management framework.

The responses are tabulated and presented as shown in Appendix 2, where B1 through B16 refers to banks 1 through 16. There are a total of six categories and 46 questions (Q1 ~ Q46) in rows and total of sixteen banks (B1 ~ B16) in columns. The response ‘1’ indicates lowest on the scale and response ‘5’ indicates highest on the scale.

The tabulated statistics of all responses are shown below in Table 1. The data is sorted in the order of average score within each category (Risk types, OR causes, OR events, OR loss, Strategy, OR processes).
<table>
<thead>
<tr>
<th>Category</th>
<th>Question</th>
<th>Min</th>
<th>Avg</th>
<th>Med</th>
<th>Mode</th>
<th>Max</th>
<th>Std D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk types</td>
<td>Credit risk</td>
<td>4</td>
<td>4.81</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.4</td>
</tr>
<tr>
<td></td>
<td>Market risk</td>
<td>4</td>
<td>3.88</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0.5</td>
</tr>
<tr>
<td></td>
<td>Operational risk</td>
<td>3</td>
<td>3.5</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>0.73</td>
</tr>
<tr>
<td></td>
<td>Misalignment with strategy</td>
<td>3</td>
<td>3.5</td>
<td>3.5</td>
<td>3</td>
<td>4</td>
<td>0.52</td>
</tr>
<tr>
<td>OR causes</td>
<td>People</td>
<td>4</td>
<td>4.75</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.45</td>
</tr>
<tr>
<td></td>
<td>Internal processes</td>
<td>3</td>
<td>4.31</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0.7</td>
</tr>
<tr>
<td></td>
<td>System</td>
<td>3</td>
<td>3.31</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0.48</td>
</tr>
<tr>
<td></td>
<td>External event</td>
<td>1</td>
<td>1.68</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>0.67</td>
</tr>
<tr>
<td>OR events</td>
<td>Business disruption and system failure</td>
<td>4</td>
<td>4.81</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.4</td>
</tr>
<tr>
<td></td>
<td>Internal fraud</td>
<td>4</td>
<td>4.75</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.45</td>
</tr>
<tr>
<td></td>
<td>Clients, products and business practices</td>
<td>4</td>
<td>4.75</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.45</td>
</tr>
<tr>
<td></td>
<td>Execution, delivery and process management</td>
<td>4</td>
<td>4.75</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.45</td>
</tr>
<tr>
<td></td>
<td>External fraud</td>
<td>3</td>
<td>3.25</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0.45</td>
</tr>
<tr>
<td></td>
<td>Damage to physical assets</td>
<td>2</td>
<td>3.25</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0.68</td>
</tr>
<tr>
<td></td>
<td>Employment practices and work place safety</td>
<td>2</td>
<td>2.75</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>0.45</td>
</tr>
<tr>
<td>OR loss</td>
<td>Legal liability</td>
<td>4</td>
<td>4.69</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.48</td>
</tr>
<tr>
<td></td>
<td>Regulatory and compliance (including taxation)</td>
<td>4</td>
<td>4.69</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.48</td>
</tr>
<tr>
<td></td>
<td>Write-downs</td>
<td>4</td>
<td>4.56</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.51</td>
</tr>
<tr>
<td></td>
<td>Loss of recourse</td>
<td>4</td>
<td>4.31</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0.48</td>
</tr>
<tr>
<td></td>
<td>Restitution</td>
<td>3</td>
<td>4.06</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0.67</td>
</tr>
<tr>
<td></td>
<td>Loss of damage to assets</td>
<td>3</td>
<td>3.81</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0.64</td>
</tr>
<tr>
<td>Strategy</td>
<td>Regulatory compliance</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Staff (Internal people)</td>
<td>4</td>
<td>4.94</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.25</td>
</tr>
<tr>
<td></td>
<td>Systems reconciliation</td>
<td>4</td>
<td>4.68</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.34</td>
</tr>
<tr>
<td></td>
<td>Value for customer</td>
<td>4</td>
<td>4.69</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.48</td>
</tr>
<tr>
<td></td>
<td>Operational efficiency</td>
<td>4</td>
<td>4.69</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.48</td>
</tr>
<tr>
<td></td>
<td>Corporate governance (Operational control)</td>
<td>3</td>
<td>4.69</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.7</td>
</tr>
<tr>
<td></td>
<td>Processes</td>
<td>3</td>
<td>4.69</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.6</td>
</tr>
<tr>
<td></td>
<td>Trust or Credibility</td>
<td>4</td>
<td>4.63</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.5</td>
</tr>
<tr>
<td></td>
<td>Technology</td>
<td>3</td>
<td>4.19</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0.75</td>
</tr>
<tr>
<td></td>
<td>Network advantage</td>
<td>2</td>
<td>4.13</td>
<td>4.5</td>
<td>5</td>
<td>5</td>
<td>1.02</td>
</tr>
<tr>
<td></td>
<td>Customer loyalty</td>
<td>3</td>
<td>4.06</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>0.85</td>
</tr>
<tr>
<td></td>
<td>Brand power</td>
<td>2</td>
<td>3.94</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0.93</td>
</tr>
<tr>
<td></td>
<td>Product innovation (Differentiation)</td>
<td>2</td>
<td>3.94</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0.93</td>
</tr>
<tr>
<td></td>
<td>Growth</td>
<td>3</td>
<td>3.5</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>0.82</td>
</tr>
<tr>
<td></td>
<td>Competitive Environment advantage</td>
<td>2</td>
<td>3.38</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>0.89</td>
</tr>
<tr>
<td></td>
<td>Business complexity</td>
<td>1</td>
<td>3.06</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>1.12</td>
</tr>
<tr>
<td></td>
<td>Cost position</td>
<td>1</td>
<td>2.94</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>1.06</td>
</tr>
<tr>
<td></td>
<td>Real Asset advantage</td>
<td>2</td>
<td>2.75</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0.68</td>
</tr>
<tr>
<td></td>
<td>Government protection</td>
<td>1</td>
<td>1.94</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0.44</td>
</tr>
<tr>
<td></td>
<td>Star-performers</td>
<td>1</td>
<td>1.56</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>0.81</td>
</tr>
<tr>
<td>OR processes</td>
<td>Cash management</td>
<td>4</td>
<td>4.68</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.34</td>
</tr>
<tr>
<td></td>
<td>Tracking access to valuable assets</td>
<td>4</td>
<td>4.69</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.48</td>
</tr>
<tr>
<td></td>
<td>Payments processing</td>
<td>3</td>
<td>4.38</td>
<td>4.5</td>
<td>5</td>
<td>5</td>
<td>0.72</td>
</tr>
<tr>
<td></td>
<td>Document management</td>
<td>3</td>
<td>4.19</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0.75</td>
</tr>
<tr>
<td></td>
<td>Physical assets</td>
<td>2</td>
<td>3.06</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0.57</td>
</tr>
</tbody>
</table>

Table 1. Tabulated Statistics of Survey Responses

60
Operational Risk Causes

Responses to questions on Operational Risk Causes are tabulated with statistics as shown below in Table 2.

<table>
<thead>
<tr>
<th>Category</th>
<th>Question</th>
<th>Min</th>
<th>Avg</th>
<th>Med</th>
<th>Mode</th>
<th>Max</th>
<th>Std D</th>
</tr>
</thead>
<tbody>
<tr>
<td>OR causes</td>
<td>People</td>
<td>4</td>
<td>4.75</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.45</td>
</tr>
<tr>
<td></td>
<td>Internal processes</td>
<td>3</td>
<td>4.31</td>
<td>4</td>
<td>5</td>
<td>0.7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System</td>
<td>3</td>
<td>3.31</td>
<td>3</td>
<td>4</td>
<td>0.48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>External event</td>
<td>1</td>
<td>1.69</td>
<td>1</td>
<td>3</td>
<td>0.87</td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Tabulated Statistics of Operational Risk Causes

The respondents ranked people and internal processes as being the most common causes of operational risks. It is interesting to note that people are controllable, yet they were reported as the main source of operational risks for banks. The “internal fraud” as an operational risk event occurrence has responses ranging from 4 to 5 with the mean 4.7, which is high as well, leading to conclude that it is people who cause internal fraud in banks.

The “external event” as a cause of operational risk event occurrence has responses ranging from 1 to 3 with the mean 1.6 only, which leads to conclude that the external event is not considered as significant source of operational risk for these banks.

Operational Risk Events

Responses to questions on Operational Risk Events are tabulated with statistics as shown below in Table 3.
The events with the most impact were business disruption, internal fraud, business practices, and process management. Note again that these are all internally controllable events for the most part. Also, physical events (safety and physical asset damage) were not important.

**Operational Risk Losses**

Responses to questions on Operational Risk Losses are tabulated with statistics as shown below in Table 4.

The most critical losses were identified as legal liability, compliance, and write-downs. However, all losses are ranked as closed to 4 or higher, which indicates that any loss arising from occurrence of operational risk event is significant. Again, though note that physical asset damage is not that critical.
Risk Types

Responses to questions on Risk Types are tabulated with statistics as shown below in Table 5.

<table>
<thead>
<tr>
<th>Category</th>
<th>Question</th>
<th>Min</th>
<th></th>
<th>Avg</th>
<th>Max</th>
<th>Mode</th>
<th>Max</th>
<th>Std D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk types</td>
<td>Credit risk</td>
<td>4</td>
<td>4.81</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Market risk</td>
<td>4</td>
<td>4.38</td>
<td>4</td>
<td>5</td>
<td>0.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operational risk</td>
<td>3</td>
<td>3.5</td>
<td>3</td>
<td>5</td>
<td>0.73</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Misalignment with strategy</td>
<td>3</td>
<td>3.5</td>
<td>3</td>
<td>4</td>
<td>0.52</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5. Tabulated Statistics of Risk Types

Respondents reported the most important risk types as credit risk and market risk. It is interesting to note that operational risk is not considered as important as credit or market risk, even though there are instances of failure of banks due to operational risks. Moreover, the impact of loss due to such a failure of a bank is enormous and is to the extent that the bank has to be closed down.

Strategy

Responses to Strategy questions are tabulated with statistics as shown in Table 6.

<table>
<thead>
<tr>
<th>Category</th>
<th>Question</th>
<th>Min</th>
<th></th>
<th>Avg</th>
<th>Max</th>
<th>Mode</th>
<th>Max</th>
<th>Std D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy</td>
<td>Regulatory compliance</td>
<td>5</td>
<td>4.5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Staff (Internal people)</td>
<td>4</td>
<td>4.94</td>
<td>6</td>
<td>6</td>
<td>0.26</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Systems reconciliation</td>
<td>4</td>
<td>4.86</td>
<td>5</td>
<td>5</td>
<td>0.34</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Value for customer</td>
<td>4</td>
<td>4.69</td>
<td>5</td>
<td>5</td>
<td>0.48</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operational efficiency</td>
<td>3</td>
<td>4.69</td>
<td>5</td>
<td>5</td>
<td>0.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Corporate governance (Operational control)</td>
<td>3</td>
<td>4.69</td>
<td>5</td>
<td>5</td>
<td>0.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Processes</td>
<td>3</td>
<td>4.69</td>
<td>5</td>
<td>5</td>
<td>0.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trust or Credibility</td>
<td>4</td>
<td>4.63</td>
<td>6</td>
<td>6</td>
<td>0.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Technology</td>
<td>3</td>
<td>4.19</td>
<td>4</td>
<td>5</td>
<td>0.75</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network advantage</td>
<td>2</td>
<td>4.13</td>
<td>4.5</td>
<td>5</td>
<td>1.02</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Customer loyalty</td>
<td>3</td>
<td>4.05</td>
<td>4</td>
<td>6</td>
<td>0.96</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Brand power</td>
<td>2</td>
<td>3.94</td>
<td>4</td>
<td>5</td>
<td>0.93</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Product innovation (Differentiation)</td>
<td>2</td>
<td>3.94</td>
<td>4</td>
<td>5</td>
<td>0.88</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Growth</td>
<td>3</td>
<td>3.6</td>
<td>3</td>
<td>6</td>
<td>0.82</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Competitive Environment advantage</td>
<td>2</td>
<td>3.38</td>
<td>3</td>
<td>5</td>
<td>0.89</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business complexity</td>
<td>1</td>
<td>3.06</td>
<td>3</td>
<td>5</td>
<td>1.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cost position</td>
<td>1</td>
<td>2.94</td>
<td>3</td>
<td>6</td>
<td>1.06</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Real Asset advantage</td>
<td>2</td>
<td>2.75</td>
<td>3</td>
<td>4</td>
<td>0.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Government protection</td>
<td>1</td>
<td>1.94</td>
<td>2</td>
<td>3</td>
<td>0.44</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Star-performers</td>
<td>1</td>
<td>1.66</td>
<td>1</td>
<td>3</td>
<td>0.81</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6. Tabulated Statistics of Strategies
The most important strategies were based on compliance, internal people, systems reconciliation, customer value, operational efficiency, governance and operational control, processes, trust, technology, network advantage, customer loyalty, and brand power.

Three distinct strategy groups are identified using the graph as shown in the following Figure 21. Strategy questions are on horizontal axis and responses are on vertical axis; a separate graph is drawn for each bank B1 through B16.
As there is so much variation between each bank in the graph, it indicates that the banks follow different strategic positioning. Based on high importance and low response variation, we find that there are three distinct strategic options (Brand position, Governance and operational control position, Growth position). This indicates that the strategies differ among banks but they are clubbed together within these groups. These three groups with associated strategies are presented below in Table 7.

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Avg Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes</td>
<td>4.69 BP</td>
</tr>
<tr>
<td><strong>Brand power</strong></td>
<td></td>
</tr>
<tr>
<td>Product innovation (Differentiation)</td>
<td>3.94 BP</td>
</tr>
<tr>
<td>Cost position</td>
<td>2.94 BP</td>
</tr>
<tr>
<td>BP Total</td>
<td>15.5</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>5 TCS</td>
</tr>
<tr>
<td>Staff (Internal people)</td>
<td>4.94 TCS</td>
</tr>
<tr>
<td>Systems reconciliation</td>
<td>4.68 TCS</td>
</tr>
<tr>
<td><strong>Governance and operational control</strong></td>
<td></td>
</tr>
<tr>
<td>Trust or Credibility</td>
<td>4.63 TCS</td>
</tr>
<tr>
<td>Technology</td>
<td>4.19 TCS</td>
</tr>
<tr>
<td>Customer loyalty</td>
<td>4.06 TCS</td>
</tr>
<tr>
<td>Business complexity</td>
<td>3.06 TCS</td>
</tr>
<tr>
<td>TCS Total</td>
<td>35.4</td>
</tr>
<tr>
<td>Value for customer</td>
<td>4.69 SLI</td>
</tr>
<tr>
<td>Operational efficiency</td>
<td>4.69 SLI</td>
</tr>
<tr>
<td>Network advantage</td>
<td>4.13 SLI</td>
</tr>
<tr>
<td><strong>Growth</strong></td>
<td></td>
</tr>
<tr>
<td>Competitive Environment advantage</td>
<td>3.38 SLI</td>
</tr>
<tr>
<td>Real Asset advantage</td>
<td>2.75 SLI</td>
</tr>
<tr>
<td>Government protection</td>
<td>1.94 SLI</td>
</tr>
<tr>
<td>Star-performers</td>
<td>1.56 SLI</td>
</tr>
<tr>
<td>SLI Total</td>
<td>26.6</td>
</tr>
</tbody>
</table>

Table 7. Strategy and Base Positioning

After further evaluation of strategy positionings with the Delta Model strategy framework, they appear to be linked to Best Product (BP), Total Customer Solutions (TCS) and System Lock-In (SLI), as shown in the following Figure 22. Here, the BP is aligned with Brand Position of operational risk management, TCS is aligned with
Governance and Operational Control of operational risk management, and SLI is aligned with Growth.

Figure 22. Delta Model with ORM Positioning

Here, we have three distinct clusters, each associated separately with Brand Position, Growth Position or Corporate Governance Position.

Therefore, we would argue that managing operational risks in isolation won’t result in containing the risk losses, but if they are aligned with business strategy the containment of risk losses seems to be possible. However, interestingly the differentiation of product did not figure in operational risk management. Considering the notion that
brand can be built by cost position or product differentiation position and the survey analysis says that the product differentiation is not important for operational risk management, one could therefore think of Brand position is same as Cost position.

We have also analyzed the data using a statistical technique called clustering. Before explaining the analysis of clustering, we would present below an overview of this statistical technique. To analyze the data using the statistical technique, we used JMP software which is windows based SAS software.

The “Clustering” statistical technique groups the points whose values are close to each other relative to others. In other words, the data with similar values are clumped together to form clusters. Clustering is a process that starts with each point in its own cluster. At each step, the two clusters that are closest in terms of responses are combined into a single cluster. This process continues until there is only one cluster containing all the points. This kind of clustering is good for small data sets (a few hundred observations) (JMP 2004).

While clustering the data points into specific number of clusters, the distance formula is used to see which point is close to which cluster. There are various methods to calculate the distance. We used Ward’s minimum variance method where the distance between two clusters is the ANOVA sum of squares between the two clusters added up over all the variables. At each generation, the within-cluster sum of squares is minimized.
over all partitions obtainable by merging two clusters from the previous generation. The sums of squares are easier to interpret when they are divided by the total sum of squares to give the proportions of variance (squared semi partial correlations) (JMP 2004).

Ward’s method joins clusters to maximize the likelihood at each level of the hierarchy under the assumptions of multivariate normal mixtures, spherical covariance matrices, and equal sampling probabilities.

Ward’s method tends to join clusters with a small number of observations and is strongly biased toward producing clusters with roughly the same number of observations. It is also very sensitive to outliers.

The distance when clustering calculated using Ward’s method is shown below (JMP 2004).

\[ D_{KL} = \frac{\frac{1}{N_K} \sum_{i \in C_K} (x_i - \bar{x}_K)^2 + \frac{1}{N_L} \sum_{j \in C_L} (x_j - \bar{x}_L)^2}{\frac{1}{N_K} + \frac{1}{N_L}} \]

where \( n \) is the number of observations,

\[ n \]
\[ v \] is the number of variables
\[ x_i \] is the \( i \)th observation
\[ C_K \] is the \( K \)th cluster, subset of \{1, 2, ..., \( n \)\}
\[ N_K \] is the number of observations in \( C_K \)
\[ \bar{x} \] is the sample mean vector
\[ \bar{x}_K \] is the mean vector for cluster \( C_K \)
\[ ||x|| \] is the square root of the sum of the squares of the elements of \( x \) (the Euclidean length of the vector \( x \))
\[ d(x_i, x_j) \] is \( ||x_i - x_j|| \)
With this overview in mind, we now analyze the data using clustering statistical technique.

We have analyzed the data by doing clustering of banks based on their responses to questions related to strategic positioning. See Figure 23.

Figure 23. Banks Clustering

We have found that there are three distinct bank clusters. Cluster 1 consists of banks 1, 5, 6, 7, 8 and 13. The cluster 2 consists of banks 2, 3, 4, 12, 14, 15 and 16. The cluster 3 consists of banks 9, 10 and 11. Each cluster is associated separately with a distinct strategy positioning. The strategy of Brand Position is aligned with operational risks of physical assets and system failures. The strategy of Growth Position is aligned with operational risks of people, legal and regulations. The strategy of
Corporate Governance Position is aligned with operational risk of internal and external processes. This strategy alignment with operational risk management is in line with the data analysis done before, which reinforces that the operational risk management has to be aligned with business strategies.

However, an interesting observation is that we couldn’t notice any trend by type (regional, national or international) or size (small, medium or large) as shown in Figure 24 & 25.

![Banks Size vs Strategy](image)

**Figure 24. Banks Strategies by Size**
Since there is no particular trend among banks by either size (small, medium or large) or type (regional, national or international), it leads to think that operational risk management applies to all banks, no matter what the size is and where it is operating.

I have analyzed the data by doing clustering of responses to questions related to strategic positioning, as shown below in Figure 26.
We find here that there are again three distinct clusters. Cluster 1 consists of Cost position, Real asset advantage, Government protection, Growth, and Business complexity. Cluster 2 consists of Brand power, Customer loyalty, Product innovation, Network advantage, and Competitive environment advantage. Cluster 3 consists of Customer value, Operational efficiency, Governance and operational control, System reconciliation, Internal people, Technology, Processes, and Trust. Cluster 1 can be thought of as Growth cluster considering the fact that all other responses in this cluster are closely related to growth. Cluster 2 can be thought of as Brand cluster as other responses in this cluster are related to brand and customer satisfaction. Cluster 3 can be
thought of as corporate governance and operational control as other responses are related to operations and regular banking functions.

Interesting thing in this inverted clustering is that we have found Cost and Growth are in same cluster, but a new cluster called Brand is formed. This suggests that whether we should call Cost cluster or Brand cluster is not so clear.

In the following Figure 27, we have done clustering based on responses to questions related to operational risks. Here, we find that there are three clusters. Cluster 1 consists of Internal processes, Restitution, and Loss of asset damage. Cluster 2 consists of People, External fraud, Business disruption, Process management, Write-downs, Loss of recourse Legal liability, Compliance, Credit risk, and Market risk. Cluster 3 consists of System, External event, External fraud, Employment practices, Damage to physical assets, Operational risk, and Alignment of strategy. After analyzing the close relationship among responses within clusters, the cluster 1 represents processes, cluster 2 represents people, and cluster 3 represents physical assets/systems.

These three clusters are aligned with strategy position clusters explained before, which indicates that banks are not only saying that there are distinct strategies to be followed but also saying there are distinct emphasis on operational risks. Therefore, aligning the bank’s operational risk with its strategy is crucial.
To understand how banks are treating operational risks in comparison with other risks such as credit risk and market risk, we have done clustering on risk types as shown in the following Figure 28.

Figure 27. Operational Risk Emphasis
Among risk types, we find that there are two distinct clusters. Cluster 1 consists of credit risk and market risk. Cluster 2 consists of operational risk and misalignment with strategy. This shows that misalignment with strategy is not much related to credit risk or market risk but it is very much related to operational risk. Therefore, it is important for a bank to align operational risk management with its own business strategy.

To help identify business areas that can be associated with RFID technologies, we have done the clustering based on responses to questions related to importance of business areas as shown in the following Figure 29. There are three distinct clusters. The business areas of “Cash management” and “Tracking access to physical assets” are in same cluster (Cluster 1), indicating that these two have some commonality - therefore we would say tracking access to cash bundles in the bank using RFID technologies is important.
Figure 29. Business Areas for Operational Risk Management

Cluster 2 consists of business areas of “Document management” and “Payments processing”, which can be improved by incorporating RFID technologies. Cluster 3 consists of business area of “Physical assets”, which banks considered as a separate resource and it can be RFID tagged just like any inventory product in supply chain management.
4.4 Results and Recommendations - ORM Business Area Processes for RFID Technologies

The following wheel diagram, Figure 30, summarizes all of the business areas of a bank where RFID technologies could be used to minimize the operational risks based on the importance shown by survey responses.

![ORM Business Areas for RFID Technologies](image)

Figure 30. ORM Business Areas for RFID Use

The business areas mentioned in the above wheel diagram are potential candidates for RFID use and these will create the need for having audit trail of access information (Access Trail) to the assets. There are also customer profiling applications, but in the interest of privacy concerns, we will not highlight this use.
4.5 Results and Recommendations – Operational Risk Management (ORM) Framework

Based on previous analysis we have devised an effective operational risk management framework as shown in the following Figure 31. This framework consists of 6 layers: 1) Best practices, 2) Custom, 3) Culture, 4) Structure, 5) Philosophy, and 6) Value. We believe that no single improvement such as audit review and risk governance would significantly improve the operational risk management, thus we recommend that banks follow a holistic view considering all underlying elements of these six layers.

Operational Risk Management (ORM) Framework

Figure 31. ORM Framework
The best practice or benchmark such as Basle II provides only the first step needed for effective operational risk management. Second step is to align four different elements (ORM strategy and its alignment with business strategy, RFID based technology strategy, ORM metrics and measurement, External relationship management). Third step is to consider People and Performance Culture Management. The fourth step is to put in place right structures (Governance Structure and Organization Structure). The fifth step is to have ORM Philosophy that is responsible to make sure the ORM is dynamically aligned with the changing business strategy as business climate is changed. Successful building of these five steps creates an effective ORM organization, creating value out of operational risk management.
5. Conclusion and Further Research

Operational risk management is indeed very critical and it should be aligned with a bank’s business strategy such as competing on Cost, Growth, or Corporate Governance & Operational Control. The most important operational risk management is with people, cash, physical assets and documents, and they should be RFID-tagged so that operational risks could be mitigated to some extent. The banks could minimize operational risks by following the operational risk management framework.

This work could be further carried out by examining the large amount of data from banks that have serious operational risk management troubles in the past to compare and contrast with the findings. Also, since banking industry is going to implement operational risk management techniques, as per Basle II benchmark, in the near future, it would be interesting to study what actually banks have done and what was in fact expected, and how successfully they could implement the operational risk management solutions.
References


Basle II, 2003, Basle II Accord, BIS, October

BIS, Banking International Settlement, http://www.bis.org/


Hax, Arnoldo C., Wilde II, Dean L, 2001, The Delta Project: Discovering New Sources of Profitability in a Networked Economy, PALGRAVE.


JMP – SAS Manual, 2004


Appendix 1. Survey Questions

1) Causes of operational risk. (What causes operational risk event happening?)
Please rate each of the following on the scale of 1-5, one being the cause of lowest risk and 5 being the cause of highest risk.
   a) Internal processes
   b) People
   c) System
   d) External event

2) Events of operational risk. (What operational risk events could happen?)
Please rate each of the following on the scale of 1-5, one being the lowest impact on bank and 5 being the highest impact on bank.
   a) Internal fraud
   b) External fraud
   c) Employment practices and work place safety
   d) Clients, products and business practices
   e) Damage to physical assets
   f) Business disruption and system failure
   g) Execution, delivery and process management

3) Losses due to operational risk events. (What could be the loss as result of operational risk events?)
Please rate each of the following on the scale of 1-5, one being the lowest loss and 5 being the highest loss.
   a) Write-downs
   b) Loss of recourse
   c) Restitution
   d) Legal liability
   e) Regulatory and compliance (including taxation)
   f) Loss of damage to assets

4) What importance would you give for the following risks?
Please rate each of the following on the scale of 1-5, one being the least important and 5 being the most important.
   a) Credit risk
   b) Market risk
   c) Operational risk
   d) Risk of misalignment of operational processes with the business strategy (cost-based, product differentiation-based, and growth-based)

5) What importance would you give for the following strategies?
Please rate each of the following on the scale of 1-5, one being the least and 5 being the most.
   a) Cost position
   b) Brand power
   c) Customer loyalty
   d) Real Asset advantage
   e) Government protection
   f) Product innovation (Differentiation)
   g) Network advantage (through complementors, customer-to-customer dependence, etc)
   h) Value for customer
   i) Operational efficiency
j) Growth
k) Corporate governance (Operational control)
l) Business complexity
m) Regulatory compliance
n) Systems reconciliation
o) Staff (Internal people)
p) Technology
q) Processes
r) Environment advantage (Market, Competition, Suppliers, Buyers, Complementors)
s) Trust or Credibility
t) Star-performers ratio with respect to other staff (1→ few star performers, 3→ same as other staff, 5→ many star performers)

6) What importance would you give for the following processes in terms operational risk management?
a) Cash management
b) Document management (including work flow processing such as approval, document usage, etc)
c) Physical assets (physical inventory) management
d) Tracking access to valuable assets by people, etc
## Appendix 2. Banks’ responses

<table>
<thead>
<tr>
<th>OR causes</th>
<th>B1</th>
<th>B2</th>
<th>B3</th>
<th>B4</th>
<th>B5</th>
<th>B6</th>
<th>B7</th>
<th>B8</th>
<th>B9</th>
<th>B10</th>
<th>B11</th>
<th>B12</th>
<th>B13</th>
<th>B14</th>
<th>B15</th>
<th>B16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal processes</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>People</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>System</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>External event</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>OR events</td>
<td>Internal fraud</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>External fraud</td>
<td>6</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Employment practices and work place safety</td>
<td>7</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Clients, products and business practices</td>
<td>8</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Damage to physical assets</td>
<td>9</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Business disruption and system failure</td>
<td>10</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>OR loss</td>
<td>Execution, delivery and process management</td>
<td>11</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Write-downs</td>
<td>12</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Loss of recourse</td>
<td>13</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Restitution</td>
<td>14</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Legal liability</td>
<td>15</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Regulatory and compliance (including taxation)</td>
<td>16</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Loss of damage to assets</td>
<td>17</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Risk types</td>
<td>Credit risk</td>
<td>18</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Market risk</td>
<td>19</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Operational risk</td>
<td>20</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Misalignment with strategy</td>
<td>21</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Cost position</td>
<td>22</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Brand power</td>
<td>23</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Customer loyalty</td>
<td>24</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Real Asset advantage</td>
<td>25</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Government protection</td>
<td>26</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Product innovation (Differentiation)</td>
<td>27</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Network advantage</td>
<td>28</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Value for customer</td>
<td>29</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Operational efficiency</td>
<td>30</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Growth</td>
<td>31</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Corporate governance (Operational control)</td>
<td>32</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Business complexity</td>
<td>33</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>34</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Systems reconciliation</td>
<td>35</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Staff (Internal people)</td>
<td>36</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Technology</td>
<td>37</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Processes</td>
<td>38</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Competitive Environment advantage</td>
<td>39</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Trust or Credibility</td>
<td>40</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Star-performers</td>
<td>41</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>OR processes</td>
<td>Cash management</td>
<td>42</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Document management</td>
<td>43</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Payments processing</td>
<td>44</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Physical assets</td>
<td>45</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Tracking access to valuable assets</td>
<td>46</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>