REPORT 13 DECEMBER 2006

D NO. 06-11714-601

2006:18

Firms' management of operational risk and FI's recommendations

TABLE OF CONTENTS

Foreword

During the autumn of 2005 and spring of 2006 Finansinspektionen carried out a comprehensive review of the operational risk management in fifteen Swedish banks and credit market companies (firms). This review performed at the request of those firms. It was part of an assessment of how well they were complying with the requirements of the regulations regarding the standardised approach for capital requirements in relation to operational risks. FI has reviewed the policy and methodology documentation of the firms and undertaken on site visits in order to examine how those approaches have been implemented within the organisations.

The reports summarises the current situation with regard to operational risk management in those firms. The purpose of this is to describe current practice related to risk analysis approaches, risk management mechanisms and risk organisation. The report does not cover advanced approaches, i.e. Advanced Measurement Approaches (AMA), to quantify operational risks.

FI's view of the various issues is presented in each of the areas covered. However, it must be emphasised that these views are merely recommendations which are, to some degree, beyond the requirements set out in the regulations related to the standardised approach. There may be solutions other than those proposed that are compatible with the regulations.

Summary

During the autumn of 2005 and spring of 2006 Finansinspektionen reviewed, at their request, the management of operational risks in fifteen firms. This review has provided FI a good overview of the market.

These firms identify and evaluate operational risks using a self-assessment approach, evaluating risk on the basis of probability and severity. In certain cases self-assessment is supplemented by risk indicators. The firms that FI reviewed have also introduced, or are in the process of introducing, structured databases of loss and incident data.

In general, there is consensus in the market regarding the approaches used for operational risk management. However, there are significant differences in how these approaches are implemented and how far the firms have progressed in applying them.

Most of the firms manage their operational risks using action plans linked to their self-assessment tool. Naturally the operational risk profile is also affected by many other decisions taken within the organisation, including by its board. Another tool for managing operational risks is continuity planning. This is structured differently in different companies, but in all cases includes some form of crisis organisation and also including back-up solutions for electricity, communications and IT systems.

The function responsible for operational risk control is usually subordinate to a senior officer who reports to the firm's managing director. This operational risk report contains a consolidated risk summary, which is submitted to the board, usually every six months. The report contains all operational risks, including those related to compliance and security. In some cases the security organisation is part of the operational risk organisation. In other cases, the risk control function receives reports from the security organisation to ensure a comprehensive operational risk report to the board.

FI recommends that the board play an active role in risk management and establish a general framework to cover all fundamental issues. A number of tools should be used to identify and evaluate operational risks: self-assessment or process-based risk analysis, risk indicators and analysis of incident and loss data. The risk analysis should cover all operational risks and be reported to the board. The responsibility for the central analysis and control of operational risks should lie with a risk control function that reports directly to the managing director.

Introduction

Operational risks

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Typical examples of operation risk are data entry errors, dependence on key personnel, internal and external fraud, and system failure.

Operational risk is different to credit risk and market risk in that a firm will very seldom actively take on operational risk in order to earn money. Exceptions to this can be services that involve the firm taking over particular activities from its clients (*insourcing*).

The standardised approach for capital requirements for operational risks

The new capital requirements directive (CRD), based on the Basel 2 agreement, are currently being implemented. These regulations contain provisions for calculating the capital requirements for credit risks, market risks, operational risks and other risks.

With regard to operational risk the new capital requirements regulations allow three possible approaches:

- *the basic indicator approach*, where the capital requirement is determined as an income indicator multiplied by 15 percent
- *the standardised approach*, which works in the same way but using different percentages for different business areas
- *advanced measurement approaches*, in which the firm itself constructs models in order to quantify its operational risks based on historical data.

In the regulations related to the standardised approach there are a number of qualifying criteria which firms must fulfil in order to be allowed to use the approach. These involve requirements related to:

- policy documents for operational risks
- risk management processes
- documentation of risk management processes
- governance and control
- reporting
- calculation of the income indicator.

Finansinspektionen's Regulations FFFS 2005:19 regarding the measurement and management of operational risk, in which the standardised approach is regulated, can be found at www.fi.se. (This regulation will be substituted by the FFFS 2007:1 by 1 February 2007, also accessed at www.fi.se)

Finansinspektionen's review

During the autumn of 2005 and spring of 2006 FI carried out a review of operational risk management in firms that requested such a review in accordance with the Capital Adequacy and Large Exposures Act.[1] Fifteen firms, including large and small banks, savings banks, and credit market companies, asked to have their operational risk management approaches reviewed.

The review was carried out in two stages:

- an off site analysis of the firm's risk management, based on the documentation they had submitted to FI
- on-site visits – a review of how risk management processes are implemented and whether the firms follow the prescribed instructions.
-

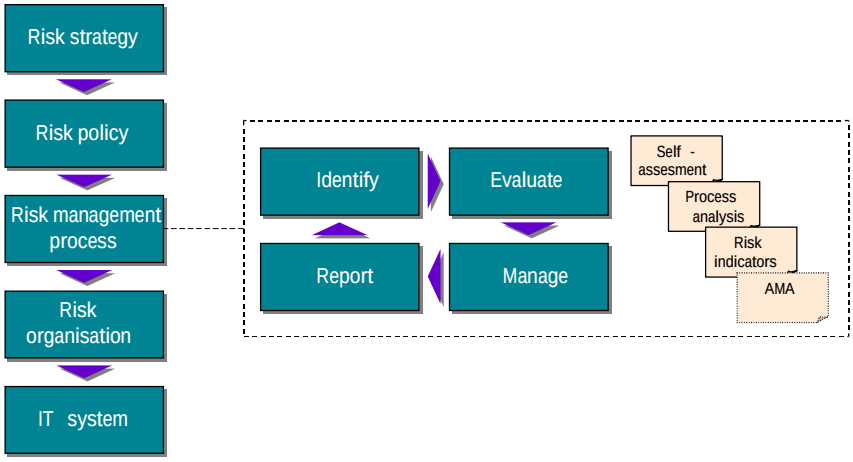
Within the framework of these on-site inspections, FI visited the central risk control organisation, various local or regional organisations and, where necessary, the investment bank operation and foreign branch offices or foreign subsidiaries.

During the review FI communicated the shortcomings identified to all firms. On completion of the off site examination all the firms had failed with regard to the requirements for policy documents and most had shortcomings in their reporting. In most cases these shortcomings have been attended to. On completion of the review most of the firms fulfilled most of the requirements contained in the regulations.

The review has provided FI with a good overview of how the firms manage operational risk. When compared with an equivalent situation a couple of years ago, it is clear that the new regulations have contributed towards the promotion of improved risk management. FI has also observed that many firms have started to see a tangible business benefit in having a structured process for identifying operational risk.

[1] Chapter 7, section 13, paragraph 2 of the Capital Adequacy and Large Exposures (Credit Institutions and Securities Companies) Act (SFS 1994:2004)

Components in a risk management system



It is important that risk management in a firm is managed systematically at a strategic level. As far as possible the risk profile should be the result of conscious decisions. Operational risk should be a component when making important decisions that affect operational activities.

The risk strategy is formalised through a risk policy and other policy documents, which also normally contain demands on the risk management process, approaches and tools used, the risk organisation and risk reporting.

The risk management process covers, at the highest level, the identification and evaluation of risks, measures to control the risks and risk reporting. This process is supported by various analysis tools such as self-assessment, process-based risk analysis, risk indicators, and advanced internal model approaches.

The risk organisation includes all officers with a role in the risk management process, including the risk control function, board, managing director, operational risk managers within different departments in the company, line managers etc.

The need for IT-system support is often more limited for operational risk than for market or credit risk. Normally an incident database is used, with a suitable reporting interface and, in certain cases, system support for self-assessment approaches.

The following chapter in this report has been structured on the basis of the generic risk management process as above. First the tools for identifying and evaluating risks are described, then the mechanisms for risk management and, finally, reporting. Risk organisation issues are discussed in conjunction with reporting.

Identifying and evaluating operational risks

The analysis of operational risk

While the areas of market and credit risk have an arsenal of advanced models for quantifying risks, the area of operative risk is still at a stage where qualitative, subjective analysis approaches are the most commonly used. Two main analysis approaches can be identified: self-assessment and process-based risk analysis.

The risks are generally evaluated in terms of probability and severity on a scale of four or five. In most cases the severity is expressed in monetary terms. However, the bases of evaluation often vary within a large organisation in order for each of the organisational units to benefit from its own risk evaluation - a significant risk for a small business area is perhaps completely insignificant for a large one. This means that it is a challenge to consolidate risk at the group level. The risk control function therefore often plays an important role in the analysis by making an overall assessment.

Designing and introducing this type of analysis approach generally takes a fairly long time. It often takes a number of years before the organisation has learnt to use the approach and to use it consistently.

Often risk indicators are used to supplement subjective approaches (see below).

Self-assessment of operational risks

The most common type of analysis approach for operational risk is self-assessment. However, the exact approach used to evaluate operational risk through self-assessment varies greatly between firms.

Self-assessment is normally undertaken once a year in a workshop by senior officers with expertise from the sub-process or the organisation to be analysed. In some cases risk identification is supported by forms with predefined risk areas in which the participants can fill in the evaluation of the probability and severity of risks. In practice there is a significant difference between the risks that have been assessed in this respect. In certain cases a form is used in which in principle all risks have been predefined, and evaluation means only evaluating those specific risks. In other cases self-assessment is undertaken entirely without the support of predefined risks or risk categories.

Self-assessment can be carried out for organisational units, processes or IT systems. Usually analyses are undertaken by organisational unit, using some supplementary analysis in the process dimension.

There are also considerable variations between the firms on which organisational level the risk analyses have been carried out. In some cases the analysis is carried out for an entire region in Sweden, and in other cases

at a lower level. This often varies within firms, depending on the risk profile and the inherent risk in the activities carried out in the different parts of the organisation. If the analysis is carried out at a low level in the organisation it can be difficult to cover the entire operation every year.

Certain banks have introduced systems for self-assessment and for storing and analysing self-assessment data.

Process-based risk analysis

A more structured but somewhat more time consuming alternative to self-assessment is process-based risk analysis. This approach is based on systematic scrutiny of process documentation, which is normally in the form of process maps, and the identification of risks supported by a detailed risk rating. This type of analysis can be conducted by an independent analyst in collaboration with the process owner and, if necessary, experts in the relevant fields.

The data produced by a process-based risk analysis is typically similar to the result of a self-assessment: the evaluation of probability and severity, normally on a scale of four or five.

Process analysis requires more resources than self-assessment because it requires the entire process documentation to be available and continuously updated. On the other hand documenting important processes is valuable in itself as it directly reduces the potential effect of certain operational risks, principally those dependent on key personnel and other personnel-based risk. A process analysis can also provide a more systematic risk identification process than self-assessment.

Process-based risk analysis is a far less common tool than self-assessment. The tool can be difficult to use in a large, complex organisation and is not used by any of the major banks reviewed.

Incident and loss databases

All of the firms which have been reviewed have some form of incident and loss reporting, even though certain firms are still at a relatively early stage of development. Reporting normally covers all losses above a specific threshold, often SEK 50,000, and incidents which have been sufficiently serious but have not resulted in loss. The reporting threshold is determined on the basis of the character of the operation and size of the firm. A report is normally made for each loss, describing the event, the damage, loss amount and the measures taken or to be taken. The incidents or losses are often categorised based on those types of event described in the new capital requirements directive. This information is stored in a database and statistics are reported periodically to the boards of several of the firms.

One significant challenge when introducing an incident and loss database is to achieve reports that cover all the incidents that occur. It is difficult to incentivise organisations to report losses and incidents.

Analysis of risk in new products

All of the reviewed firms have some form of documented new product approval process (NPAP). This process is often sophisticated for investment bank operations. The scope of the NPAP often depends on the product type. Normally the process includes the following components:

- checking that the product can be managed by all parts of the organisation (front, middle, and back office etc.)
- documentation of the process or a procedure description for the new product
- checking that there are evaluation and risk measurement models for the product
- all relevant line managers should approve the new product.

Risk indicators

Risk indicators are typically in the form of key ratios which measure the function of one of the processes in the operation, and monitor it over time. For example this can be measuring the proportion of transactions that are cancelled, the average length of employment in a unit or the number of breaches of limit in a period. The aim is generally to supplement subjective risk analysis approaches with a more objective follow-up of observable, empirical units that can be expected to correlate to specific operational risks.

There are generally few firms that use risk indicators. However, certain large banks have developed the use of this tool in investment bank operations. Certain firms are attempting to use risk indicators in other areas of their business, however, development in this field is slow as it is difficult to identify suitable indicators. The difference can be explained by the fact that operational risks are generally significantly higher for investment bank operations than in other activities.

Finansinspektionen's recommendations

All firms, irrespective of size, should have a well-documented risk analysis approach designed for the activities being carried out. The analysis should be process orientated to correctly capture risks which affect several parts of the organisation.

It is important to systematically identify the business critical processes and IT systems and to ensure that these are analysed thoroughly for operational risk. It is also very important that enough attention is paid to extreme events in the risk analysis, as these risks will hopefully not be captured by internal loss databases.

Firms should also track, store, analyse and report incident and loss data in a structured manner. This data is valuable in it support for the risk identification process but also has value in being able to support efforts to effectivise and improve processes. The information provided by a functioning loss database about realised operational risks, can also help to increase the awareness of operational risk in the organisation.

At the very least risk indicators should be used within investment bank operations, preferably within other areas as well depending on risk profile. The indicators used should depend on the type of activity and any weaknesses in the processes being analysed.

To supplement the analysis of processes and systems a process should also be in place to analyse the risk in new products. This makes the organisation aware of the changes to the risk profile created by a new product. The analysis of operational risk should be an integrated part of the process of developing and approving new products. All parts of the organisation which will handle a specific product should approve the decision-making background data and documents for a new product.

The management of operational risks

Policy documents for operational risks

The new capital requirements regulations are stricter with regards to the role of the board of directors on the risk management of financial institutions. In many cases this is reflected in the policy documents for operational risk approved by the board. The quality of the policy documents in the firms reviewed has been varied. During the review most firms have been criticised to some extent in this respect. In certain cases the responsibility for establishing the framework for operational risk management has been delegated almost entirely to the managing director. In other cases the board has been directly involved in setting requirements for all relevant aspects of risk management.

The firms that have done best in this respect have allowed the board to set out:

- the firm's definition of operational risk and a categorisation of the risks
- tolerance levels for operational risks
- roles and responsibilities for the board, risk control function, business area managers, process owners and other senior officers involved in operational risk management
- the tools to be used to identify and evaluate operational risks
- a reporting plan including requirements regarding the content of the reports
- overall outsourcing principles.

Tolerance for operational risks

Defining the tolerance for operational risks is difficult and no uniform practice has emerged and firms use different definitions in their policy documents. Certain firms only define unacceptable losses. This solution merely provides a measure of the outcome which can be tolerated rather than a forward looking approach on the risk that one is prepared to take. Other firms take the risk analysis approach as a basis, for risk tolerance. For example by requiring that action be taken when the risk exceeds a certain level or by linking specific risk levels to specific requirements for corrective action.

Control of the risk profile

All firms reviewed use action plans for operational risk management which are directly associated with the risk analysis approach used. For each significant risk identified on the basis of selected criteria, a corrective action to reduce this risk is set. These action plans are generally documented when the risk analysis is carried out.

It is important to remember that the operational risk profile depends on a large number of decisions taken in different areas, those decisions made as a

direct consequence of the risk analysis are only a small proportion of these. Decisions about the structure of the operation, choice of IT platform, launch of new products etc., may have a very significant effect on the total risk.

Continuity planning

An important component of operational risk management is a thorough and customised continuity plan. This requires good analysis and a decision on which components of the operation are most worth protecting. Continuity planning covers threat and vulnerability analysis, crisis organisation, back-up solutions and security activities such as the availability of extra electrical supplies, communications etc. There were differences in the degree to which continuity planning had been developed in the firms reviewed. Some organisations focus on the ability of the crisis organisation to handle situations arising, in which both contact with the media and decision-making are planned and trained for. Other organisations develop plans to cover as mush as possible. One common development is that the responsibility for these plans is very clear, process owners and systems owners have an express responsibility for operations, even in a crisis situation. For this reason much of the continuity planning is carried out within the line organisation.

IT, communications and electrical supply are central to continued operations and there are often well-developed back-up solutions in place for these.

Finansinspektionen's recommendations

It is very important that the board and management are actively involved in the firm's risk management. The board should set out the overall principles for risk management:

- risk categorisation and definitions
- risk organisation including the division of responsibility between the board, risk control function and relevant senior officers in the line organisation
- approaches and tools to be used
- the content and frequency of reports
- tolerance levels for operational risks
- principles for outsourcing
- requirements for continuity planning and crisis readiness.

An established risk categorisation aims to create a common conceptual tool for the entire organisation and allow effective reporting and management.

The tolerance for operational risk set by the board should be linked to the risk evaluation approach. If some form of model for allocating financial capital is used, this can also be taken as a basis when defining the tolerance for operational risk.

The risk analyses carried out should be directly associated with an action plan for reducing non acceptable risks. In addition, the action plan should

contain information about those responsible and the final date for this corrective action. The risk analysis should also support the continuous improvement of processes and procedures.

The decision-making background data for all large decisions affecting operational activities (for example the structure of the operation or setting up in new countries) should contain a thorough analysis of how the operational risk profile will be affected.

Continuity planning is an important tool for managing risks which have potentially serious negative consequences. It is important that the organisation practices the planned activities and that the crisis organisation trains continuously.

Organisation and reporting

Organisation and division of responsibility

The main component of the risk organisation is the risk control function. Often the same organisational function is responsible for the management and reporting of operational risk as for other risk areas. An important issue for the risk organisation in all risk areas is the independence of the risk control function in relation to the business units. This is especially problematic with regards to operational risks, as operational risk is present throughout the organisation. In certain firms the risk control function is part of the same organisation as the credit function, while in other cases it is directly subordinate to the managing director or another senior officer reporting directly to the managing director. Smaller firms often have an organisation in which the head of risk control reports directly to the managing director, while in larger banks it is more common that risk control is organised together with the credit function in one way or another.

With regards to operational risk the internal review and compliance functions also play an important role. The internal review function plays an important role with regards to evaluating internal control and the compliance function is naturally important with regards to risks related to compliance. Although these three functions are (and should be) generally independent of each other, most firms have ensured that there are reporting lines from, for example, compliance to the risk control function in order to ensure that the reporting of operational risk as a whole is made to the board. The same applies to risks regarding security in those cases where the security organisation is not part of the risk control function.

Because operational risk must be identified and assessed by personnel with expertise in the relevant processes, it is common for the risk control function to have contact persons in different parts of the organisation. These people are responsible for driving the risk analysis process and reporting identified risks to the risk control function. The risk control function normally aggregate the risk analyses made by various units and by doing so produces an overall assessment of risk exposure for the entire firm which is then reported to the board and managing director.

Risk reporting

There are significant differences between firms in their reporting of operational risk to the board. Many firms have been criticised by FI for this during the review process. In certain firms there has, in principle, been no reporting. Even between firms with more comprehensive reporting the differences in content and quality are considerable.

Those firms with the highest quality reporting make relatively comprehensive reports twice a year which contain a aggregation of the risk analyses made in order to provide a current picture of the firm’s exposure to

operational risk by business area and risk category. In addition, incident and loss statistics and major incidents and losses are reported.

Finansinspektionen's recommendations

The responsibility for analysis and control of operational risks should lie with a risk control function that reports directly to the managing director. As risk analyses will always be based on qualitative assessments made by people working in the processes concerned (using self-assessment for example) the independence of the risk control function is vital to ensure the duality of the risk assessment. Because there is operational risk throughout the organisation, even in departments with no business responsibility, it is best that the function with responsibility for operational risk control be directly subordinate to the managing director.

The firm's board and management should receive reports about operational risk which cover at least:

- the total exposure to operational risk
- information which allows the recipient to see whether exposure is within the set tolerance level
- statistics for incidents and operational losses
- specific information about serious losses or incidents
- risk mitigation measures taken
- follow-up of previous corrective action.

Reporting should be structured so that the recipient can read and understand the report with out a verbal explanation, although a verbal explanation should always be given at board meetings. All operational risks, including security risk and compliance risk, should be gathered in a report to provide the board and senior management with an aggregated picture of the firm's risk exposure.

Continued development

By fulfilling the requirements in the standardised approach, firms can lay the foundations for and proceed with the development of more advanced approaches for managing operational risk. The standardised approach is not particularly risk sensitive. For the advanced measurement approach, the most advanced approach for capital requirements for operational risks, the structured tracking and saving of incident and loss data is the most important keystone for developing the models and approaches required to meet the capital requirements regulations. FI would like to see firms take this step in order to increase their risk management's degree of sophistication and obtain a clearer link between risk and capital.

However, even when using more advanced risk quantification approaches, one can never ignore that operational risk is primarily a process issue. Good internal control, competent personnel and high quality processes and systems are the most important factors in operational risk management. In addition, advanced statistical models for quantifying operational risk will always be undermined by significant model risks, which is why they should always be used in parallel with subjective models such as self-assessment or process analysis.