Operational Risk Management

May 2009

CRO FORUM

Table of contents

1. Executive summary

Operational risk has resulted in bankruptcies in the financial services industry in the past and remains one of the key risks to manage in the future. Further, European supervisors considered the causes of failures (and near-failures) of a number of insurers and their analysis showed that the causes were mostly associated with inappropriate risk decisions resulting from underlying internal failures rather than inadequate capitalisation per se.

Operational risk can be generally defined as the risk of loss, resulting from inadequate or failed internal processes, people and systems, or from external events. At the heart of operational risk management is a clear understanding of the operational risk events that may occur and the strength of the company's processes and mitigation activities to prevent or respond to such events.

The CRO Forum believes that operational risk should be managed actively at operating levels in line with the policies and guidelines as defined at company level. We believe that operational risk is unique to every company and operational risk management should take into account the specific context, such as the strategy, objectives and organizational structure of the company, but also external factors such as the business and regulatory environments in which the company operates.

We believe that adequate operational risk management is forward-looking and has the primary focus on pro-actively identifying, assessing and evaluating operational risk events that may occur and evaluating the strength of the company's processes and mitigation activities to prevent or respond to such events. The operational risk management efforts should have a transparent relationship to operational risk measurement, which we believe should follow a pragmatic approach taking into account the lack of relevant data and uncertainty in respect of tail events.

2. Introduction

This paper is part of a series of work by the CRO Forum under their Best Risk Management Practices initiative. The paper outlines important principles and considerations that should be part of best risk management practices for the management of operational risk within an insurance company.

More specifically:

- Sets the principles guiding the development of this operational risk best practice paper
- Defines operational risk
- Describes effective operational risk management, including
  - Operational risk policy
  - Operational risk appetite and tolerance
  - Operational risk identification and assessment
  - Operational risk monitoring and mitigation
- Describes the need for expert opinion in measuring operational risk

3. Guiding Principles

The CRO Forum believes the following principles underlie the establishment of best practices for the management of operational risk within (re)insurance companies. Each of the principles is developed more fully in the remainder of the paper.

Principle 1: Operational risk management within context

Operational risk, like all other risk management functions, should be designed in accordance with the strategy, organisation, product, distribution and the other unique characteristics of a (re)insurance company.

Principle 2: Operational risk should be managed within defined risk tolerance

Senior management should articulate a risk tolerance for a (re)insurance company and the operational risks should be managed in line with the tolerance.

Principle 3: Operational risk management is forward-looking

Management of operational risk is forward-looking and focuses on pro-actively identifying, analyzing, assessing and evaluating the organization's readiness for potential operational risk events (including extreme events).

Principle 4: Operational risk management includes risk mitigation objectives

Significant operational risks that threaten the company's business objectives and its franchise value should be managed through mitigation activities and monitored actively.

Principle 5: Operational risk management is embedded in the business and its culture

A (re)insurer is exposed to operational risk in each significant business process and this should be reflected in its business practices and culture.

Principle 6: Operational risk measurement and management considers different data sets and scenarios

Effective operational risk measurement and management considers different data sets, both internal and external to the organization, and scenarios. Lessons learned from these events and scenarios are considered in line with the forward-looking nature of principle 3.

Principle 7: Transparent relationship between operational risk management and operational risk measurement

Companies should, to the extent it is possible, be able to describe the relationship between operational risk management and measurement. Measurement, if any, should take into account the strength of risk mitigating activities and diversification across risk categories, lines of business and/or geographies.

4. Operational Risk Definition

Operational risk can be defined as the risk of loss, resulting from inadequate or failed internal processes, people and systems or from external events.

This definition highlights the four causes or sources of operational risk events, being inadequate or failing:

- Processes
- People
- Systems
- External events

For reporting and analysis purposes, companies will also need to classify the operational risk events that may occur. This classification may distinguish different operational risk event types such as fraud, business practices, business disruption and employment practices. We believe it is important that the classification of events satisfies management information needs within the specific context of the organization to facilitate that operational risk reporting is used for real business decisions. Similarly, (re)insurance companies will need to further apply operational risk definitions and scoping of the operational risk management function in line with their unique circumstances, such as the company's strategy, objectives, organizational structure and overall enterprise risk management efforts, but also taking into account external factors such as the business and regulatory environments in which the company operates. This explicit consideration for context facilitates inclusion of and appropriate focus on significant operational risk causes and events for the company.

Principle 1: Operational risk management within context

Operational risk, like all other risk management functions, should be designed in accordance with the strategy, organisation, product, distribution and the other unique characteristics of a (re)insurance company.

Operational risk events can result in different types of losses, including mainly:

- Financial loss
- Reputation damage

Next to this, causal analysis of operational risk events may highlight inefficiencies and even lost opportunities for the company. This analysis is crucial to change the culture of operational risk management from being reactive and a burden to pro-active and a benefit to the company.

5. Operational Risk Management

This section first covers the operational risk policy that outlines the scope and definitions, the overall operational risk management approach of the company, roles and responsibilities with respect to the company's tolerance for operational risk. We then move towards a description of the key components of an operational risk management framework, being operational risk identification, assessment, monitoring and mitigation. With regard to operational risk reporting, we suffice with pointing out that the presentation and classification of operational risk information should facilitate the use for real business decisions.

5.1 Operational Risk Policy

If a company does not exercise sufficient and regular assessment and monitoring of operational risk events that may occur, it may experience significant losses affecting the profitability or even solvency of the undertaking. In order to guard against this, and in keeping up with good risk governance practices, (re)insurance companies develop written operational risk policies that are approved by senior management and the operational risk management function ensures implementation within all operating levels.

An operational risk policy should outline the scope and definitions, the overall operational risk management approach of the company, and the roles and responsibilities with respect to operational risk management. The policy should describe minimum standards that the company must meet to consider itself to be adequately protected from operational risk and also the minimum frequency of related risk assessments, monitoring and measurements. As noted, not all (re)insurance companies will address these points in the same way given their context. What is critical is that the company's management is convinced that the specifics of its operational risk policy are appropriate given its own unique combination of business objectives, processes, products, distribution channels and applicable regulations.

5.2 Operational Risk Tolerance

Operational risk will generally be tolerated if it is inherent to conducting (re)insurance activities and supports the realization of business objectives.

Principle 2: Operational risk should be managed within defined risk tolerance

Senior management should articulate a risk tolerance for a (re)insurance company and the operational risks should be managed in line with the tolerance.

In practical terms, risk tolerance is the level of risk beyond which management action will be triggered. If a risk has been identified and assessed to be beyond management's risk tolerance, an appropriate risk response should be developed and implemented. In case of an operational risk event that is beyond management's risk tolerance, a root-cause analysis would be conducted and an appropriate risk response developed and implemented.

5.3 Operational Risk Identification and Assessment

There are many different methods employed by (re)insurance companies to identify their operational risks, but one of the most common starting points is the development of a risk assessment methodology. This raises and maintains operational risk awareness throughout the company while documenting (the nature of) the operational risks the company is facing. Whatever techniques are being used, it is important that the risk identification process is forward-looking and not only based on past experience. To facilitate this, companies can identify and assess their risks in light of their strategy and against objectives defined for business areas. Appropriate risk responses should be defined in case risks have been identified and assessed to be beyond management's risk tolerance.

Other techniques that (re)insurance companies may use for identifying risks timely include analysis of external data, 'near misses' and indicators for operational risk and control failures at the operating level. Audits and other reviews by different functions may further highlight failures in process, people and systems or from external events that may result in increased operational risk and trigger management actions.

Forward-looking operational risk identification and assessments, while applying different techniques as outlined above, implies that operational risks may need to be managed for which the company has no internal loss experience. For example, even if a life insurance company has no significant internal operational risk events with regard to inappropriate sales or marketing activities and related suitability issues, it still should give appropriate consideration to this risk given significant external operational risk events in this area. This principle requires the inclusion of expert opinion in the risk identification and risk assessment processes of the company.

Principle 3: Operational risk management is forward-looking

Management of operational risk is forward-looking and focuses on pro-actively identifying, analyzing, assessing and evaluating the organization's readiness for potential operational risk events (including extreme events).

Separate attention will need to be given to tail events as their identification and assessment could require specific operational risk management techniques, generally involving expert opinion and external data. Developing scenarios is a popular way of understanding the organization's readiness for extreme operational risk events and in case of significant business disruption thinking through the related business continuity planning and testing.

5.4 Operational Risk Monitoring and Mitigation

The significant risks identified need to be monitored actively. Status overview of risk responses need to be prepared for management review on a periodic basis. Next to this, (re)insurance companies will usually implement and report upon indicators for operational risk failures at the operating level. Appropriate mitigation techniques in relation to significant risks identified need to be formulated and their effectiveness periodically evaluated. Mitigation techniques should either prevent the operational risk event from occurring or limit or reduce its impact if it does occur.

Principle 4: Operational risk management includes risk mitigation objectives

Significant operational risks that threaten the company's business objectives and its franchise value should be managed through mitigation activities and monitored actively.

To be fully effective, operational risk management should be integrated in all significant business processes including but not limited to product development, sales, underwriting, investments and claims. The risk mitigation realized and the information produced by operational risk related activities should be genuinely relevant for (use within) the business, beyond generating input for operational risk measurement and external reporting.

The company should further recognize that all employees can cause operational risk events, unlike other risk categories such as mismatch risk and investment risk that are within the circle of influence of a relatively small part of employees. This makes operational risk control a significant challenge and implies that line management should be directly responsible for managing operational risk consistent with the company's operational risk policies and guidelines.
Practices supporting this principle would include risk self assessments, formalized management reviews, training programs focussing on limiting human failures and maintaining operational risk awareness throughout the company, and combining reporting about the operational risk profile with performance related management information at the operating level.

Further, senior management should promote a strong risk culture through communicating sound business principles to all employees and living up to these principles in practice when faced with adverse events or circumstances. Line management should promote a strong risk culture in particular through maintaining internal control standards intact in any circumstances.

Principle 5: Operational risk management is embedded in the business and its culture

A (re)insurer is exposed to operational risk in each significant business process and this should be reflected in its business practices and culture.

6. Operational Risk Measurement

Operational risk can be measured through proxies or an internal model. Proxies will in many cases not truly reflect the operational risk profile of the company and we believe that sufficient conservatism needs to be built in the model in case a (re)insurance company measures its operational risk in this way given the limited analysis to support the figures. Only a risk-based internal model can reflect the risk profile of the undertaking and the strength of its internal controls. We believe that an internal modelling approach needs to take into account the relevance of all data elements: internal operational risk events, external operational risk events, expert opinion regarding scenarios and risk and control self assessments. Given differences in the context of companies as outlined different times above, (re)insurance companies may have a different focus on using data or scenarios and the selection and weighting of the different data elements in their risk measurement. Each company must be able however to transparently substantiate their modelling and data element choices. The quality of modelling work depends on the quality and consistency of the data that can be obtained.

Principle 6: Operational risk measurement and management considers different data sets and scenarios

Effective operational risk measurement and management considers different data sets, both internal and external to the organization, and scenarios. Lessons learned from these events and scenarios are considered in line with the forward-looking nature of principle 3.

We note though that industry experience of operational risk modelling seems to be evolving towards a hybrid approach, encompassing a mix of hard data (internal and external losses) and scenario analysis. In practice, we believe that a range of operational risk data should be considered in developing a forward looking operational risk capital model. Sound model building includes procedures for model validation, which not only increases the reliability of the model, but also promotes improvements and a clearer understanding of a model's strengths and weaknesses around management and user groups.

The operational risk management framework should ensure appropriate alignment between operational risk management and measurement. Risk management and risk measurement needs to be linked allowing taking into account the strength of mitigation activities and providing incentives for strong operational risk management. Further, we believe that diversification benefits for operational risk are substantial and should be recognized across the entire undertaking, all lines of business and risk categories.

Principle 7: Transparent relationship between operational risk management and operational risk measurement

Companies should, to the extent it is possible, be able to describe the relationship between operational risk management and measurement. Measurement, if any, should take into account the strength of risk mitigating activities and diversification across risk categories, lines of business and/or geographies.

A particular issue with operational risk modelling is that boundaries between operational risks and other risks are not clear-cut and can vary across organizations. Boundary issues between operational and other risks need to be transparently resolved and soundly substantiated by the company. Key is that the organization ensures all significant risks are included in its internal models for calculating its required capital.

7. Conclusion

In conclusion, we offer this best practices paper as an industry guide for discussing how operational risk management and measurement can be shaped in practice. The agreement to a common set of principles will facilitate the further development and implementation as we all will have a common basis upon which to continue building industry efforts in this relatively young risk management discipline. It is our hope that this contribution will strengthen operational risk management practices in the (re)insurance industry and improve the knowledge of operational risk professionals globally.

Recent publications of the CRO Forum

Internal Model Admissibility
30 April 2009

Insurance Risk Management Response to the Crisis
17 April 2009

Internal models benchmark study
30 January 2009

Addressing the pro-cyclical nature of Solvency II
25 November 2008

Public risk disclosure under Solvency II
17 November 2008

CRO Forum QIS4 Benchmark Study
31 October 2008

Liquidity Risk Management
29 October 2008

Members of the CRO Forum

CRO FORUM

The CRO Forum is supported by a Secretariat that is run by

KPMG Advisory N.V.
Burgemeester Rijnderslaan 20, 1185 MC Amstelveen or
PO Box 74500, 1070 DB Amsterdam
The Netherlands
Tel. +31 (0) 20 656 8283
Fax +31 (0) 20 656 8225
www.croforum.org