Risk Assesment: An Important Tool for Companies

PANAIT NICOLETA GEORGETA
Department of Finance and Accounting
Faculty of Economic Sciences
185 Calea Văcărești, 4th District, Bucharest code: 040051
"Nicolae Titulescu" University, Bucharest, Romania
nico.panait@gmail.com

PANAIT COSTIN ALEXANDRU
Ph.D. candidate, University of Craiova cod: 200585
13, A.I.Cuza Street, Craiova, Dolj, ROMÂNIA
costin.panait@gmail.com

Abstract: *The study summarizes what it means risks, the main risk management strategies. The complexity of the business environment, liberalization and internationalization of financial flows, brings rapid innovation, diversified financial markets, new opportunities but also multiplied risks. Companies from Romania establish the types of risks they are prepared to take and the threshold at which risk is considered significant. The process of determining the risks that are taken includes the nature, the scale and the complexity of risk.*

Keywords: *companies, company's risks, the strategy of the companies, profit, risk management*

1. Introduction

Risk management is not an end in itself, but a key instrument supporting the management in achieving corporate objectives. This applies, in particular, to the risk management.

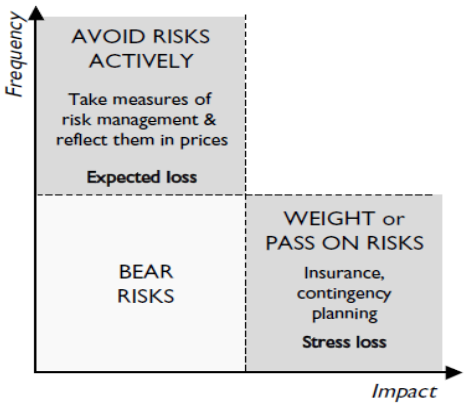
There is a close relation between a company's mission, its vision and general strategic orientation on the one hand, and its willingness to take risk (risk appetite, risk tolerance), risk policy and risk strategy, on the other hand. All these elements have a strong impact on corporate culture and, therefore, on values, opinions and attitudes of employees. It is decisive for the well-balanced interaction of those elements whether the focus is on formal compliance with regulatory requirements or expectations of the capital markets or whether operational risk management is fully embraced by the management and all employees in their day-to-day work. While the basic components of a risk management system are similar, companies often significantly differ by their culture.

The corporate culture of a listed, internationally active companies orientated to shareholder value, a multinational companies rooted in a region and committed to supporting its members or a savings companies focusing on public interests differ more than the basic components of their risk management systems which always include the identification, assessment, treatment and control of risks. It is the culture, mission and vision that shape the readiness of these companies to take risks, their risk tolerance and risk profile, and thereby the concrete form of risk management competences.

Using the relation between loss frequency and severity, a rough differentiation can also be made between the measures for managing the relevant risks (chart 1) in the case of infrequent vents involving low loss potentials, the most economical solution is to bear the risks, i.e. accepting them as a part of expected loss and including them in the calculated costs. As a rule, risk acceptance depends on a cost-benefit analysis or weighting of expected income versus risk. A rational reason for accepting risks would be that the expected loss is lower than the cost of management activities to mitigate the risks.

If the frequency of specific loss events exceeds a certain level, risk management methods pay off serving to actively avoid such loss events – their costs naturally have to be covered by the prices. As the impact increases and the frequency of the events decreases (unexpected loss, stress loss), there is a transition from these measures to crisis or disaster management (business contingency management); to cover the material damage, risk mitigating measures are frequently used, e.g. insurance contracts.

Chart 1. Matrix on Operational Risk Management as a Function of Impact Potential and Frequency of the Related Events



2. Risk Identification and Assessment

After laying the organizational basis and establishing the framework, the next step frequently is to build a loss event collection and risk inventory (self-assessment).

The management of risks can be described as a cycle comprised of the following steps:

- risk identification;
- risk assessment;
- risk treatment;
- risk monitoring.

Chart 2. Risk Management

In order to control and limit its risks, a company first has to become aware of the potential risks. By identifying risk sources and risk drivers, a sound “health check” – in line with the saying that “prevention is better than cure” – allows a company to take preventive measures.

During risk identification and assessment, companies should consider several factors in order to establish the risk profile of a company and its activities, for example:
types of customers, activities, products, design, implementation and effectiveness of processes and systems, risk culture and risk tolerance of a company, personnel policy and development, and environment of the company.

The following tools have proven especially useful for this work: self-assessment (risk inventory), loss database, business process analysis, scenario analysis, and risk indicators.

Quantification combined with qualitative management already permits improvements in control and monitoring.

3. Risk Inventory

Self-assessments aim at raising awareness of risks and at creating a systematic inventory as a starting point for further risk management processes as well as process improvements towards better performance.

In most cases, they take the form of structured **questionnaires** and/or (moderated) **workshops** and complementary **interviews**. Their main purpose essentially is to identify significant risks and then evaluate them.

Special attention should be paid to the identification of those risks, which could endanger the survival of the institution. A SWOT analysis **(**this tool is very often used in strategic planning and can contribute to linking strategy definition, including the development of a risk strategy) and risk management) serves to identify and present one's own strengths and weaknesses as well as opportunities and threats. Depending on the purpose defined, self-assessments may have a different orientation or approach:

- risk orientation;
- control orientation;
- process orientation;
- goal orientation.

Depending on the approach, the inventory focuses on one component and derives the other elements from the identification of the key component. Workshops organized in the context of risk management primarily aim at highlighting risks. Because it is usually very important for such a self-assessment to know the core processes and sub-processes of a company, the implementation of risk management could be preceded by a workshop identifying and evaluating processes. This could be repeated, if necessary, e.g. when important new products are introduced or when organizational changes take place.

Structured questionnaires, which could also be distributed through the intranet, offer the advantage of easy data recording, also in the case of big organizations with numerous organizational units. **Moderated workshops** contribute to raising awareness and communicating risks across different organizational units to a particularly high extent. In many cases, a survey (questionnaires and/or interviews) will be carried out before such a workshop.

Based on the results, the workshop may then concentrate on significant risks, controls and processes. The decision on which instruments to use also depends on corporate culture and the participation of senior management. The active involvements of senior managers as well as a participatory culture are factors contributing to the success of a workshop.

Self-assessments may be limited to identifying and assessing risks, but ideally control and risk self-assessments (CRSA) expand risk assessments by highlighting existing or additionally required controls for mitigating the key risks identified. If considerable control gaps exist, CRSA workshops may develop suitable measures and action plans. A CRSA can determine the net risk of a process, business line or activity that is relevant as a target value for measures of qualitative risk management. The net risk depends on the magnitude of the inherent risk taking account of the effectiveness of existing control measures:

Net risk = Inherent risk – Controls

For the net risk, risk treatment measures can be planned and summarized in an action plan. For this residual risk only, there is a detection risk.

The detection risk is the risk that an auditor does not detect a significant risk. The following relation applies to the audit risk that is relevant for a risk-oriented audit approach of internal and external auditors:

Audit risk = Inherent risk x Control risk x Detection risk

In order to be successful, self-assessments need careful **preparation**. Specifically, this means that the most suitable approach has to be chosen and the participants have to be selected and trained. Before the self-assessment, the participants should, for example, be familiarized with the risk definition adopted by the company and other elements of the company's framework for managing risks that are essential for understanding the system. If possible, core processes to be assigned to risks and controls within the framework of self-assessment should be identified and documented already beforehand.

Self-assessments should not be performed only once when risk management is introduced, but regularly. In practice, most of the bigger companies perform such assessments once a year. Smaller companies should schedule a review at least when major changes take place, e.g. restructuring or taking up new business lines.

Repeated self-assessments involve the danger of a certain fatigue effect that occurs after the first few assessments. There is, for instance, a tendency to take over the results of the previous year without critically reviewing them.

This may be avoided by changing the membership of the group and by inviting employees who can contribute a new perspective to take part in the self-assessment workshop. Care should always be taken to ensure the consistency of the methodology and the comparability of the results.

Depending on the organization, internal auditors will be involved in self-assessment at different intensities. For smaller companies, internal auditors may be particularly helpful in the implementation phase because the internal audit function, even if outsourced, has knowledge about risks, controls and processes across the organization. In their turn, internal auditors can improve the risk orientation of audit planning on the basis of self-assessment results. In bigger companies, internal auditors should perform their own risk assessment independent of the management's self-assessment with a view to audit planning. On the one hand, internal auditors can obtain important information for their own work by analyzing different assessments and, on the other hand, they can provide an independent evaluation of self-assessment results and thereby contribute to quality control. At any rate, the risk controlling unit (or a comparable unit) has to stay in charge of the methods used and the risk owners, primarily the line managers, are to remain responsible for the management of risks, i.e. responsibility must not be transferred to internal auditors as this would impair their **process independence**.

5. Informational Risk - Internal Loss Databases

Internal loss databases are used to record and classify loss events. The systematic collection of loss data within forms the basis for an analysis of the risk situation and, subsequently, for risk control. The quality of models measuring risk strongly depends on the quality of the loss data recorded in the database.

An effect in collecting internal loss data is that primarily frequent loss events with low severity are recorded. ("high-frequency, low-severity events"). For this reason, the benefits of an internal loss database relate less to risk modeling, but rather to its use for improving the efficiency of processes and the internal control for those risks that should be reduced.

Internal loss databases are not suited for covering rare loss events involving high ("low-frequency, high-severity events") and even losses, which endanger the survival of the institution. Major loss events occur extremely seldom, but may basically hit many companies. Therefore, all companies wishing to model their risk need to rely on external data.

This reveals risk clusters reflecting the risk profile of companies. Moreover, trends can be identified over time. Loss databases can have a very simple form. However, simple procedures rapidly reach their limits in bigger or more complex organizations when data from diverse areas or several companies have to be collated. Other organizational changes, too, may raise problems related to data consistency. As a rule, bigger institutions, therefore, use intranet-based solutions ensuring the decentralized, but uniform input of loss data.

The data fields should both meet the regulatory requirements of the approach selected and permit data analyses offering benefits internally. Please note that characteristics not recorded initially are difficult to add at a later stage. Therefore, a balance has to be found between information depth as well as benefits and costs. Examples of important data fields are: date (loss event, detection, entry into the books), severity of loss (gross loss), value adjustments, provisions, write-offs, loss-related compensations, event-type category, business line, geographic location, company (within a group), organizational unit, description specifying significant drivers or causes of the loss event, etc., and reference to credit or market risk.

It is important to have strict standards for events that must not be input (e.g. rumours or pending procedures). While rumors have to be excluded at any rate, pending procedures are a good example of borderline cases for which "viable" solutions have to be found and laid down in the standards.

A decision also has to be made on how to handle non-monetary losses and "near misses". These are difficult to evaluate, but can provide important information if recorded systematically. Specifications are also required on how to treat opportunity costs/loss of profit or profits resulting from mistakes made.

Operational losses frequently have a history and a kind of life cycle, i.e. they are not confined to a single point in time, but gradually become known and develop over time. The estimation of the loss may change due to new information, links between losses can become identifiable little by little or connected loss events may be spread over a period of time. Finally, compensations paid under insurance contracts or lawsuits impact the loss amount, but it often takes relatively long until the definitive loss amount is determined. As a result, loss databases should be appropriately flexible in order to take account of such changes. It is important

to avoid duplication, for example by recording related events that can be traced back to one root event in connection with that event.

An approval procedure is required for recording losses. The input of loss data should be checked and approved. As a rule, the executives of the recording units will approve the entries in line with their powers, while losses exceeding a certain level should require approval by the unit responsible for risk controlling. Furthermore, an escalation procedure should be established to ensure that losses are reported to the relevant units in line with specific criteria.

In the approval procedure, it is also important to define a rule for passing on information to, and coordinating measures with, the accounting division. There is no harmonized non-recording threshold below which loss data need not be stored. This threshold frequently depends on the institution's size, the business line or the methods used. While this threshold is usually rather high in investment banking, a particularly low threshold is selected if the intention is to collect data on minor, frequent loss events in order to reduce their number by targeted measures.

6. Business Process Analysis

Within the framework of risk management, business process analyses are used, in particular, to link processes, risks and controls in a risk analysis. They may also have the purpose of ensuring risk-oriented process optimization.

The identification of business processes across all organizational units is a prerequisite for allocating loss data to processes and determining the risk for a business process. Moreover, there is a close connection between business process analyses and self-assessments. On the basis of self-assessment, it should be possible to allocate the significant risks and controls identified to the business processes. As a result, at least a rough business process analysis should already be carried out before self-assessment.

In a business process analysis, processes and process steps are assigned to products and process chains are examined for risk-sensitive items. For such items, loss scenarios can be defined. Scenarios are a mandatory element required for the approval of an AMA as well as a central input for a scenario based AMA.

Through the documentation of processes and the identification of the organizational units involved in them, processes can be made transparent and improved with regard to effectiveness and efficiency. It is recommendable to define first the processes that are especially critical with regard to risks and thereby prioritize them. The subsequent business process analysis should focus on these processes. In a process map or process matrix, management processes, operative processes and supporting processes can be presented together with their interactions. Process descriptions, which are updated as necessary, facilitate communication between process owners and the employees who are process users. Important criteria are the processes' transparency, user-friendliness and up to datedness.

A business process analysis is a procedure requiring great efforts. It has to be maintained on an ongoing basis and must be reviewed regularly, but makes it possible to establish links between cause and effect and, due to the improvements it triggers in process management, may provide an added value.

7. Conclusion

Various companies need different types of information on risk management. Therefore, an element of effective risk management is regular reporting on the risk situation (in appropriately aggregated form) to the level responsible as a basis of decision-making as well as to monitoring levels (supervisory board, internal audit) and ad-hoc reporting in the case of significant events or changes in the risk situation. It also depends on the control culture of a company whether communication is mainly limited to reporting to higher levels in the hierarchy or whether the focus is on open communication in all directions and across the company.

Control of a company's most important risks should be embedded into a companywide risk management system providing a portfolio and bank-wide overview of risks. In this context, risk management and an internal control system are complementary instruments supporting the management in achieving the objectives. In order to establish a common language, to permit measurements and assessments by the same standards and to facilitate the coordinated response to risks, it is recommended to introduce integrated frameworks including risk management and internal control system and, therefore, the control and monitoring of risks, activities and processes throughout the enterprise. Such frameworks, be it for risk management or company-wide risk management, should be simple and easily understood by the addressees.

The separate management of different risks, i.e. dealing with them in isolated risk silos, prevents effective risk management. Risks may arise in one area and, frequently with some delay, impact other areas. But related risks may also occur in several areas and have effects across the organization whose significance is not realized in the individual areas.

References:

[1]. Mihai, T., *Technology and banking management*, Expert Publishing House, Bucharest, 2003, pag.151

[2]. Socol, A., *Accounting and management of banking companies*, Economic Publishing House, Bucharest, 2005, p. 45

[3]. P. Prunea, *The risk in economic activity*, Economic Publishing House, Bucharest, 2003, pag.20

[4]. Allen L., Boudoukh J., Sauder A., *Understanding Market, Credit and Operational Risk,* Blackwell Publishing, 2004;

[5]. Wood, Counting the Cost of Legal Risk, 2003: http://www.erisk.com/ResourceCenter/Operational/ CountingTheCostofLegalRis.asp