BBR
BRAZILIAN BUSINESS REVIEW
Vol. 6, No.2
Vitória-ES, May – Aug 2009
p. 165-180 *ISSN 1808-2386* *DOI: http://dx.doi.org/10.15728/bbr.2009.6.2.4*

High Reliability Organizations and Operational Risk Management

Janann Joslin Medeiros[†]
University of Brasília

Wellington Pinto[Ω]
Faculty of Environment and Technology Business – FAMATEC

ABSTRACT: Studies on the management of operational risk in financial organizations have predominantly utilized quantitative and probabilistic approaches. Such approaches provide managers with a way to estimate the probability of operational failure occurring but do not provide insights with regard to specific managerial actions that can be taken to avoid the occurrence of such failure. Results of our study of the processes of a large Brazilian banking institution suggest that HRO theories can make an important contribution to the effective management of operational risk. Understanding the underlying causal mechanisms that contribute to operational failures makes it possible to take steps to manage them and to reduce the probability that they will occur. In addition to suggesting a new approach to the management of operational risk in financial institutions, the study tested HRO theory in a new sector. The results clearly demonstrate that HRO concepts are relevant in financial institutions, broadening the scope of applicability of this theory.

Keywords: high reliability organizations; operational risk management; financial institutions.

Received in 09/16/2008; revised in 04/08/2209; accept in 08/05/2009.

Corresponding authors*:

[†] *Professor at the University of Brasilia*
Address: ICC Norte, Módulo 25 subsolo Veiga, Brasília- DF – Brazil - CEP: 70910-900,
e-mail: janann@unb.br
Telephone: (61) 3307-2545

Ω *Coordinate the School of Environment and Technology Business*
Address: SQN 404, BLOCO N, Brasília – DF – Brazil - CEP: 70845-140,
e-mail: wellington.pinto@caixa.gov.br
Telephone: (61)3222-7308

Editor's note: *This paper was accepted by Antonio Lopo Martinez*

1. INTRODUCTION

The Basel Committee on Banking Supervision was created with the mission of establishing patterns of operations for the minimization of risks and the provision of greater stability to the global financial system. In 1988 this Committee published the International Convergence of Capital Measurement and Capital Standards (BIS,1988), containing a set of guidelines for minimizing the risks of financial organizations and guaranteeing that they have minimum levels of solvency and liquidity, establishing secure limits for operations, and creating uniform standards. After the publication of these standards and the adoption of the preventive measures contained in the document, however, cases involving risk problems occurred in financial institutions, foremost among them being the Barings Bank case. This traditional English financial institution failed due to the loss of £869 million from operations carried out by one employee.

This case revealed that Barings Bank had deficiencies in its internal processes, flaws in its internal controls and lacked mechanisms to protect against internal fraud, situations not contemplated in the 1988 document. As a consequence, the bank was unable to detect and correct these problems in time to prevent disastrous consequences for its patrimony (REASON, 1997). The Barings case, unfortunately, was not an isolated one. Marshall (2001) presents various other examples of large-scale financial losses resulting from fraud and flawed internal processes.

Upon analyzing these kinds of problems, the Basel Committee perceived that it was necessary to deal specifically with the risk factors which generate them: human failure, systems failures and process failures, frauds and external events. These factors were defined as operational risk and in 2004, a new International Convergence, or Basel II (BIS, 2004) was adopted which contemplated, among other measures, requiring financial institutions to manage operational risk as a form of protection against unexpected losses in their business processes and achievement of greater effectiveness in their operations

Financial institutions began, then, to adopt measures to comply with future demands. These measures, to date, are limited to studies of the probability of operational losses carried out by means of quantitative techniques with the objective of determining how much capital should be allocated to cover potential operational losses. There has been no use of studies or techniques for evaluating how the organization conducts its operations as a way of identifying preventive or corrective actions for potential operational weaknesses.

A review of the literature on operational risk reveals no academic discussion or scientific reflections of an empirical nature. Rather, the bibliography on the matter consists predominantly of prescriptive methods, techniques and models for use by organizations. There is, however, a body of literature in the field of organization studies which seeks the prevention and timely correction of operational shortcomings, that of High Reliability Organizations (HROs).

Reliability is generally understood to mean fault-free performance in spite of exposure to adverse conditions. HROs are organizations which--despite characteristics such as complex processes, strong interdependence with other organizations or among units of the same organization, the use of sophisticated technologies, the need to act under constant pressure and in environments subject to high risk of accidents of catastrophic dimension—have experienced few cases of negative occurrences and possess consistent strategies for mitigating operational failures if they should occur (Reason, 2000). In other words, although they function in high-risk environments and carry out operations of great complexity, HROs have superior operational performance, with an incidence of error approaching zero.

Studies on HROs began with the research on normal accidents conducted by Perrow in the 1980s with respect to complex processes involving risky technologies (FORD et al., 2003). Perrow (1999) affirms that accidents permeate organizations as a result of tight coupling, lack of control and operational complexity. Tight coupling is understood to mean the impossibility of delaying or postponing process operations, invariable process sequencing and single paths for reaching objectives, little flexibility in supplies, equipment and personnel, and little time to correct such failures as perchance may occur. Lack of control relates to the absence of contingency plans in case failures should occur; while complex operations are characterized by multiple interconnections among component parts, units or subsystems, non-existent or non-thought out feedback routines, a variety of parameters for control of potential interactions, indirect or inferential sources of information, and limited comprehension of some processes (PERROW, 1999, p. 85-86). .

Perrow (1999) observes that there is no such thing as a perfect human or mechanical component. For this reason, as Reason (1997) ponders, complex systems have need of safety devices such as redundant or layered controls. However, complex and tightly coupled processes have their redundant safety mechanisms linked to each other. This can reduce their reliability instead of increasing it, principally by making these mechanisms and their inter-workings more complex (SAGAN, 2004). In addition, the adoption of redundancy in safety mechanisms frequently leads managers to place even more pressure on production processes because they deposit unwarranted confidence in the safety offered and because they seek increased results to compensate for the investment made in these mechanisms (SAGAN, 2004

Perrow's research stimulated investigation of how some organizations manage to maintain high patterns of operational security in spite of the complexity and tight coupling of their processes. Initial research to identify organizations that belong to this group and analyze how they structured and managed their operations to attain levels of error near zero was carried out with the U.S. Navy (ROBERTS; LIBUSER, 1993). These studies underlined the importance of learning about organizations which operate under adverse conditions but have a lower than expected number of accidents (FORD et al., 2003; ROBERTS; LIBUSER, 1993).

The present study investigates the relationship between the characteristics of High Reliability Organizations and the requirements for operational risk management in financial institutions outlined by the Basel Committee. Its objective is to identify, from this organization studies perspective, what might be the probable causes of operational failures experienced by a large financial institution and evaluate whether theories about high reliability have a contribution to make to the effective management of operational risk. To study these questions, two processes in which operational failure has been experienced were studied in a large Brazilian financial institution called, for purposes of this study, the Zeta Bank.

Perrow (1999) observed that, in spite of the fact that no studies have been carried out in the sector, the financial system is an obvious field for carrying out studies on organizational accidents, given the high volume, the complexity and tight coupling of operations and financial instruments; and the HRO literature suggests the applicability of their concepts in the banking sector. (See, for example, Roberts and Rousseau, 1989; Reason, 1998; and Vogus, 2003.) However, no previous empirical studies have specifically investigated this possible applicability.

This study investigates the applicability of the concepts of high reliability to the management of operational risk by financial institutions.

2. HIGH RISK AND HIGH RELIABILITY

According to the literature, HROs exhibit characteristics that expose their operations to high risk of failures, together with characteristics that promote high reliability as a form of preventing or softening the impact of disastrous occurrences.

Roberts and Rousseau (1989) identify the following characteristics of high risk:

- hyper complexity: a great variety of components, system and levels.
- tight coupling: interdependence among units and levels which does not permit waits or delays between one activity and another or variations in the sequencing of procedures.
- short intervals between activities**:** normally the principal activities occur in intervals measured in seconds;
- simultaneous occurrence of critical operations**:** occurrence of several complex operations at the same time, with no possibility of interrupting any of them (takeoffs and landings in airports, for example).

Bea and Moore (1993) state that organizational reliability is frequently undermined by over-ambitious production goals that cause operators to disregard security procedures. Reliability, according to these authors, is also compromised when top management, under cost pressures, does not provide necessary resources for the promotion of operational security. As a result, accidents occur due to a combination of human fault (imprudence, lack of attention), system failure (lack of preventive mechanisms or mechanisms for alert, detection and control) and organizational failure (inadequate supervision, deficient training).

Although they exhibit high-risk characteristics, HROs have other characteristics that reduce the probability of the occurrence of large-scale failures, differentiating them from other types of organization. According to Rochlin (1993), these characteristics are:

- the belief that mistakes can occur anywhere and that constant vigilance is the price of success;
- monitoring mechanisms are constantly renovated and reanalyzed, given the fact that the sources of error are dynamic;
- the belief that the operational environment is a constant source of threat and requires permanent vigilance;
- maintenance of redundant ways of solving problems at the operational level and resistance to pressures to streamline processes;
- creation, maintenance and use of organizational contingency solutions;
- organizational commitment to the use of preventive measures as well as reactive ones for confronting real and potential problems;
- training and providing organizational units involved in the process with autonomy to seek out and prepare for real problems as well as look for latent weak points in organizational processes which, upon interaction with certain kinds of conditions, can cause organizational losses;
- reluctance to test the limits of reliability;
- obedience to formal rules and codes of conduct.

The top managers of HROs consider safety as important as productivity and concentrate part of their efforts on the reduction of potential risks (GRABOWSKI; ROBERTS, 1997; LALLY, 2002; ROBERTS; LIBUSER, 1993). The most important characteristic of an HRO is the collective concern with the possibility of error. Top management believes that mistakes will always happen and trains their workforce to recognize them and be prepared for them. (REASON, 2000)

Weick and Sutcliffe (2001) characterize HROs as being in a state of constant alert for unexpected events that can cause negative impacts on their routines. This state is achieved by:

- constant concern for error, constant analysis of any and all kinds of mistake and treatment of any carelessness as a symptom that something is not going right;
- reluctance to simplify routines, seen in the attempt to understand each phase of the complex activities and maintain the phases separate in order to permit immediate management if problems occur;
- sensitivity to operational procedures, intended to constantly evaluate operational processes, in order to identify factors with the potential to cause error;
- commitment to operational functioning, through the establishment of contingency plans for maintenance of operations and based on the premise that there is no system or procedure which always works perfectly;
- respect and consideration for highly qualified professionals**,** evidenced by encouragement of the taking of decisions for problem solution by specialists in the matter, independently of their place in the hierarchy.

For Weick and Sutcliffe (2001), the first three of these characteristics create a state of alertness and concern for the unexpected while the last two promote conditions for containing such events when they occur. In short, they attribute the success of HROs to constant efforts by members to act effectively in the face of unexpected events. They believe that HROs are organized in such a way that operators are able to recognize and evaluate such events, braking their evolution or reestablishing operational functioning, if necessary. What differentiates HROs from other organizations is not the prevention of the unexpected but the ability to act immediately, in the initial stages of an unexpected occurrence, when there is only a hint that something might be wrong.

Organizational culture can be defined as the shared beliefs and values that interact with organizational structures and control systems to produce behavioral norms (REASON, 1997:192). An organizational culture oriented toward high reliability contains certain fundamental elements (REASON, 1997; WEICK; SUTCLIFFE, 2001):

- behaviors that seek to direct activities toward maximizing safety, irrespective of business pressures;
- the maintenance of high and constant levels of concern with operational weaknesses;
- support for the collection and study of data about accidents and situations where losses have almost taken place, even in the absence of large-scale failures;
- maintenance, incentive for and dissemination of mechanisms for communication of individual errors;
- definition of the administrative measures to be adopted in case non-acceptable behaviors occur. These are made clear to all members of the organization;
- procedures for adapting to a variety of crisis situations, with flexibilization of structure and of the decision-making process;
- ways of bringing all information to bear in reaching conclusions about the best way to implement operational safety.

As shown in Table 1, a review of the respective literatures suggests that many of the conditions identified in the HRO literature as contributing to accidents are similar or identical to the causes of exposure to operational risk identified in the operational risk literature.

Causes of operational risk identified in the operational risk literature	Conditions which contribute to accidents identified in the HRO literature
Human failure	Human factor: lack of attention, forgetfulness, poor motivation, carelessness, lack of skill or knowledge, negligence (REASON, 1997)
Human and system failure	Technical factor: relationship between people and technology (REASON, 1997)
Process failure	Organization factor: inadequate processes or budgets; conflicts of interest; insufficient or non-existent training (REASON, 1997)
System failure	Technological innovations (LALLY, 2002)

Table 1 - Comparison of the Causes of Risk Situations

A fundamental conceptual difference between the two literatures is perceptible, however. The HRO literature treats human, technical and organizational failures as *consequences* of "organizational posture", of how the organization deals with the various risk factors. In the case of the operational risk literature, human and technical errors are considered the *causes* of risk in and of themselves. Focus is on projecting the probability that they might occur rather than on taking measures to avoid their occurrence.

3. METHODS

Based on the premises about organizational reliability proposed by Weick and Sutcliffe (2001) and Roberts and Libuser (1993), a conceptual model for analysis was developed consisting of five variables along three dimensions: environment (organizational climate and culture and working conditions); people (attitudes and competence); and processes.

Two organizational processes of the Zeta Bank: management of the Brazilian System of Payments (SBP) and management of Credit Operations were studied with a view toward identifying possible causes of exposure to operational risk as defined by BIS (2004): human failure, process failure, system failure, human fraud or external event.

These specific processes were selected on the basis of the volume of resources involved and the number of daily transactions carried out, as well as the availability of data and the possibility of maintaining confidentiality with respect to the identity of the organization.

To evaluate the exposure to risk offered by the variable "organizational climate and culture", the indicator used was "existence of reward or punishment related to error". In addition, indications of evidence of the presence of characteristics of a high reliability culture were sought. For investigating the variable "working conditions", two indicators were used: existence of pressures and adequacy of resources. To evaluate "attitudes," four indicators were used: perception, responsibility, proactivity and reactivity. The indicators used to evaluate the risks posed by "competence" were learning, training and knowledge. Based on Roberts and Rousseau (1989), Rochlin (1993) and Bea and Moore (1993), as discussed in the previous section, six indicators were used to evaluate the exposure to risk offered by processes: tight coupling, complexity, constant human action, ability to return to normal functioning, occurrence of unexpected events and suppression of safety routines.

Research was carried out by means of the application of a questionnaire, non-participant observation, and documentary research. Topic outlines, developed from the concepts used in the analytic model, were used to guide non-participant observation and the documentary research. Documentary research was used to collect data with respect to losses and operational failures and to map the processes being analyzed. Documents reviewed were internal documents of Zeta Bank that dealt with bank processes in which operational losses

had been experienced. Respondents to the questionnaire were employees of the Zeta Bank involved with the two processes chosen for closer study: seven who work with management of the SBP and twelve involved with management of credit operations. Non-participant observation was carried out over the course of the research project to provide a means of verifying information about processes contained in the documents reviewed and perceptions of operators obtained by means of questionnaire. In addition, in view of certain points of view expressed in responses to the questionnaire, an interview was conducted with the manager of the Technology Unit in order to understand how these issues appeared from his perspective.
For analysis of the data, flowcharts were developed of the processes studied. In addition, the technique of pattern matching was used in analyzing the data, in which comparisons were made between the patterns of the variables observed empirically and the patterns expected on the basis of the theoretical framework used (YIN, 2001).

4. RESULTS

In this section, we present the findings on the processes selected for analysis at Zeta Bank - management of the SBP and management of Credit Operations.

Management of the Brazilian System of Payments (SBP) Process . The implantation of a new Brazilian Payment System (SBP) took place in April of 2002. The principal objective of the new system was to make transfer of resources between the clients and users of different banks more agile and safe. The most striking change brought about by the SBP was the introduction of an instrument called Available Electronic Transfer (TED, from its initials in Portuguese), utilized to effect on-line transfer of resources between banks. The system thus functions as though the client has made a cash deposit directly in the account of another client, who thus has the money immediately available.
The new system lessened the time during which money involved in the transactions was blocked and diminished the credit risks assumed by business firms, given the fact that, unlike checks, which can be held or returned for lack of funds, TEDs are irreversible.
The objective of the SBP was the improvement of the security of the financial system as a whole. In the previous system, bank accounts were only updated every 24 hours and, in the case of the failure of a financial institution, it was impossible to undo all the operations that it had carried out without jeopardizing the solvency of other financial institutions. The Brazilian Central Bank, or rather, the Brazilian taxpayers, had to absorb the costs of such bank failures.
Under the new system, payments are made individually, as they happen, and only if the bank on which the transfer is drawn has sufficient funds to cover the amount. In this way, if a bank does not have resources available to honor its commitments, it must stop operating at that exact moment and thus will not generate further risks to other banks, to the Central Bank, to investors or to society.

Operational risks. In the first weeks of functioning of the SBP, a client transferred R$11.071.333.34 from Zeta Bank to another bank, but the communication link with the Central Bank system was down. This created a backlog of messages to be sent by means of the back-up system near the closing time established by the regulatory agency, generating pressures to meet the statutory deadline. The contingency procedure requires that a bank employee using one system manually enter the amount of the transfer and an employee using a different system liberate this amount.

In the liberation of the amount to be transferred, the first system provided all the information with respect to the operation, including the amount. This system, however, does not record the period that separates cents from *reais* (the Brazilian currency). The second system differs from the first in that it requires that a period be placed before the cents. If this is not done, the system interprets all digits as *reais*.

The first employee typed in the correct amount but, in accordance with system requirements, did not type in a period before the cents. At the moment of confirmation of this value, given the proximity of the deadline and the importance of the amount and of the client, the second employee checked the amount on his computer screen and telephoned the unit that had requested the transfer before confirming the operation. Confirming that the amount typed in (R$ 110713334) corresponded to the amount of R$ 1107133,34 requested, the second employee pressed the *enter* key, upon which the system automatically added 00 to the amount typed in, transforming R$ 11,071,333.34 into R$ 1,107,133,334.00. This created a negative balance in the Central Bank account of R$ 364,573,906.78 (three hundred sixty-four million, five hundred seventy-three thousand, nine hundred and six *reais* and seventy-eight cents).

The team which monitors the account balance with the Central Bank detected the mistake but the Central Bank system had already closed. The only alternative was to request that the receiving bank return the transfer the next day. This took place after being authorized by the party receiving the transfer but generated the payment of charges to the Central Bank for the "loan", in the amount of R$ 427.078,86 (four hundred twenty-seven thousand and seventy-eight *reais* and eighty-six cents).

Several factors identified in the HRO literature as potential promoters of organizational accidents can be observed in this case: new systems; pressure to meet deadlines; human-system interaction; inadequate training; tight coupling; system failure; failure of defensive procedures.

Environment. The deadline established by the Central Bank for concluding the day's operations is the principal negative element reported for this process by respondents to the questionnaire. This deadline pressure becomes worrisome, however, only when there is a problem with the functioning of the systems for sending and receiving messages or when confirmation of messages is pending due to registration problems within the bank.

Given the fact that the process is predominantly automated, it cannot be inferred that the environment, as a general rule, poses high risk for the organization with respect to this process. The situation changes, however, when system failure causes utilization of contingency procedures and these contingency procedures involve manual manipulations—a situation of risk pointed out by Bea and Moore (1993), Perrow (1999), Reason (1997), and Weick and Sutcliffe (2001).

With respect to organizational climate and culture, it was reported that neither rewards nor punishments have taken place with respect to operational errors in the SBP process and that procedures are in place for dealing with errors and failures that permit free expression of opinions. Nonetheless, examples cited dealt exclusively with reporting the incident to the responsible unit or to a hierarchical superior. Non-participant observation revealed that while employees speak openly about operational errors caused by or occurring in other units of the organization, they are extremely reluctant to comment about those that have occurred in their own units. This suggests an organizational climate little propitious to dealing openly with questions of operational security. Characteristics of a high reliability culture postulated by Reason (1997)--such as a systematic way of locating and disseminating active failures or latent weaknesses or the existence of clear administrative measures to be adopted in case of non-acceptable behaviors—were not observed. The data collected and analyzed offer no

evidence that the kinds of behaviors, beliefs or values are present which would form an organizational culture of high reliability in the terms of Grabowski & Roberts (1997) and Reason (1997), or that behaviors exist to direct activities toward a maximum of security, independent of business pressures.

People. This factor was investigated in terms of level of awareness of the potential for threats to operational security, feelings of responsibility for the security of operations, proactivity with respect to operational weaknesses, and reactivity (ability to react appropriately to threats when identified).

HROs can be characterized, among other things, by obedience to formal rules and codes of conduct and by the belief that the working environment is a constant source of threat (ROCHLIN, 1993). Participants in the process demonstrate *awareness* of the fact that the organization is subject to unexpected events that have the potential for causing operational losses, but they do not evince the belief that people always correctly follow established norms and routines.

Although the SBP process is seen as susceptible to unexpected events, employees do not perceive their specific organizational unit or themselves as having responsibility for operational security, invariably transferring this responsibility to other units of the organization, most specifically to the Technology Unit. This denotes a lack of personal commitment to operational security. Such commitment and the assumption of personal responsibility exist in HROs (WEICK; STUCLIFFE, 2001; ROCHLIN, 1993).

With respect to the responsibility of the Technology Unit for failures in the process, alleged by those involved in the SBP process, the manager in charge of the Technology Unit stated that there are almost 500 systems functioning in Zeta Bank. Some are quite old and slow, but their use is demanded by the business units of the bank. Among the managerial responsibilities of the business units is budgeting for improvement in bank routines. When managers are requested to collaborate in measures intended to improve system performance, rationalization of databases, redesign of processes—in other words, activities that are not directly related to the mission of their own units--they resist and give preference to the needs of their business. Thus, from the perspective of this manager, the Technology Unit has no recourse but to seek the correction of failures in an unplanned way after they happen. The problem, therefore, is not with the Technology Unit but with the business units. He, like the operators of the SBP process, assumes no responsibility for the situation. It can, therefore, be inferred that, in addition to the absence of an important element of high reliability culture—the assumption of personal responsibility for operational security--there is a fragmented and reactive way of dealing with operational weaknesses within Zeta Bank as a whole.

Proactive attitudes with respect to operational security involve search for primary and latent errors, constant vigilance of the working environment (ROCHLIN, 1993); training and simulations related to possible accidents (ROBERTS, 1990); and constant evaluation of operational processes to identify potential sources of operational problems (WEICK; SUTCLIFFE, 2001). No such proactive attitudes were identified with respect to the operational security of the SBP process. Here again no presence of a high reliability organizational culture was detected: no maintenance of high and constant levels of concern with operational fragilities even in the absence of large-scale failures, or of activities for collecting and studying information about incidents, individual accidents and situations where loss *almost* occurred, as postulated by Reason (1997).

The only "high reliability" behavior reported by employees is that of reactivity. Operational problems, when identified, are immediately dealt with and transformed into improvements in operational routines. According to Reason (1997), one mechanism of

organizational defense is the creation of understanding and concern about where risk occurs. He suggests that the best way to increase operational security is to manage and improve organizational processes instead of merely exercising direct control over them.

Two aspects of the variable "attitudes" are apparent: their strong reactive character and weak proactive nature. The absence of proactivity, as Rochlin (1993) points out, can result in future losses, given the fact that the sources of error are dynamic. Protecting against the last failure does not protect against the next one.

The evidence suggests that in the SBP process there is a high degree of installed learning, knowledge and skill among operators; but important characteristics of the organizational culture of high reliability described by Reason (1997) are missing: knowledge about potential problems and attitude of responsibility for operational security.

Processes. Considering the principal aspects of high risk mentioned by Perrow (1999)—complexity, tight coupling and inadequate controls—and the high risk conditions pointed out by Rochlin (1993), Weick;Sutcliffe (2001), and Roberts; Rousseau (1989), the SBP process cannot be characterized as presenting high risk conditions. The process requires little human action. It presents a low frequency of unexpected events, decisions taken in the operational environment, or operations carried out by specialists. An alternative form exists for carrying out activities in case there are problems with system functioning, as do defensive control mechanisms. However, both documentary research and non-participant observation provided evidence of pressures related to meeting deadlines and human-system interaction.
Even in the absence of high risk conditions inherent in the process itself, human failure, system failure and organization failure together led to the large-scale negative results reported in this case, corroborating Bea and Moore's (1993) and Reason's (1997) predictions about such situations.

Management of the Credit Operations Process. In general terms, a credit operation consists in liberating the bank's financial resources to a borrower on the basis of specific norms and procedures for each type of product. In order for the transaction to be carried out, certain steps must occur to guarantee conformance to standards, including control and other management procedures. The principal stages of the process are: client analysis, concession, maintenance and recovery of credit. In the client analysis stage, there is registration of client information and evaluation of client risk using prescribed methods. In the concession stage, the loan contract is formalized and the resources are liberated. During the maintenance stage, controls exist for receiving the amounts owed, including charges due for late payment, and for wrapping up the operation. In the recovery stage, administrative or judicial procedures are adopted for recovering past-due amounts.

In Zeta Bank, credit operations involve various organizational units that are responsible for specific stages of the process and have differing objectives, as described below.

- Credit Management – development, implementation and standardization of credit products. Objective: to provide the institution with credit products appropriate for the market.
- Branch Management – customer service and formalization of the credit operation. Objective: to sell products and meet sales goals
- Credit Risk – evaluation of the risk presented by borrowers. Objective: to manage and operationalize credit risk policies.
- Credit Recovery – administrative actions to recover past-due amounts. Objective: to manage and recover amounts owed.

- Legal - legal action with respect to amounts not recovered through administrative means. Objective: business support.

Operational losses. The recovery of past-due credit depends on the existence of accurate registers of client information—name, address and telephone, for example—so that contacts to initiate debt negotiation can be made. In addition, correct formalization of the contract is essential (the contract itself, signature, promissory note) to provide a basis for taking legal action to recover what was lent or, when applicable, contractual guarantees.
Zeta Bank has opened 400 thousand actions for recovery of past-due accounts, totaling nearly 500 million *reais*, even when adjustments to the current values of past loans are not made. These are loan contracts that were granted at least two years ago and for which no repayment has been received for more than 360 days. The database of client information, which contains information registered at the time the contract was signed (name, address, telephones and e-mail), permitted recovery of information with respect to only 100 thousand of these contracts. Even so, in only 25,000 files (6.25% of past-due accounts) was this information correct and up-to-date, permitting contact with the debtor. Inaccuracies were found in the client information of approximately 70% of accounts past due for 35 days or less, promising future problems of a similar nature.

This process, taken as a whole, exposes the institution to unexpected events which cause financial losses and for which it is difficult to take remedial action. This is due at least in part to the fact that there has been no determination on the part of top management that such occurrences be eliminated, contributing to the absence of an organizational culture of high reliability.

The losses described can be seen to result from weaknesses discussed in the HRO literature: absence of layered defenses; non-compliance with operating standards and routines; human-system interaction; pressures; tight coupling of stages of the process; incompatibilities among the objectives of the units involved; latent risk conditions; and absence of a high reliability organizational culture.

Environment, people and processes. The working conditions for the Credit Operations process pose potential sources of high risk given the pressure to meet sales objectives and deadlines and the conflicting objectives of the various units involved in the process, one of the concerns of Weick and Sutcliffe (2001) and the lack of orientation to observe a maximum of security, independent of business pressures (REASON, 1997).

There was little consensus in the answers received with respect to liberty to talk about operational failures. Non-participant observation, however, evidenced that the topic is not dealt with openly by employees, as was also observed with the SBP process. At the same time, the human, financial and technological resources available to the process were observed to be adequate.

While employees accurately perceive the susceptibility of the process to unexpected events, it was observed that they do not always act in the safest way. As was also the case in the SBP process, employees do not feel personally responsible for the security of operations, placing the blame elsewhere for the failures that occur. A favorite scapegoat, once again, is the Technology Unit. The manager of that unit reported that there are 32 systems related to the credit process, each one responding to the needs of a specific manager, with its own databases, which does not permit an integrated view of the entire process.

There was no evidence of proactive behaviors with respect to organizational weaknesses and faults. Furthermore, there was no evidence that learning is taking place in the Credit Operations process. Operational flaws are not used as a way of improving the security

of routines, recommended by Weick and Sutcliffe (2001) as a means of building high reliability. In addition, the element of reactivity is absent in this process, evidenced by the fact that although performance weaknesses have been identified, no steps have been taken to correct these weaknesses. Respondents report conflict among organizational units as the cause of some delays in administrative decisions and in the updating of routines and products, as well as slowness in the management process, especially in terms of information.

While training and knowledge about operational functioning exist, there is little installed knowledge about or concern for factors that might cause problems with operational security. This is consistent with the previously reported absence of proactivity on the part of the operators of this process and also with absence of the characteristics of a high reliability culture.

High risk conditions as outlined by Perrow (1999) are present in the Credit Operations process in the form of tight coupling, great complexity (a large number of interfaces between organizational units and systems) and constant human-system interactions.

Analysis of the flowchart of operations developed from data collected for the study permits the characterization of the credit operations process as one of hyper-complexity, in the terms of Roberts and Rousseau (1989): it involves a great variety of components, systems and levels and each operational unit has its own objectives, procedures, standards, routines, training and command hierarchy.

From the flowchart, it is also apparent that there are no layers of defense and that decisions are highly centralized. In addition, documentary research revealed a large number of human errors and that there is no single unit or person with direct supervision over the process as a whole. Furthermore, the noncompliance with standards and routines evidences lack of obedience to formal rules and codes of conduct, contrasting negatively with the characteristics of high reliability suggested by Rochlin (1993).

The evidence suggests that the management of the Credit Operations process presents high-risk characteristics discussed in the HRO literature and that these are probable causes of the large-scale operational losses identified.

5. DISCUSSION

In this study we investigated from the perspective of studies on High Reliability Organizations what might be the causes of operational failures experienced by a large financial institution and whether the HRO literature might offer possible solutions for any operational weaknesses identified.

Findings show that the two processes investigated differ in key respects. For example, the SBP process is not characterized by high-risk conditions. Nonetheless, the evidence clearly demonstrates that reliability in this process was compromised by a combination of human error (lack of attention, lack of knowledge), system failure (absence of preventive mechanisms for detection, alert and control), and organizational failure (inadequate supervision, deficient training), resulting in a large-scale operational loss. No high reliability culture is in place that might serve as the basis for foreseeing future problems or for mitigating them should they occur.

In the case of the Credit Operations process, high-risk conditions are present, in terms of hyper-complexity, constant human-system interaction, tight coupling between stages of the process and inadequate control of the activities carried out. Reliability is also compromised by non-compliance with operating standards and routines. Even though operational weaknesses have been identified, no actions have been taken to counteract them. Taking such

actions is difficult in the absence of a high reliability culture and the presence of divergent and parochial interests.

None of the findings of the study is discrepant with the findings of previous HRO studies. On the contrary, results are in accordance with previous findings and provide evidence from a kind of organization not previously studied empirically—a financial institution—with respect to the following:

- pressures related to task compliance can lead to the suppression of security procedures in the absence of a high reliability organizational culture; and
- tight coupling between stages of the process or units may set off a chain reaction of errors throughout the entire process.

The results of the study are in accordance with findings of previous normal accident and HRO research, as well, in that they suggest that operational failures result from a variety of different combinations or configurations of factors rather than a single cause (REASON, 1997; PERROW, 1999).

The comparison of the operational failures studied at Zeta Bank, however, suggests a possible sharpening of focus with respect to observations from earlier studies, in the sense that it is evident in the SBP failure that the absence of high risk conditions does not, by itself, guarantee that operational failure will not occur. In other words, operational failure can take place even under relatively low-risk conditions, depending on the interrelationship among the factors present in a given situation in a given period of time and the absence of adequate defenses. Additional studies specifically focusing on operational failures under low-risk conditions appear relevant.

6. CONCLUSIONS

The evidence of the study clearly demonstrates the relationship of the operational losses experienced by Zeta Bank in its Brazilian System of Payment (SBP) and Credit Operations processes to causes of operational failure predicted in the HRO literature, permitting an affirmative answer to the first of the research questions addressed.

The answer to the second question is also affirmative. HRO theory offers solutions for management of the factors that, from the perspective of operational risk management, cause loss:

- to deal with human error: a high degree of operator responsibility: rapid decision-making (ROBERTS; ROUSSEAU, 1989) constant vigilance, obedience to formal rules and codes of conduct (ROCHLIN, 1993); establishment of an organizational culture of high reliability (GRABOWSKI; ROBERTS, 1997); rewards and incentives for improving security (ROBERTS et al., 2001);
- to deal with system error: constant monitoring, contingency solutions, proactivity and reaction (ROCHLIN, 1993); real-time technology management (ROBERTS; LIBUSER, 1993); contingency plans (WEICK; SUTCLIFFE, 2001); appropriate specifications, appropriate business procedures and processes, operating capacity, and organizational propensity for innovation (LALLY, 2002);
- to deal with process errors: redundancy in controls and in information systems; rapid decision-making (ROBERTS; ROUSSEAU, 1989); foreseeing and reaction (ROCHLIN, 1993); non-simplification of routines, sensitivity to operational procedures (WEICK; SUTCLIFFE, 2001);
- to deal with frauds: high level of operational reliability and security (La Porte and Consolini cited in ROCHLIN, 1993); prioritization of security

(GRABOWSKI; ROBERTS, 1997);
- to deal with external events: constant vigilance of the operating environment (ROCHLIN, 1993).

Langley (1999) argues that designing process research that selectively applies concepts from different theoretical traditions to process data can enrich theory. This is what we have attempted to do in this study, bringing concepts from the HRO tradition to bear on problems from the operational risk management tradition. Our findings strongly suggest not only that HRO theory can be broadened to include financial institutions but that the study and practice of operational risk management might benefit from the incorporation of concepts and solutions from HRO theory, thus offering a potential contribution to both the HRO literature and to the operational risk management literatures.

Some limitations to the method used must be pointed out. Data from documentary research with respect to registration of operational failures and fragilities existing in operational security may not be entirely reliable. Some of the material consulted may be partial, distorted or incomplete. The questionnaires relied upon perceptions of respondents, also notoriously partial. Attempts were therefore made to counterbalance these limitations by use of multiple sources of evidence and triangulation of data. Review of documents with respect to the processes studied and the operational losses experienced were supplemented by review of accounting and internal audit reports. Non-participant observation and an interview with the manager of the Technology Unit were used to supplement the perceptions of the operators of the processes studied.

In addition, certain limitations are inherent to the case study strategy utilized, chief among them the question of generalization of the results. While the case study strategy has its limitations, it also has strengths that may outweigh the disadvantages, depending upon the purpose of the research. The case study strategy is faithful to the richness, dynamism and complexity of process data and enables a deeper understanding of organizational phenomena. In cases using process data, even one or a few cases offer the strong possibility of identifying fundamental process drivers, often being sufficient to produce useful insights (LANGLEY, 1999). In the investigation reported here, based on detailed process data, we found evidence that the processes driving the operational failures studied were the same as those observed in the HRO literature, permitting the inference that HRO principles might have a contribution to make to the management of operational risk in financial institutions. Obviously, other studies with similar results would strengthen this finding.

Our study addresses HRO and operational risk as firm-level phenomena. While all firms in a given sector may be exposed to operational risk, it is clear from HRO studies that individual firms within a sector can manage their operational risks in such a way as to reduce the probability of operational failures.

The results of our study strongly suggest that HRO theory does, indeed, have the potential to enrich comprehension of and discussions about operational risk in financial institutions and to contribute to the effective management of such risk. Understanding the underlying causal mechanisms that contribute to operational failures makes it possible to take positive steps to manage them rather than merely estimating the probability that such failures might occur.

Puschaver and Eccles (1997) suggest that risk management in the full sense involves management of opportunity, of hazard, and of uncertainty. The management of opportunity (upside risk management) involves the actions taken by management to achieve positive gains. The management of hazard (downside risk management) involves preventing or mitigating actions, situations or events that can generate losses. In our paper we have focused

exclusively on the downside aspects of operational risk management. There is, however, a possible upside aspect to the use of high reliability techniques in managing operational risk. High reliability may, in fact, offer strategic opportunities as a possible core competence which can be developed and then leveraged for higher returns. This possibility merits further investigation.

REFERENCES

BEA, R.G.; MOORE, W.H. Operational reliability and marine systems. In: ROBERTS, K.H. (Org.). **New challenges to understanding organizations**. New York: McMillan, 1993.

BIS – Bank of International Settlements. International convergence of capital measurement and capital standards. Basel: BIS, 1988.

_____. International convergence of capital measurement and capital standards. Basel: BIS, 2004.

FORD, E.W.; DUNCAN, W.J.; BEDEIAN, A.G.; GINTER, P.M.; ROUSCULP, M.D.; ADAMS, A.M. Mitigating risks, visible hands, inevitable disasters, and soft variables: management research that matters to managers. **The Academy of Management Executive,** v.17, n. 1, p. 46-60, 2003.

GRABOWSKI, M.; ROBERTS, K.H. Risk mitigation in large-scale systems: Lessons from high reliability organizations. **California Management Review,** v. 39, n. 4, p. 152-162, 1997.

LALLY, L. Complexity, coupling, control and change: An IT based extension to normal accident theory. **Decision Sciences Institute 2002 Annual Meeting Proceedings.** New York: Decision Sciences Institute, 2002**.** Available at: <http://proquest.umi.com/pqdweb>. Accessed June 6, 2004.

LANGLEY, A. Strategies for theorizing from process data. **Academy of Management Review**, v. 24, n. 4, p. 691-710, 1999.

MARSHALL, C.L. Measuring and managing operational risks in financial institutions: Tools, techniques, and other resources. Singapore: John Wiley and Sons, 2001.

PERROW, C. **Normal accidents: Living with high-risk technologies**. New Jersey: Princeton University Press, 1999.

PUSCHAVER, L.; ECCLES, R. **Managing Upside Risk.** DerivativesStrategy.com, Nov 1997. Available at: <http://www.derivativesstrategy.com/magazine/archive/1997/1197col1.asp> . Acessed January 28, 2009.

REASON, J. Managing the risks of organizational accidents. Aldershot: Ashgate, 1997.

_____. Human error: Models and management. **Western Journal of Medicine,** v. 172, n. 6, p.393-395, 2000.

ROBERTS, K.H.; ROUSSEAU, D.M. Research in nearly failure-free, high reliability organizations: Having the bubble. **IEEE Transactions on Engineering Management,** v. 36, n. 2, p. 132-139, 1989.

ROBERTS, K.H. Managing high reliability organizations. **California Management Review, v.** 32, n. 4, p. 101-113, 1990.

ROBERTS, K.H. Some Characteristics of one Type of High Reliability Organizations. **Organization Science.** California, v. 1, n. 2, p. 160-176, 2001.

_____; LIBUSER, C. From Bhopal to banking: Organizational design can mitigate risk. **Organizational Dynamics,** v. 21, n. 4, p. 15-28, 1993.

ROCHLIN, G.I. Defining high reliability organizations. In: K.H. Roberts (Org.). **New challenges to understanding organizations.** New York: McMillan, 1993.

SAGAN, S.D. Learning from normal accidents. **Organizations & Environment**, v. 17, n. 1, p. 15-19, 2004.

VOGUS, T.J. Mapping the territory: Positive organizing as collective mindfulness, resilience, and sensemaking. **Positive organizational scholarship**. University of Michigan Business School, 2003. Available at: <http://www.bus.umich.edu/positive/contributors/timothyvogus>. Accessed October, 2003.

WEICK, K.E.; SUTCLIFFE, K.M. Managing the unexpected: Assuring high performance in an age of complexity. San Francisco: Jossey-Bass, 2001.

YIN, R.K. **Estudo de caso.** 2. ed. Porto Alegre: Bookman, 2001.