

THE NEAR-MISS MANAGEMENT OF OPERATIONAL RISK

Alexander Muermann
Assistant Professor of Insurance and Risk Management
The Wharton School, University of Pennsylvania
3641 Locust Walk, 306 CPC
Philadelphia, PA 19104-6218
Phone: 215-898-4751
Fax: 215-898-0310
Email: muermann@wharton.upenn.edu

Ulku Oktem
Senior Fellow at the Risk Management and Decision Processes Center
The Wharton School, University of Pennsylvania
3730 Walnut St., 558 JMHH
Philadelphia, PA 19104-6340
Phone: 215-573-7704
Fax: 215-573-2130
Email: oktem@wharton.upenn.edu

ABSTRACT

This article discusses the management process of operational risk in financial institutions. The authors summarize the difficulties associated with the applicability of traditional risk management means to operational risk and introduce the Near-Miss management concept as a potential tool for the banking industry.

INTRODUCTION

Over the last decades, both the banking industry and regulatory bodies have devoted massive resources to the management of market and credit risk. Models have been developed to assess both risk types based on which regulators set out transparent rules on capital requirements, supervisory review process, and market discipline to prevent banking crises. Those principles form the three pillars of “The New Basel Capital Accord” which has been issued by the Basel Committee on Banking Supervision (BCBS) in January 2001. It is not surprising that the regulation of the banking sector initiated a still ongoing debate about whether it should exist and if so, which risks should be covered under which pillar(s). Particularly the first pillar “minimum capital requirement” evoked a lot of discussion about its appropriate definition. We refer to Danielsson [2002] for a critical review on the properties of different risk measures, primarily of Value-at-Risk (VaR). Irrespective of this debate, the increasing sophistication in quantitative methodologies for market and credit risk measurement allowed banks to reduce their required capital allocation.

Only recently, the attention has shifted towards the risk management of operational risk. It has been recognized that events due to operational risk can have a devastating impact on the operations of banks. Famous cases include Barings’ insolvency and the Allied Irish Banks’ loss of \$750m due to rogue trading, the \$2bn settlement of class action lawsuit against Prudential Insurance due to fraudulent sales practices over 13 years, and the terrorist attacks of September 11. In response, regulators included the management of operational risk in their consultative document “The New Basel Capital Accord” [2001] which sets out guidelines under all three pillars. After reviewing over 250 documents from both market participants and academic institutions, the Basel Committee revised their position on operational risk management at its July 10, 2002 meeting. The Basel Committee reaffirms its position on capital requirement (Pillar One) for operational risk. However, it acknowledges the importance of *Advanced Measurement Approaches* under which banks would be allowed to determine capital requirement based on their internal operational risk assessment subject to qualitative and quantitative standards set by the Basel Committee (see “Working Paper on the Regulatory Treatment of Operational Risk”, September 2001).

In this paper, we first review the different steps of the risk management process with respect to operational risk in the banking industry: the definition of operational risk, quantitative and qualitative methods for measuring operational risk, and risk management methods with respect to operational risk. In these sections, we focus on the particular difficulties that arise with operational risk and argue that these steps cannot be treated separately as opposed to the management process of market or credit risk. We then propose the risk management concept “Near-Miss” which is used in the chemical, health and airline industries. Rather than focusing on capital requirement only, we suggest the concept “Near-Miss” to be used as an *Advanced Management Approach* to internally assess and manage operational risk in a dynamic and integrated way. It thus encompasses the *Advanced Measurement Approach* put forward by the Basel Committee.

DEFINING OPERATIONAL RISK

To facilitate the risk management decision process in large corporations, the overall risk faced by these institutions is subdivided into different risk categories. These categories are defined through different causes and/or effects. In the banking industry, market risk is defined as the systemic risk inherent in the capital market, i.e. it is the risk that is not diversifiable through trading in financial contracts. Credit risk is defined as loss exposures due to counterparties’ default on contracts. With respect to operational risk, there does not yet exist a definition that the banking industry has agreed upon. First definitions were mostly based on an exclusion principle such as “every type of non-quantifiable risk” or “all risks but market and credit risk”. The current definition of operational risk proposed by the Basel Committee on Banking Supervision (BCBS) in its “The New Basel Capital Accord” [2001]

“the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”

is clearly based upon the causes of operational risk. Although quite general, these definitions will make it difficult to appropriately assess the next steps in the risk management process; risk measurement and the selection of the appropriate management methods.

In our opinion, the difficulty in defining operational risk is two-fold. First, as operational risk is mostly idiosyncratic as opposed to market and credit risk, which have a

much larger systemic component, it will be difficult to pin down an industry-widely accepted definition. Second, a definition, somehow paradoxically, needs both to be based upon and abstract from the few major incidents that originally initiated the discussion about operational risk. As a response to the idiosyncrasy of operational risk, it seems more reasonable to us to internally define and categorize operational risk for its management. Over the last years, banks in fact started to internally define operational risk based on causes and effects related to their specific exposure. A possible categorization could have the following structure:

- Operations risk due to transaction failures, rogue trading etc.
- Physical risk due to loss or damage of assets such as buildings or computers
- Crime risk due to internal and external fraud
- Legal/liability risk due to employment practices, workplace safety, or changes in the regulatory environment
- Country risk due to severe changes in the political system

A way of abstracting from major incidents could involve a bank-internal reporting of minor incidents and observations, which would lead to a better understanding of the underlying risk structures and thus improve the existing definitions of operational risk. Clearly, such a categorization will have to change as banks learn more details about its particular exposures to operational risk through new incidents. We thus propose the implementation of an internal definition process, which dynamically adjusts according to new incidents or observations, rather than to fix a definition based on industry-impacting events such as the ones for market and credit risk.

In the following section, we discuss the assessment of operational risk with respect to both quantitative and qualitative measurement methods. We investigate the limitations of current methodologies as to their applicability to operational risk and suggest potential future directions.

MEASURING OPERATIONAL RISK

The accuracy of risk measurement methods crucially depends on the soundness of risk model and the availability of data. Proper risk modeling requires a thorough understanding of recurrent patterns that underlie the risk under consideration. The appropriateness of those risk models is inherently linked to data availability and thus the occurrence of events. Not only do incidents help better understanding the underlying risk structures but they also provide the ground for statistical testing of risk models. Furthermore, the accuracy of risk models depends on the measurability of outcomes and thus goes hand in hand with a sound definition and understanding of effects.

With respect to market risk, there exist large and publicly available data sets based on which the effects of market risk can be quantitatively measured as profit and losses (P&L) that arise from trading in financial markets within certain time periods. It is thus possible to deduce accurate estimates for distributional parameters by using sophisticated statistical analysis such as the estimation of volatilities based on intra-day trades. The assessment of credit risk and its management has improved immensely since banks in the eighties became aware of its potentially adverse impact. Various models and econometric techniques for credit risk valuation have been developed based on which regulatory capital requirement would have to be allocated to prevent major banking crisis (see Caouette et al. [1998] for an overview). The validity of those models relies on large databases, i.e. on frequently occurring credit risk events. Herring [1999] critically reviews the accuracy of those models and its potential impact on financial stability when dealing with low frequency events.

Operational risk, however, encompasses events with very differing frequencies and possibly patterns of occurrence and severities. As a first step in determining the applicability of statistical analysis it seems appropriate to qualitatively categorize potential incidents into a frequency – severity matrix (see figure 1 below) based on experience and experts' opinion.

Insert Exhibit 1 here

This matrix gives additionally first guidance in prioritization of events. Risk managers should pay highest attention to high frequency – high severity (area 1) and relatively low attention to

low frequency – low severity (area 4) events. After well-known cases of rogue trading (e.g. Barings or Allied Irish Banks) and in particular after the attacks of September 11, a lot of discussion across corporations, governmental bodies, and research institutions has been focusing on how to manage low frequency – high severity (area 2) events and relatively little on the management of high frequency – low severity (area 3) events. It is our opinion, however, that by focusing on high frequency – low-impact events (area 3), we will be able to improve our understanding of low frequency – high impact events (area 2) as those frequent, small events may serve as a signaling device for rare but big events. Here we draw upon studies on Near-Miss management in the “safety” area and offer a systemic management tool that is presented below.

In the following, we discuss both the high frequency – low severity and low frequency – high severity areas in more detail. We give examples of events related to operational risk, introduce quantitative and qualitative tools for and discuss difficulties with respect to risk measurement. For this purpose, we will assume that a solid definition of operational risk is in place based on which data can be collected and simulations and scenarios can be constructed.

Region 2: Low frequency – high severity

Low frequency – high severity events include most famous incidents, which doubtlessly have a major impact not only on the operations of affected banks but also in terms of creating awareness of their existence. Unfortunately, the low frequency of these events implies very few data points. The estimation of probabilities and loss distribution will thus only produce highly unreliable results. Risk management decisions based solely on those statistical outcomes may lead to consequences that are as devastating as the ones to which the analysis has been applied to. It seems appropriate to increase the size of the internal dataset and thus the reliability on data by considering external databases. In fact, in 2001 the Basel Committee on Banking Supervision started an “Operational Risk Data Collection Exercise” to gather information about banks’ internal capital allocations and their overall operational loss experience. However, data on operational losses are usually highly confidential and their reliability thus questionable, particularly with respect to low frequency

– high consequence events. Carefully designed scenario analysis based on experts’ opinions and post-event analysis seems to provide a better way of gaining knowledge about the driving factors and the magnitude of operational losses. Nevertheless, subjective risk perception of those events will play an important role when it comes to deciding on the appropriate risk management method.

Low frequency – high impact events are not unique to the banking industry. Other industries, such as the aviation, health and chemical process industry (CPI) are faced with similar issues. In those industries, risks that may cause potentially devastating events are managed by focusing on high frequency – low impact events. In particular, aviation and CPI over the last decades have been focusing on events classified as “Near-Misses” to reduce major accident rates. Recently there has been an increasing interest in expanding the concept to other areas, such as healthcare and information technology (National Academies of Engineering Meeting, February 2002). Such a management practice has not been implemented in the banking sector yet. For example, when an ordinary transaction fails causing a small loss, its causes ought to be explored to remedy the situation so that a major transaction failure does not occur. Below, we introduce this concept and its integration into a management system for reducing the likelihood of low frequency – high impact events by focusing on smaller incidents.

Region 3: High frequency – low severity

Examples of operational loss events that occur frequently and cause relatively small losses include transaction failure, credit card fraud, or accounting irregularities. The advantage of high frequency events is the possibility to create large databases to which statistical analysis can be accurately applied. Appropriate statistical analysis would include estimation procedures, simulations, and regression analysis. Historical data, if based on a thorough definition of outcomes related to operational losses, can be used to estimate the loss distribution, i.e. the probabilities of such events and subsequent losses within certain time periods. Parameters of the fitted loss distribution can then serve as input factors for further simulations. In addition, regression analysis can be applied to determine potential risk driving factors such as frequency of transactions or staff turnover.

It is the concern of risk managers that the qualitative matrix above is actually not accurate or stable and that low severity events actually turn out to be high severity events. To account for this possibility, extreme value theory has been applied in the way that the tail of the loss distribution is fitted separately by fat-tail distributions, such as the Pareto, Weibull, or Gumbel distribution, whereas the empirical distribution is used for the lower part of the loss distribution. We refer to the monograph by Embrechts et al. [1997] and the references therein for a concise overview on extreme value theory. A major drawback of that approach, however, is that risk measures (e.g. the Value-at-Risk) depending on the overall loss distribution are very sensitive to the chosen threshold level that separates the empirical from the fitted fat-tail distribution (see figure 2 below). A concept that defines optimality related to the choice of the threshold level has not been developed yet. Diebold et al. [2000] critically review the applicability of extreme value theory to risk management.

Insert Exhibit 2 here

Before we introduce the Near-Miss concept as a tool for managing operational risk in the banking sector, we first turn our attention to the traditional means.

MANAGING OPERATIONAL RISK

Risk managers usually have a large set of management methods available out of which the optimal combination should be selected with the aim of maximizing business value. Those methods include loss reduction, insurance within and outside of the company, or hedging. In the following, we discuss the potentials of those management practices with respect to operational risk.

- Operational loss prevention aims at reducing the frequency and/or severity of events leading to operational losses. Such activities include internal auditing, penalties, rewards, or duplication of processes and seem applicable when dealing with fraud, crime, mis-pricing, or system failure.

- Capital allocation against operational losses provides a means of self-insurance. The adequacy of the capital amount to be allocated relies on the validity of both the risk measure – the mapping between the loss distribution and the capital amount – and the underlying statistical analysis. Hence, this risk management method seems only applicable in the context of high frequency events such as transaction failure, credit card fraud, or accounting irregularities.
- As most losses due to operational risk are bank-specific and thus almost uncorrelated across different banks, insurance provides an excellent means of pooling and diversifying those risks across the industry. In fact, insurance products based on operational risks have been available for decades such as single-peril coverage for *Directors and Officers Liability* or *Professional Indemnity*. Only recently, events like unauthorized trading or computer crime have been included into multi-peril policies such as the FIORI-product (*financial institutions operational risk insurance*) launched by Aon and Swiss Re. However, both ex-ante and ex-post moral hazard issues may give rise to high premiums and renegotiation costs. Not only may operational risk be managed more negligent if insurance is in place (ex-ante), but also the difficulty in measuring actual losses may cause biased reporting (ex-post).
- Hedging provides another channel of reducing risk exposures. The existence of an instrument (e.g. financial derivative) whose value depends to some extent on the fundamental exposure of a corporation is crucial for reducing the overall risk exposure through hedging. This idea has not only lead to the search for existing hedging opportunities but also to the creation of new instruments as a response to growing concerns about the consequences of certain risk types. Particularly after major natural catastrophes in the nineties – Hurricane Andrew, the Northridge and Kobe earthquakes – risk securitization appeared in the form of exchange-traded and OTC financial instruments. Examples of these contracts include Catastrophe Futures and Options that were traded at the Chicago Board of Trade and Catastrophe Bonds that are traded as OTC derivatives. Following this development, it has been suggested to create financial instruments to deal with operational risk. However, the experience

with securitization of catastrophic risk has shown that such a market can only be successful if these instruments are designed in a way as to overcome problems arising from moral hazard issues, basis risk, and non-transparent valuation mechanisms. These problems seem very apparent in the context of operational risk as most operational losses are due to bank-specific, internal events. The market for tax derivatives, however, represents an exception to the issues mentioned above.

Risk prevention and reduction thus seems to be the most appropriate management device with respect to operational risk. The implementation of such internal management mechanisms is immensely powerful particularly during times in which underlying risk patterns have not been thoroughly understood, sound risk models have not been developed, and large databases have not been constructed yet.

Regulation of Operational Risk

In response to the problems related to the risk management methods mentioned above, the banking industry called for regulatory bodies to address operational risk. Therefore, regulators set out a framework on capital requirements involving methods of risk quantification (see “The New Basel Capital Accord” [2001]). However, the idiosyncrasy of operational risk not only questions the point of the regulatory objective to prevent systemic crises but also causes any quantification framework outlined by regulators to be extremely vague – disregarding the difficulties mentioned in the above section on risk measurement. As the amount of capital to be allocated relies on the validity of those quantification methods, any capital determination from outside fails in addressing the specific risk causes and/or effects of different banks. On the contrary, regulatory capital requirement may have an adverse impact on risk taking behavior to provide a certain return on investors’ capital and thus cause additional operational losses. Last, there is no evidence yet that capital allocation may have avoided famous bankruptcies due to rogue trading or other operational risk events.

Proposal

Based on the above discussion, it seems most appropriate to implement a management system that internally defines operational risk, develops quantitative and qualitative frameworks of assessing operational risk, and determines the mixture of loss prevention tools that is most efficient for a particular bank. From our discussion it follows that these steps are inherently and almost viciously connected with each other. This relationship, furthermore, changes dynamically over time according to availability of data, accuracy of statistical methods, innovation of risk management methods and circumstances surrounding the bank's operations. To understand operational risk and its impact better we cannot focus on those risk management steps separately and for a given time frame only. One way to simultaneously address those steps is to solidly and continuously examine small, frequently occurring incidents.

NEAR-MISS – A RISK REDUCTION TOOL

We consider *Near-Misses* as weak signals some of which contain a genetic signature of a serious, adverse effect. In reviewing incidents in process industries, it has been observed that for every major accident there have been a large number of incidents with limited impact and an even larger number of incidents with no damage. Analogously, major operational losses in the banking industry have its predecessors in forms of small abnormalities that do not necessarily cause any losses. On the contrary, those precursors sometimes appear as extreme profits as, for example, in the case of Barings. Such structure of incidents is commonly accepted in process industries and represented by the safety pyramid (see Bird and Germain [1996] such as the one shown in figure 3 below). Near-Misses represent the lower portion of the pyramid.

Insert Exhibit 3 here

Despite their limited impact, Near-Misses provide insight into potential major adverse conditions and business disruptions. Therefore, addressing Near-Misses timely and properly

discourages major problems from flourishing (see Jones et al. [1999]). It is important to note that even though investigations have shown that almost all major incidents had precursors with minor or no consequences not all minor incidents have the potential to cause a major accident.

Near-Misses are defined in a variety of ways by different authors (see Barach and Small [2000] and Phimister et al. [2001]). While some definitions are very focused and based on the extent of the potential negative consequences, such as

“Near-Miss is an undesired event or sequence of events with potential to cause serious damage”

we prefer a broader definition which focuses not only on the negative side of Near-Misses but also on their positive contribution to a system’s operation. For the purpose of managing operational risk in financial institutions, we thus propose the following definition:

“Near-Miss” is an event, a sequence of events, or an observation of unusual occurrences that possesses the potential of improving a system’s operability by reducing the risk of upsets some of which could eventually cause serious damage.

Our definition contains three important features:

- It views Near-Misses as “improvement opportunities” which are positive experiences encouraging employees to report rather than to hide.
- It includes all operational disturbances, some of which have the potential to cause serious damage while others are inconveniences that mainly cause inefficiencies.
- It not only captures events but also includes observation.

We believe that by casting the net widely and positively we improve the chance of catching key precursors and indicators of major operational risks as well as identify system inefficiencies that can be addressed in a more leisurely manner. The latter can also have a big pay-off for an institution where the operating system includes continuous improvement principles.

Operational Risk Management Process

Along the lines of the Near-Miss system that has been developed for chemical process industries by Phimister et al. [2001], we propose the following eight-step “Operational Risk Management” (ORM) process for financial institutions:

- 1 Identification (recognition)** of a Near-Miss.
- 2 Disclosure (reporting)** of the identified information/incident.
- 3 Prioritization and Classification** of the information for future actions.
- 4 Distribution** of the right level of information to the proper channels.
- 5 Analyzing Causes** of the problem.
- 6 Identifying Solutions** (remedial actions).
- 7 Dissemination** of actions to the implementers and (optional) general information to a larger group for their knowledge.
- 8 Resolution (wrap-up)** of all open actions and completion of reports.

Step 1: Identification

The first step of any Near-Miss system is the recognition of a Near-Miss. This is especially challenging in a financial institution’s setting where the operational risk factors are not well defined. The broad definition of Near-Miss given earlier compensates for the vagueness of operational risk making Near-Miss a natural fit to identify most, if not all, operational risk issues. In practice, it would help to provide examples and guidelines to improve awareness. Also, we advise to revisit the definition periodically looking for improvement opportunities based on experience to date. Establishing a culture sensitive to the Near-Miss concept is critical for successful implementation of a Near-Miss system and takes time and effort to develop. Identification of current and potential problems can be encouraged by recognizing and rewarding observant people and by publicizing identified problems as well as the actions taken to address them.

Step 2: Disclosure

Reporting should be made very simple to encourage everyone who observes or experiences a problem to fill-out a report without spending much time and effort. It is important to capture as many Near-Misses as possible even though not all of them will have the same importance. Reporting can be encouraged by acknowledgement and recognition. It is important to note that the person who identifies a Near-Miss and the one who reports it does not have to be the same. For example, if someone complains to her/his supervisor about a problematic situation, the supervisor, who may resolve this person's problem or bring it to the attention of others, can also report it as a Near-Miss.

Step 3: Prioritization and Classification

This is a very critical step in establishing an **effective** Near-Miss system since this step determines, out of the large number of Near-Miss reports, which ones will require and to what extent the attention of the limited resources of the financial institution. It is at this step a decision is made about the nature as well as the extent of the further attention (analysis, evaluation) that has to be given to a Near-Miss. Therefore, the prioritization process has to be well defined from the beginning and revised continuously to include lessons learned from an on-going stream of reports and analysis. Because of its critical nature in the whole process, in the next section we will look at how prioritization would work in a financial organization.

Step 4: Distribution

Once Near-Miss (NM from hereon) information is reported into the "NM System", it needs to be directed to the people who can act on this information. Identification of these people strongly depends on the design of Priority/Classification (P/C) matrix developed by each institution (see appendix). Since the operational risk landscape is not well defined in financial institutions, we suggest each institution start from a central clearing person at each location who can direct the information to the right department for their attention. As the NM

practice progresses natural categories of NM's and the proper follow-up channels will emerge and will help establish a standard procedure for this step.

Step 5: Causal Analysis

Once a NM is reported based on the given priority the reporter, a supervisor or a group of experts related to the subject matter (e.g. IT support) should identify the cause(s) of the problem and come-up with actions(s) to eliminate the recurrence of this or similar incidents. Clearly priority given to a particular NM plays an important role in these follow-up activities. If the reported incident is labeled as “high priority”, it may require a rather thorough causal analysis such as identification of root-causes to help tackle the problem at the basic level. This can be accomplished through a team of people analyzing the situation using various root-cause analysis techniques (see Guidelines for Investigating Chemical Process Incidents, American Society of Safety Engineers [1992]). As an example, let us assume that within a period of several months various incidents were reported related to either sending information to the wrong person or entering the data to the wrong location on the computer program with respect to individual savings account transactions. Recurrence of similar incidents indicates that implemented solutions have not been satisfactory. Over time, due to repeating events of similar nature, the priority of new NMes will become higher with each report. At some point this will result into a meeting involving the designer of the web system and several different users, including the ones who reported the related NMes, to talk about necessary changes of the design of the screen and/or flow of the operation. Identification of direct and root causes is another developmental process that we suggest to be revised periodically to address the needs of each NM appropriately.

Step 6: Solution Identification

Once causes of a problem are identified, the next step is finding viable solutions for each cause. A few important points for this step are:

- Matching solutions to causes, hence making sure that each cause has been addressed.

- Reviewing identified solutions to ensure that they will not cause new problems themselves (management of change).
- If possible, including a member of the department who will implement the solution in the discussions.

Step 7: Dissemination

Once an action (or a set of actions) is determined

- the action should be approved by the proper channels and assigned to a group to implement
- a larger group including other departments, financial institutions or contracts, etc. may need to be informed of the incident and the actions taken.

Both of these activities are highly dependent on the nature of the operational issues being considered and must be completed (especially, informing the implementers) to ensure system's effectiveness.

Step 8: Resolution

This is the step where all actions are completed including follow-up with the proper departments and personnel. It is at this step that one needs to identify and track all open actions and pursue with the right people for their closure. These activities may involve seeking approval from higher management ranks to obtain priority for implementation procedures. It is also highly desirable and extremely motivating to give feed back to the employee who identified the NM and/or reported it. There are several action tracking software packages available on the market. We recommend using one of the commercial programs for this function if it is not already built into the NM management system.

Prioritization

In a well-designed Near-Miss management systems (NMMS) in financial institutions there would be two separate prioritization processes. The first is strategic prioritization (SP), the second is individual prioritization (IP). Since prioritizing activities are closely coupled with the structure of a NMMS, in this section we detail a process based on a NM structure proposed in the section that follows thereafter. In such a system, a Near-Miss Management Strategic Committee (NMMSC) (see section *Near-Miss Management Structure*) at the corporate level and/or a Near-Miss Management Council (NMMC) at the branch level are responsible for SP. These activities aim to provide guidance and set standard procedures for IP and would mainly consist of:

- Ranking the prioritization criteria and their attributes for various types of NMEs.
- Rating methods to be used for IP.
- Reviewing and revising the NM system prioritization including independently reclassifying a group of NMEs for further verification and/or modification of prioritization criteria.

There are several tools in the literature for SP, such as Analytical Hierarchy Process (AHP) (see Saaty [2001]), Comparison Risk Ranking (CRR) (see FitzGerald and FitzGerald [1990]), or Bootstrapping (see Kleindorfer et al. [1993]). AHP is a well-established and widely used process for complex decision making which enables inclusion of multi-layer attributes. CRR is used for simplistic but quick ranking of a small number of options. Bootstrapping makes use of past data and proves to be a good and viable tool for continuous improvement of the prioritization process. Since SP activities involve working with a finite number of options at any given time, we can also categorize these processes as “Batch Prioritizing.”

Prioritizing is closely related to classification of NMEs for which NMMSC establishes guidelines and procedures. In an efficient NM system the prioritization of a NM is done by the person filing the report at the time of reporting based on the guidelines and criteria set forth in principle by NMMSC. Since the classification of a NM and its priority are closely

linked, guidelines and procedures for both must be simple, clear and easily understandable by everyone in the organization (see examples in the appendix). IP can be considered as a “Continuous Prioritization” since each NM is prioritized individually on a regular basis. Continuous prioritization is not as thoroughly studied in the literature as batch prioritization. In the following, we present some continuous prioritization tools for consideration:

- “Worst-case Scenarios” require estimation of maximum but realistic damage that could have happened or can happen in the future if similar incidents take place again.
- “Repeating Events” require knowledge of past incidents and give higher priority on a sliding scale for similar events that occur multiple times.
- “Incident Reach” is a concept where higher priority is given to events that can reach several “Nodes” of a system rather than having only a local effect.
- “Screening” allows classifying NMes into two categories, high or low priority, by comparing each against a given criteria.
- “Sifting” is an extension of “Screening” where NMes are prioritized through a series of questions based on criteria set forth by the NMMSC.

If priorities are automatically associated with a corrective action for a given NM, then the departments who have responsibilities for these actions should be part of the group designing the prioritization system, such as the NMMSC.

Near-Miss Management Structure

There is no NMMS which is unilaterally accepted across industries. We propose the following system (presented in figure 4 below) based on discussions with industrial and academic institutions as well as the guidelines provided by the Basel Committee (see “Working Paper on the Regulatory Treatment of Operational Risk”, September 2001). This structural relationship applies to both business units and physical locations.

Near-Miss Management Strategic Committee (NMMSC)

The NMMSC is an integral part of the independent operational risk management function. This high level corporate group is established based on policies and procedures set by Board of Directors and Senior Management to provide oversight to the NM practice of the financial institution. Key functions of this committee are:

- Establishing guidelines for corporate and site NM structures.
- Developing criteria for classification of NMes.
- Establishing prioritizing procedures for each NM class.
- Auditing the NM system.
- Integrating quality and other management tools (see Phimister et al. [2001]) into NM management practice.
- Identifying gaps in the NMMS based on analysis of incidents with higher damage (beyond near-misses) and taking corrective actions.
- Developing guidelines for training site management and employees on NM system.

Near-Miss Management Council (NMMC)

Each branch has its own NMMC responsible for NMMS at that branch. These committees function independently but communicate with each other under the auspices of the NMMSC. Most business and operational functions such as trading and sales, retail banking, asset management, and information technology are represented in this committee at the decision maker's level who have resources and authority to follow-up on any required action. Some of the NMMC's key functions are:

- Adapt criteria set by NMMSC to the branch practices.
- Monitor site NM practices.
- Promote the program.
- Ensure availability of necessary resources for analysis and corrective action, especially for high priority NMes.

- Periodically analyze reported NMes for further improvement of the system.
- Train employees on NM implementation.

Managers (M), Supervisors (S) and Employees (E)

Managers, supervisors and employees are the main force behind a successful NM system. When trained properly they recognize operational issues before these issues become a major problem and cause any damage. Keeping this group motivated is an important function of the NMMC.

Insert Exhibit 4 here

System Review

In a well-established NM system, with people observing every little abnormality and reporting all potential issues as well as incidents, most NM reports will not be indicators of major (high severity) problems. However, paying attention not only to the high priority items but also to the other reported issues would help improving the system's productivity and operability.

NMes fit into the total quality management principles for operational risk as mentioned in Marshall [2001] and Hoffman [2002]. Each NM observation or incident may serve as a risk indicator or an event data point. These points individually and collectively must be analyzed for causes and corrective actions, the system changes must be implemented, and revised practices must be observed for new indicators. As such not only the potential for catastrophic events are reduced but also the system operations are improved.

CONCLUSIONS

This paper proposes to focus on high frequency low impact “Near-Miss” events to address key operational risk issues in financial institutions. The broad definition of the Near-Miss concept makes it indigenous to all operational issues in financial institutions and provides necessary flexibility to accommodate differences between various practices. Establishing a system that captures all current and potential problems regardless of their impact is important. Equally important is establishing effective prioritizing systems. Employees and administrators need clear guidelines to be able to recognize high priority events that are likely to cause major problems. Another critical step is identifying and implementing solutions to prevent accidents from flourishing. This requires management commitment and oversight.

The “Near-Miss” concept and the “Near-Miss Management System” explored in this paper are based on studies and practices in other industries and incorporate all those important processes. They not only satisfy the qualifying standards for *Advanced Measurement Approaches* put forward by the Basel Committee (see “Working Paper on the Regulatory Treatment of Operational Risk”, September 2001) but additionally provide guidelines on managing operational risk. We thus propose the “Near-Miss” concept as an *Advanced Management Approach* for operational risk to be implemented as a supervisory review process under Pillar Two. We also recommend removing operational risk from Pillar One (regulatory capital requirement) due to its idiosyncratic nature.

REFERENCES

American Institute for Chemical Engineers. "Guidelines for Investigating Chemical Process Incidents." Center for Chemical Process Safety, Publication No: G-19, 1992.

Barach P., and S.D. Small. "Clinical Review - Reporting and Preventing Medical Mishaps: Lessons from non-Medical Near-Miss Reporting systems." *British Medical Journal*, 320 (2000), pp. 759-763.

Basel Committee on Banking Supervision. "Consultative Document: The New Basel Capital Accord." Bank for International Settlements, 2001.

———. "Consultative Document: Operational Risk." Bank for International Settlements, 2001.

———. "Working Paper on the Regulatory Treatment of Operational Risk." Bank for International Settlements, 2001.

Bird, Jr., F.E. and G.L. Germain. *Practical Loss Control Leadership*. Det Norte Verias Inc., USA, 1996.

Caouette, J.B., E.I. Altman, and P. Narayanan. *Managing Credit Risk: The Next Great Financial Challenge*. Wiley Frontiers in Finance, John Wiley & Sons, Inc., Toronto, 1998.

Danielsson, J. "The Emperor has no Clothes: Limits to Risk Modelling." *Journal of Banking and Finance*, 26:7 (2002), pp. 1273-1296.

Diebold, F.X., T. Schuermann, and J.D. Stroughair. "Pitfalls and Opportunities in the Use of Extreme Value Theory in Risk Management." *The Journal of Risk Finance*, 1:2 (2000), pp. 30-36.

Embrechts, P., C. Klueppelberg, and T. Mikosch. *Modelling Extremal Events. Applications of Mathematics No. 36*, Springer, Berlin Heidelberg, 1997.

FitzGerald, J. and A.F. FitzGerald. *Designing Controls into Computerized Systems*. Redwood City, CA: FitzGerald, Jerry and Associates, 1990.

Herring, R.J. "Credit Risk and Financial Instability." *Oxford Review of Economic Policy*, 15:3 (1999), pp. 63-79.

Hoffman, D.G. *Managing Operational Risk: 20 Firmwide Best Practice Strategies*. Wiley Frontiers in Finance, John Wiley & Sons, Inc., New York, 2002.

Jones, S., C. Kirchsteiger, and W. Bjerke. "The Importance of Near Miss Reporting to Further Improve Safety Performance." *Journal of Loss Prevention in the Process Industries*, 12 (1999), pp 59-67.

Kleindorfer, P., H.C. Kunreuther, and P.J.H. Schoemaker. *Decision Sciences: An Integrative Perspective*. Cambridge University Press, New York, 1993.

Marshall, C. *Measuring and Managing Operational Risk in Financial Institutions: Tools, Techniques and Other Resources*. Wiley Frontiers in Finance, John Wiley & Sons, Inc., Singapore, 2001.

National Academies of Engineering. "Cross-Industry Analysis of Catastrophic Precursors." Roundtable, Washington, D.C., 2002. <http://www.nae.edu/precursors>

Phimister, J.R., U. Oktem, P. Kleindorfer, and H. Kunreuther. "Near-Miss Management Systems in the Chemical Process Industry." Working Paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, 2001.

———. “Statistical, Analytical and Management tools for Near-Miss Programs.” Working Paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, 2001.

Saaty, T.L. Decision Making for Leaders. Pittsburgh, PA: RWS Publications, 2001, 3rd edition.

APPENDIX

Identifying operational risk categories and classifications within each category strongly depends on the financial institution’s range of activities. In the table below, we provide some examples of categories, classifications, priorities and distribution targets to clarify some of the concepts mentioned in the article.

Insert Exhibit 5 here

EXHIBIT 1
Frequency-Severity-Matrix

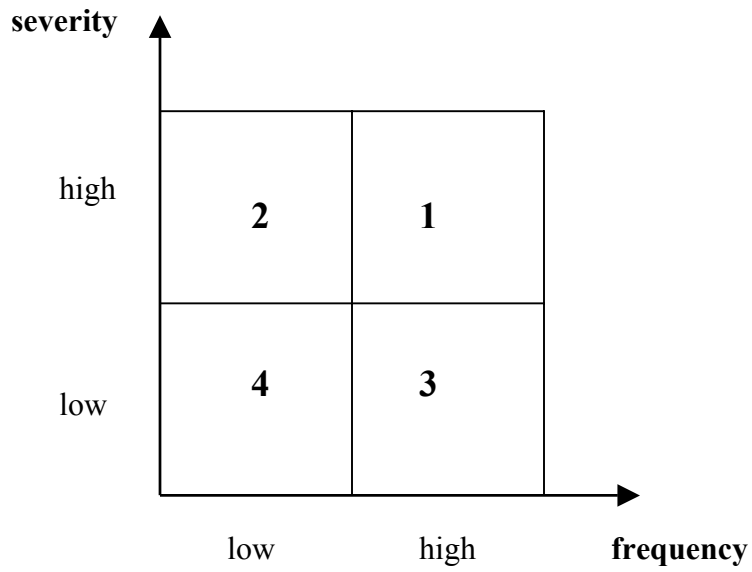


EXHIBIT 2
Extreme Value Distribution

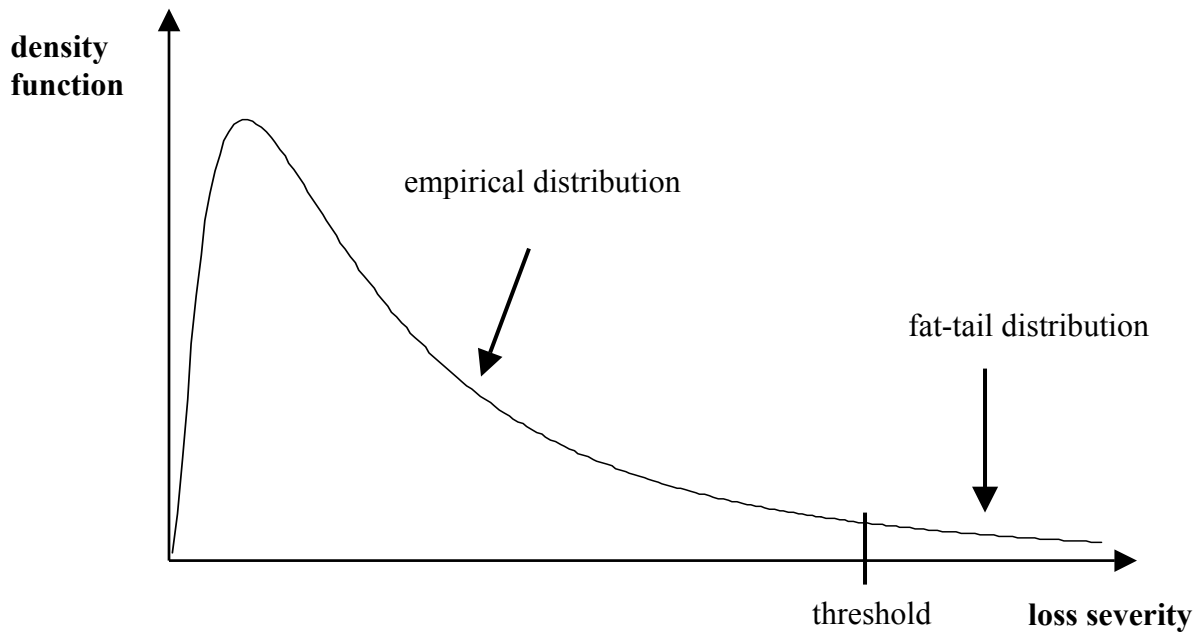


EXHIBIT 3
Safety Pyramid with 1969 US Ratio Study

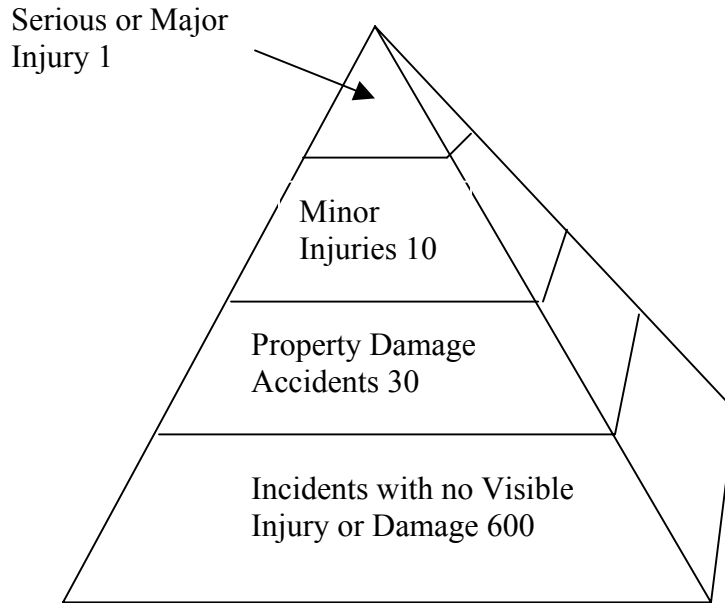
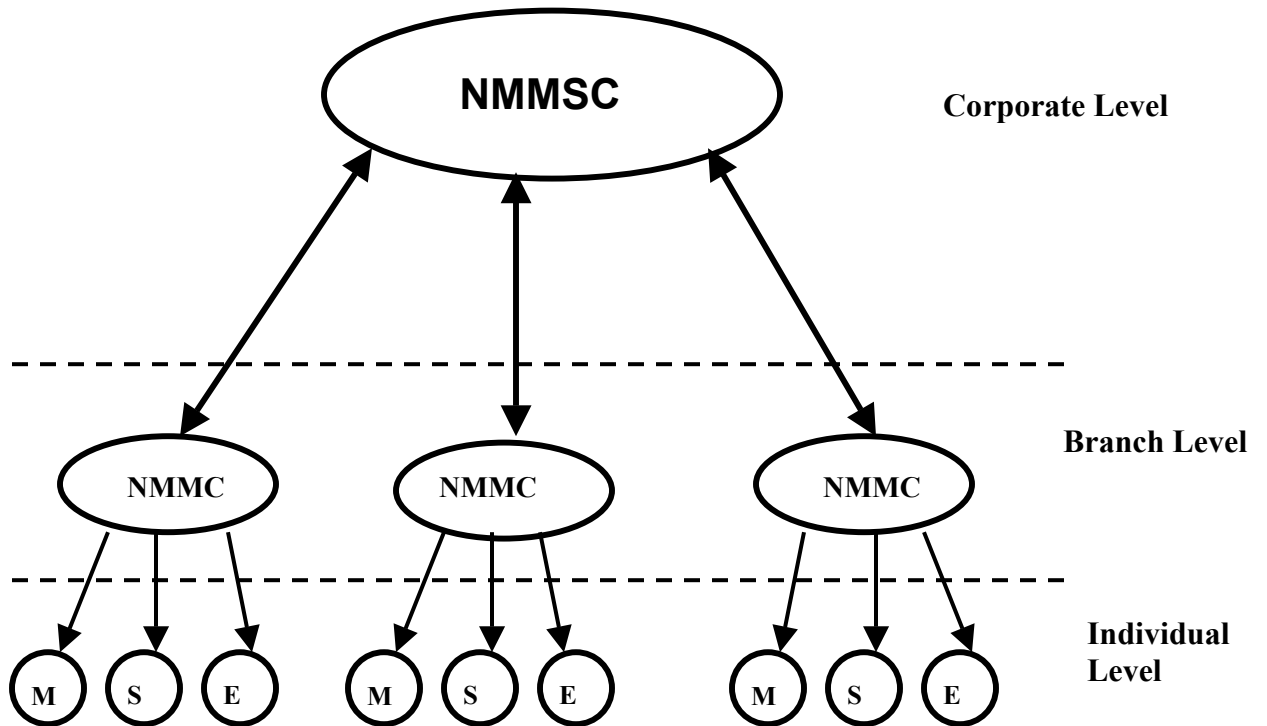


EXHIBIT 4
Near-Miss Management Structure



**EXHIBIT 5
Priority/Classification Matrix and Its Relation to the Distribution System**

Category	Class	Attributes Level 1	Attributes Level 2	Priority	Primary Recipient	
Employment Practices/ Workplace Safety	Personal Injury (Physical/Mental)	Physical Problems Including Human/Machine Interface	Lifting Heavy Loads	Medium	Safety Manager	
			Repetitive Motion Problems	High		
			Bad Furniture Layout	Low		
	Physical Environment		Poor Air Quality	Medium	Maintenance Manager	
			Extreme Temperatures	Low		
			Asbestos	High		
				Medium		
	Rogue Trading	Transaction Irregularity	Safety Behavior	High	Safety Manager	
			Discrimination	High		
			Transaction Not Reported	High		
Business Disruption and System Failures	Abnormal Profits or Losses		Position Mismarked	Medium	Human Resources Manager	
			Transaction Unauthorized	High		
			Realized Losses (Gross/Net)	Medium		
	IT	Hardware		Potential Losses	High	Quantitative Risk Manager
				Failures	High	
				Speed	Low	
				Brand Variation	Low	
	Communication	Telecommunication		Graphic User Interface	Medium	IT Manager/MIS Manager
				Program Design	High	
				Program Limitation	Low	
Phone				Medium		
Internet Connection				Medium		
Utility	Outage Insufficient Level		Wireless	Low	Facility Manager	
			Distribution Frequency	Low		
			Pick-Up Location and Time	Low		
				Low		
				Low		