Principles of Operational Risk Management and Measurement

September 2014

CRO FORUM

Table of contents

Introduction

The 2014 White Paper on Operational Risk is an update to the 2009 CRO Forum White Paper. The primary objective of the 2014 White Paper is to highlight the development of operational risk in the insurance industry and of the regulatory framework Solvency II. The 2014 White Paper will summarize the important principles and considerations that should form part of the best practices for the management of operational risk within an insurance company. Additionally, a section dedicated to the measurement of operational risk has been introduced with the notion of providing guidance and considerations to the quantitative aspect of operational risk. The premise of this White Paper is to present principles of operational risk management whilst maintaining focus on the important aspects of the quality of business and risk management processes.

The White Paper is intended to be in all aspects proportional and thus applicable for both larger and smaller insurance companies. Insurance and Reinsurance companies differ from banks not only in respect of the business model, but also in respect of the risk profile. The latter is true for the high level risk classes, where insurance companies are assuming "insurance risk" with their balance sheets, it is also true for the overall composition and weighting of the various operational risks faced by insurance companies[1].

Unlike market or credit risks where risk exposures are managed centrally, operational risk cannot be managed centrally and is the responsibility of every employee. As a result, robust operational risk management requires an appropriate governance structure and sponsorship of the executive management committee, accompanied by the right "tone from the top". Especially effective operational risk management is gained through the early involvement of the subject in senior management activities and decision making processes.

[1] Where this document refers to "insurance companies" it also implies that it is valid for both direct insurance companies and reinsurance companies.

Executive summary

Updating the 2009 White Paper on operational risk management was becoming necessary because of the substantial developments of the insurance industry in recent years. Whilst early adopters of this discipline were looking to the banking models of operational risk, it was becoming clear that insurance companies had to develop their own understanding and models to measure and manage this risk. The first part of this paper describes the principles for effective operational risk management in the insurance industry.

Insurers look to all industries to study their risk classes and risk profiles in order to implement what makes sense. Although they have largely adopted the same definition of operational risks, the risk profiles of the insurance industries are different. This is especially true as regards defining the insurance boundary event. However, a common issue is that responsibility for the awareness and mitigation of operational risk lies with every employee. Usually only a few individuals can expose insurance companies to extreme losses from insurance, financial, market or credit risks. In the case of operational risk, excessive exposure can be caused by any resource that the internal processes rely on to be executed (people, systems, infrastructure, etc.).

To embed such risk awareness and culture it takes senior management commitment, a strong and clear "tone at the top" and defined roles and responsibilities for management and employees in the business, risk management, independent assurance and audit functions. In addition it takes a robust framework, which includes all elements from identification, measurement, monitoring through to control & mitigation activities as well as business resilience and continuity processes.

Embedding operational risk management into all processes of the end-to-end value chain is a key element and because of this it is important to involve senior management early in decision making processes. The quality of the business and risk management processes drives the effectiveness of the operational risk management framework.

The second part of the document dives deeper into the topic of the measurement of operational risk. This paper focuses on the scenario based approach and elaborates on the requirements and practices needed to support this method. This focus is not meant to suggest the superiority of this method above other approaches; it has been selected because it is recognized that a number of insurance companies use this method.

Risk measurement is also a vehicle for embedding risk culture into the organization, by allowing the prioritization of risk mitigation options and by confirming that exposures to risks are within the accepted level of tolerance of the organization. More generally, it also allows for more efficient deployment of capital and assures capital adequacy allocation.

The key to the scenario-based approach is the identification, assessment, challenge and validation of the relevant scenarios through expert judgment, supporting factors and senior management sign-off. The clarity and the understanding of the chosen scenarios and appropriate governance around the process help ensure the necessary credibility.

As with many things, operational risk management and measurement require continuous improvement of the process and properly skilled people in the risk organization, in order for it to be effective and successful. Measurement of operational risk is not about finding the exact truth; it is about finding a reasonable numerical assessment with the aim to support the quality of (risk) management decisions.

Part A: Best Practices

The practices presented in this part of the paper are all related to each other, and should not be viewed in isolation.

A1. Definition

Practice 1: Adopt a broad scope for the management of operational risk

According to global regulatory authorities, operational risk is generally defined as "the risk of loss due to failed or inadequate internal processes, systems, people and external events." The definition includes legal and compliance risk but excludes strategic and reputational risks. This also represents the basic definition for the measurement of operational risk, e.g. calculation of required capital for operational risk.

As operational risk events can also lead to adverse consequences (beyond a pure loss) on business outcomes, it is important to capture the scope of these operational risk impacts beyond those generating financial operational risk losses. Therefore, a broader definition for the management of operational risks reads as:

"*The risk of loss or other adverse consequences on business outcomes resulting from failed or inadequate internal processes, systems, people and external events.*" This definition includes legal and compliance risk but excludes strategic and business risks.

The broader definition of operational risk provides for a more comprehensive assessment of risk across financial, operational, regulatory and reputational impacts to the business. Examples of various impacts that operational risk event can lead to include: unintended economic losses or gains, negative publicity, consumer detriment (conduct), censure from supervisory agencies, operational and business disruptions, damage to customer relationships and heightened regulatory scrutiny.

Possible reputational impacts following an operational risk event should be assessed as part of the operational risk management process. As a consequence of this definition, operational risk is inherent in all insurance products, activities, processes and systems and the management of such risk is a fundamental element of an insurer's risk management program. In addition, activities or processes outsourced to third party service providers should be considered in the operational risk framework of the organisation.

There are different root causes of operational risk. Some illustrations include the following:

- *Internal processes*: failure in the design and execution of core insurance and support processes such as sales and marketing, underwriting, policy issuance, customer billing and premium collection, reinsurance placement, claims payments, actuarial reserving and outsourcing processes;
- *Systems*: inadequate data and security protections, weak access controls, unstable and overly complex systems, lack of adequate testing prior to production, deficient systems/tools;
- *People:* human errors, fraud, unmanaged staff turnover, overreliance on key personnel, unmatched skills to job requirements, inadequate management oversight;

- *External events*: natural disasters (floods, fires, earthquakes, etc.) as well as man-made disasters (terrorism, political and social unrest) may impact the ability to operate on an ongoing basis; changes in the regulatory environment including new regulations.

Note: 'Insurance boundary events' often stem from other risk events (insurance, market, credit) that are caused by operational failures in people, process, systems and/or from external elements. It is recommended for insurers to consider all boundary events for their management of operational risk.

A2. Governance and risk culture

Practice 2: Ensure a strong "Tone at the top" – the boards role

Operational risk governance sets the "tone at the top" that is necessary to embed a strong risk management culture throughout the organisation. It should also promote adherence to the risk tolerance defined by the board or any other administrative, management or supervisory body (AMSB), while pursuing corporate objectives and adapting to the changing regulatory and market environments.

The AMSB should play a key role in establishing a robust operational risk management practice across the organization, with the need to:

- Embed a strong operational risk management culture throughout the organization;
- Establish, approve and periodically review the framework for operational risk management (FORM);
- Monitor and approve the capital allocated to operational risk versus the risk profile of the insurer;
- Oversee senior management to ensure effective implementation and communication across the organization; and
- Approve and review the risk tolerance.

The risk culture of an insurance company should foster an open dialogue of risk issues at all levels with the appropriate reporting and escalation of the most significant risks. The organisation's management should determine which risks it will choose to mitigate, transfer or accept according to the company's overall risk appetite and tolerances.

It is important to understand that operational risks can be triggered by any employee of the company, whereas only a finite number of individuals can expose the firm to other risks such as insurance risks, financial risks like market- and credit risks. Risk awareness and monitoring of compliance with corporate policies and standards should be implemented across the entire company. Therefore it is important that all employees have an understanding of the sources of operational risk within their day-to-day working environment. For this purpose, risk awareness programs together with operational risk policies and procedures play an important role.

Practice 3: Implement risk tolerances for operational risk

Operational risk is seen as a risk that cannot be avoided and comes as a consequence of doing business. From a semantic point of view, rather than setting an appetite, practitioners speak of setting a tolerance for operational risk.

Defining tolerances for operational risk is a key step in building a robust operational risk management framework. The tolerances serve to monitor and manage operational risk, by setting the limits and boundaries that will alert the governance structures to levels of exposure (up to and) beyond which management action needs to be triggered. Therefore, it is important that risk

tolerances and limits for operational risk capture, as far as possible, the type and nature of the activities run by the insurance companies. For different categories of operational risk, different tolerances may apply, e.g. internal fraud, business continuity, etc

Risk tolerances should allow the balancing of local and global views of managing risk. This can be a complex endeavour considering the diversity of business activities and countries in which insurance companies can operate, as well as the complexity in modelling operational risk drivers and compiling representative, historical event sets. One solution to consider, therefore, is to adopt different metrics to define exposure and tolerance to operational risk.

Risk tolerances should be measurable, even if based on qualitative assertions for the maximum acceptable risk. Insurance companies typically set limits for the amount of capital it accepts. Depending on how sensitive the measurement of the capital charge is to operational risk drivers (standard formula as opposed to internal models), it may need to be complemented by other, non-capital related measures, in order that management actions can have an effective impact on exposure. Insurance companies may, for instance, develop scorecard operational risk self-assessment tools. Such tools, centred around drivers, can assess exposure to operational risk, and produce qualitative scores on which limits can be set. Other organisations may set limits to key risk or key performance indicators (e.g. staff turnover, budgeted losses, etc.) where they are reasonably satisfied that the indicator serves as a good proxy for exposure to drivers or effects of operational risk.

Measures developed at group level may be insufficient in capturing local requirements, leading local management to complement group frameworks (minimum standards) with measures developed to meet local business needs (including local regulation). Typically, where a loss data collection process is in place and used for both capital calculation and risk management purposes, the threshold set for reporting losses to the group operational risk function may be too high for the management teams of a subsidiary. In this case, local management may be required to set a lower threshold more appropriate to their size and complexity.

Therefore, it is sound practice that the AMSB, at group and/or local level, should approve and review operational risk tolerances, to ensure they are consistent with the overall framework and local needs for managing the risk. Thus giving senior management at all levels the remit to develop governance mechanisms appropriate for the size and nature of the activities (monitoring, escalation etc.) relating to the approved risk tolerances.

Guidelines

- Recognize a level of operational risk tolerance in the risk appetite framework that is commensurate with the fulfilment of business objectives helps to place focus on the management of the risk;
- Define tolerances that are measurable and allow for active monitoring;
- Define tolerances that capture the type and nature of the activities run by the insurance companies allow for active monitoring;
- Consider, given the complexity in establishing a universal measure, more than one measure to define operational risk tolerance (group versus local considerations); and
- Use both group and local metrics to capture local business specificities, but ensure that both are complementary /consistent.

Practice 4: Define clear roles and responsibilities for operational risk management capabilities

As part of an effective operational risk management framework, roles and responsibilities are defined according to the three lines of defence concept:

1. All employees of the organization have the primary responsibility of managing operational risk, and adopting the control framework as an inherent part of their day-to-day job (first line of defence role).

2. The oversight functions should have dedicated resources in charge of defining and maintaining the methodology and framework for operational risk (second line of defence role). Senior Management needs to ensure that there is a sufficient pool of, skilled (risk management as well as business knowledge) and trained resources available. Main responsibilities should include:

   – Advising senior management to identify operational risks and establish an effective risk based internal control system;

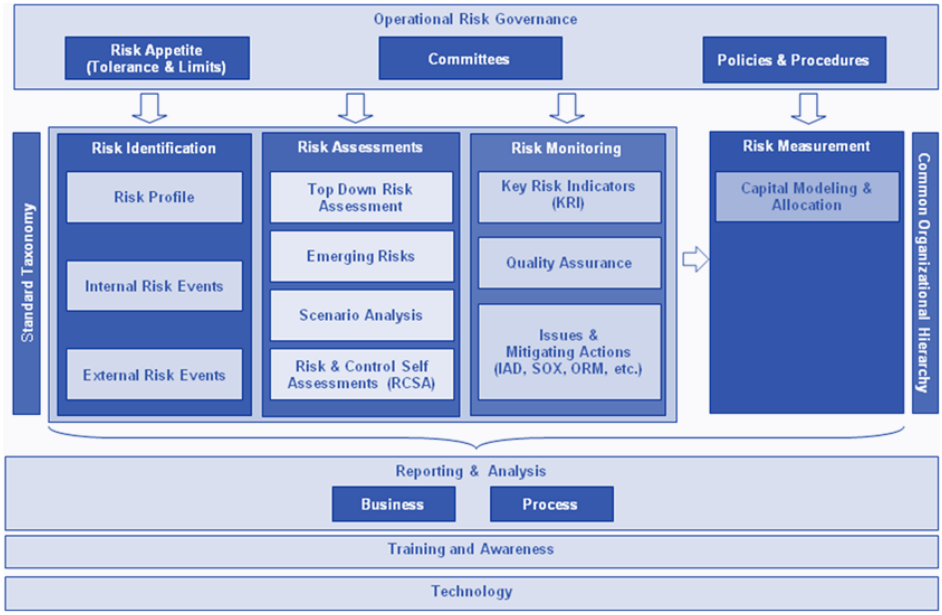
   – Providing challenge and oversight to senior management validating that the internal control system is operating effectively across the company; and

   – Implementing clearly defined policies and standards.

3. Internal audit provides an objective and independent assessment of the operational risk framework including risk management activities performed in both the first and second lines of defence (third line of defence role) as well as validation through independent testing.

A3. Framework for operational risk management

Practice 5: Embed robust risk identification and assessment processes



The objective of the risk identification and assessment process is to articulate operational risk exposures using probability/impact techniques, to support the prioritisation of resources in the mitigation of these exposures. The scope of the identification and assessment process should be forward looking and cover the end to end business process, including outsourcing arrangements. Internal and external data should be utilised where possible to ensure learning and thematic risks are considered from across the industry.

A risk profile is defined as an evaluation of a firm's willingness to take risks, as well as the threats to which a firm is exposed, given a firm's risk tolerance. Significant changes to the business environment should trigger a reassessment of the risks, so it delivers a more dynamic risk insight.

While it is recognised different techniques can be utilised to perform identification and assessment, a key success factor is delivering an integrated view of the risk assessment, drawn from different sources of data, including historic and forward looking assessments. Presentation of risk exposures on a probability/impact matrix to provide a risk profile is useful in ensuring that a clear view of risks is understood in order to support an appropriate treatment in mitigation, escalation and reporting.

Three approaches can be utilised to deliver an aggregated and holistic view of risk exposures:

a) *Loss data collection and incident management*

To improve the assessment of the overall risk profile, internal loss data can provide useful management insight in identifying risks, understanding root cause and assessing control adequacy. The collection of loss data should also capture information not usually obtained for pure measurement reasons, such as opportunity costs and reputational risks, albeit they may not be entirely quantifiable.

In order to complete the picture of information supporting risk identification and also the decision making process, external loss data can be effectively integrated with internal loss data. This provides senior management with elements for considering low frequency, high impact events, which have impacted other companies in the industry. Loss data consortia across the industry may provide useful benchmarking and insights. In addition, external operational events should be monitored through media comment to consider potential unidentified risk exposures and lessons learned.

b) *Top-Down Risk Assessment*

The business strategy of the firm is key in providing a forward looking focus to assess the potential changes to operational risk exposures and also their potential constraints to delivering that strategy. This strategic view should also recognize the changing external environment (e.g. technological or regulatory changes, macro trends). This approach should also include consideration of emerging risks in order to assess the proximity of new risks to the organisation.

It is also important that senior management assesses and monitor the operational risk capability and the risk culture of the firm in order to identify where operational risk exposures are more likely to crystallise.

Scenario analysis is a technique/tool to obtain expert opinion to identify potential operational risk events and assess their potential outcome. Focusing analysis on 'low probability, high impact' scenarios is useful to complement the risk and control self-assessment which will focus on more frequent events of lower impact. Scenario analysis should draw on risks identified through top-down assessments and the integration of external and internal data to support expert judgment. Completion of scenario analysis should inform mitigating actions and additional control requirements, and can potentially be used to inform strategy and business planning. In view of the expert judgment being used, a robust governance framework is required to support scenario analysis and reduce biases and subjectivity. Scenario analysis can be used to support business resilience plans (see Practice 10) and also measurement of operational risk from a capital perspective (see Part B of the paper).

Combining these views in an overall top down assessment for senior management can then be used to frame the context of the bottom up risk assessment as detailed below.

c) *Bottom-up Risk Assessment*

The business managers and their reporting lines have the primary responsibility to identify and assess risks inherent to their activities and processes. They should consider the current environment and also potential changes driven by strategic direction. They should perform this assessment using an integrated risk and control self-assessment that will cover, on a risk based approach, key operational risk categories and end to end processes in order to gain a holistic perspective of operational risk exposures.

Operational risks should be assessed in terms of probability and impact. Various dimensions to assess the potential impact of the risks may include, for example: customer detriment, financial loss, financial misstatement, regulatory impact, reputational impact and cost/complexity of resolution.

The following input can be considered within risk identification workshops: internal and external audit issues, regulatory issues, key risk indicators, near miss experiences, loss experience (both

internal and external), operational capabilities and risk culture. Residual risks should be assessed following the articulation of appropriate controls and their respective design adequacy and operating effectiveness (see Practice 9).

The identification, escalation and management of risk events (losses and near misses) are an integral part of a robust identification and assessment of operational risk.

Practice 6: Embed operational risk practices in taking key decision-making across the organization's value chain

In general, operational risk exposure may increase when insurance companies engage in new activities, develop new products, enter unfamiliar markets, implement new business processes or technology systems, and/or engage in businesses that are geographically distant from the head office. Moreover, the level of risk may change when new product activities, processes, or systems progress from an introductory level to a level that represents material sources of revenue or business-critical operations. The insurance company should ensure that its risk management infrastructure is appropriate and that it keeps pace with the rate of growth of, or changes to, products activities, processes and systems.

Insurance companies should embed operational risk practices (reviews, challenge, assurance) in decision-making of strategic change initiatives, new products, transaction reviews and due diligence activities. Such practices should consider:

- Changes to the operational risk profile and risk tolerance;
- The necessary controls, risk management processes, and risk mitigation strategies;
- Changes to relevant risk thresholds or limits; and
- The procedures and metrics to measure, monitor, and manage operational risk.

The operational risk practices should also ensure that appropriate investments have been allocated for human resources and technology infrastructure as part of the decision making process. The implementation process should be monitored and fed back into the risk management framework in order to identify any material differences to the expected operational risk profile, and to manage any unexpected risks.

Practice 7: Embed Robust Measurement Process

Risk measurement is a core component of a sound operational risk management framework that informs senior management decision-making, analyses the impact of these risks on the company's capital needs and helps to set operational risk tolerances. It can also serve as a tool to promote risk culture and effective risk management.

Operational risk can be measured through proxies or via an internal model. Proxies in many cases do not truly reflect the operational risk profile of the company, and are therefore difficult to base the risk management framework on. We believe that a risk based internal model can better reflect the risk profile of the undertaking and the strengths of its internal controls.

To be robust, an internal modelling approach should take into account the relevance of all data elements: internal operational risk events, external operational risk events, assessment of operational risk management processes, expert opinion regarding scenarios and risk and control self-assessment.

Given differences in the size and complexity of organisations, 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 methodology. Each organisation must be able, however, to transparently substantiate their modelling and data element choices.

Sound internal model building includes procedures for model validation, which not only increase the reliability of the model, but also promote improvements and a clearer understanding of a model's strengths and weaknesses around management and user groups.

The principles to quantifying operational risk are developed in Part B of this document.

Practice 8: Embed risk monitoring process

The regular (and focused) monitoring and reporting of operational risk exposure is based on a comprehensive risk profile, including all relevant data (management information).

Monitoring will allow an organisation to quickly respond to any change in business development (internal or external) or other dynamics (including emerging risks) and assist in the effective and efficient operation of the business. It includes the periodic verification & validation of the quality of business processes and key controls.

Monitoring should reside within the clearly defined roles and responsibilities (practice 4), with the output being reflected in the risk reporting.

Guidelines:

- Clearly articulate a risk tolerance (appetite) prior to implementing an effective monitoring process;
- Have consolidated key risk and control registers to allow for an effective risk monitoring environment;
- Complete the monitoring process on a regular basis depending upon the frequency that the controls allow or require;
- Use Key Risk Indicator (KRI) to provide either early warning or detective signals to highlight potential issues to management in a timely fashion;
- Use various approaches to conduct monitoring, dependent on the type of key control, e.g. process walkthroughs, workshops, interviews, document research, or subject matter expert (SME) opinion;
- Have a methodology in place to ensure risks across the overarching operational risk framework have been considered and where exclusions have been made with supporting evidence for that exclusion;
- Perform monitoring exercises that result in documented results leading to improvement actions where necessary. These actions should be assigned to relevant business process owners for implementation and closure; and
- Feed back the combined monitoring efforts into a central risk management dashboard to enable effective reporting to senior management.

Practice 9: Implement a robust internal control system

The internal control system of the organisation is a key element in the framework for operational risk management[2] and the underlying business processes. Organisations should have a robust control environment based on policies, processes, systems, skills and capabilities. The use of an Enterprise Risk Management framework (e.g. COSO) is recommended for this purpose.

An internal control is a tool to prevent or manage the potential impact of a failure in a firm's policies, processes, systems, skills or capabilities.

Internal controls should be designed to provide reasonable assurance that a firm will have efficient and effective operations, safeguard its assets; produce reliable financial reports; and comply with applicable laws and regulations. A sound internal control programme comprises of five components that are integral to the risk management process:

- Control environment;
- Risk assessment;
- Control activities;
- Information and communication; and
- Monitoring activities.

Key controls may be automated or manual depending on the business process, but in each case they must be clearly documented.

A firm should ensure that it has a relevant level of competency within the organisational structure to ensure a clear understanding of the risks it faces within its business processes to enable it to achieve the goals of all stakeholders.

In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management can complement controls by seeking to transfer the risk to another party such as through insurance. The AMSB should determine the maximum loss exposure the firm is willing to have and should perform an annual review of the firms risk and insurance programme. While the specific insurance or risk transfer needs of a firm should be determined on an individual basis, many jurisdictions have regulatory requirements that must be considered.

Because risk transfer is an imperfect substitute for sound controls and risk management programmes, firms should view risk transfer tools as complementary to, rather than a replacement of, thorough internal operational risk control. Having mechanisms in place to quickly identify, recognise and rectify distinct operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, transfer the risk or activities, or create a new risk.[3]

[2] May also be a part of other financial risk frameworks

[3] Risk transfer taken from the BIS publication June 2011 "Principles for the Sound Management of Operational Risk"

Practice 10: Embed business resiliency and continuity processes

The importance of business resilience and continuity planning demands understanding at senior management and board level, and appropriate investments in line with the risk profile and appetite of the firm. There is a basic requirement for firms to have business continuity plans and disaster recovery to maintain key operations. However, the objective is also to protect the company's resilience over the long term and ensure it can respond to the changing business environment. This will ensure the firm can meet short term and long term commitments to clients and deliver value to all stakeholders.

Insurers should regularly test and update business resiliency and continuity plans, to ensure an ability to operate on an ongoing basis and limit losses and other adverse impacts of severe business disruption. To truly embed resilience and continuity processes within the firm, there is a need to define critical systems and business processes across the end to end operating model, including outsourced activities and reliance on external suppliers. It is important to give consideration to business units and/or outsourcers/suppliers located within diverse geographic regions which may face political, environmental and regulatory exposures of a different nature.

It is essential that continuity plans and recovery strategies are regularly tested by business people in order to ensure they operate effectively and lessons learned from testing are embedded. In addition to financial and operations impact, testing should include an assessment of customer impact and remedial activities. The testing should include the identification of contingency in case of a stressed environment and consideration of contagion risk in a crisis situation. Governance, accountability and escalation requirements need to be clearly communicated across the firm.

Crisis management must be integrated into the overall response plan to disruptive events - with pre-planning of support for immediate communication strategies recognising the impact of social media and speed of response expected from key stakeholders. This is essential to mitigate reputational impact.

Scenario analysis can be used to focus attention on resilience over the longer term and have plans in place to respond to the "unexpected" in order to mitigate the impact of low probability, high severity events.

Part B: Quantification

B1. Introduction

In order to manage operational risk effectively, organisations need to introduce some form of measurement. This requires a full understanding of the risks insurance companies face in running their business and of the impacts of these risks on the company's capital needs. Therefore quantifying operational risk is important: as it sets a metric which is easily understood by business managers, allows for comparison with other risks and makes its impact on business clearly defined. Quantifying is also a way to establish a base upon which it is possible to make a projection through time from a capital requirement perspective, so complying with ORSA's requirements.

The Solvency II regulations provide an approach to the measurement of operational risk from a capital perspective, currently represented by the 'Standard Formula'. This is a basic metric designed to be applicable to any company; it considers operational risk as inherent to insurance business and directly connected to the typical economical dimensions of the business itself e.g. earned premiums or technical provisions. Rather than using the standard formula, a company can also use an internal model for the quantification of operational risk. Based on the financial services industry's current level of knowledge and experience, this encompasses the use of data such as internal (and external) losses, scenario analysis and other approaches based on processes and control analysis.

The remainder of the paper will focus on the use of internal models for the quantification.

Data from incurred losses provides information on past events that actually occurred in the company (or to competitors). As with any historical series, the challenge of maintaining the suitability of operational loss data through time or ensuring that it is representative of all company activities, raises some issues. Scarcity of data may affect reliability from a statistical perspective because some operational risk events happen very rarely or hopefully not at all, while the business environment may change significantly in time so reducing the value of historical information.

More generally, loss data informs organisations about the past but needs to be complemented with other types of data to inform us about the future, be it a less risky one (i.e. for better controls in place) or an unknown (i.e. because of a changing business environment).

Results from scenario analysis overcome most of the issues connected to data from incurred losses: it is forward looking, but takes into account the quality of controls that are in place. It can be applied wherever needed in order to complete the coverage of company activities even those scarcely represented in the loss data, and it provides an up to date risk profile. Of course this approach has its challenges too: quality and reliability of the underlying data used to assess the impact of the scenarios is key to producing results that reflect the real risk profile. Scenario data collection is an issue that can be dealt with by implementing a robust framework and leveraging on control processes already in place.

B2. Objectives

The operational risk management framework should ensure adequate alignment between operational risk management and measurement. Both should be linked to allow taking account of the quality of existing mitigation measures and providing incentives for strong operational risk management. Consequently, the process of risk measurement should serve as a tool to promote the risk culture and effective risk management, as the quality of risk management processes and internal controls should be reflected in the quantification of operational risk.

Operational risk quantification supports management in their decision-making processes by providing a deeper understanding of the risks embedded in the activities of the organization, therefore ensuring they can be adequately addressed. It helps management to gain insight in the most important operational risks so that the impact of changes to the business strategy and/or control environment can be properly anticipated.

Some of the key elements supported by operational risk quantification are (but not limited to):

- The prioritized improvement of the processes of managing risks (taking into account the business's existing control environment). This implies either:
  - Confirming that they are in line with the risk tolerance of the organization, or
  - Risk mitigation action. For each significant operational risk, the organisation should ascertain whether the risk-control and risk transfer are optimized in the context of cost-benefit analysis.
- A more efficient deployment of capital, via:
  - Proper resource allocation for existing and/or new business opportunities, determining whether the incremental profits are commensurate with the incremental risk.
  - Capital Adequacy Assessment: to assure 3rd parties (shareholders, supervision, institution clients) that the capital requirement covers all risks up to an agreed confidence level.

B3. Model design

The operational risk model should be understood and documented: key model assumptions and limitations should be easy for internal and external stakeholders to understand (e.g. senior business managers, internal audit and regulators). Model inputs may include loss events, risk, control and process assessments, scenarios and correlations (non-exhaustive list).

Operational Risk modelling should fully leverage the other main elements of an ORM Framework (see section A3) in order to assist in identification of relevant improvement areas and show a clear link to the business and its processes. If applicable, the model design supports an allocation of capital to segments, units, legal entities.

B4. Scenario analysis

Scenario analysis is a tool that allows management to systematically consider the risk of extreme but plausible events. The use of scenarios to capture, assess, manage, and quantify operational risks represents an essential component of a firm's economic capital model.

Scenario analysis is recommended due to the current unavailability of empirical loss data that can be relied on to calculate operational risk capital. The use of scenarios can thus be a more effective way to understand and plan for the effect of operational risk events relevant to a specific firm. This would provide the risk function, management and the AMSB with a sense of what could happen and what its effects might be.

It is best practice to define and manage scenarios with input from various subject matter experts, this ensures scenarios are consistently structured and clear boundaries are drawn between scenarios to avoid overlaps and double counting.

Senior management involvement

It is important that senior management is involved in this process, not only to emphasize its importance to all areas of the firm, but also to provide insight into the risks of the firm.

Scenarios should be intuitively clear and understandable so that non-specialists can make appropriate decisions based on the drivers of the scenarios and their consequences for the firm. It is important that each scenario is documented and supported by a narrative accessible to third party readers without a technical background.

Quantification of scenario analysis

Each scenario should be assessed in terms of severity and probability.

- *Severity (impact)*: An assessment of the cost impact the risk event will have on the operations of the business.
- *Probability (Frequency)*: An assessment of the frequency with which the risk event is likely to occur based on management experience, and previous history.

Probability and severity should be determined with the risk function or unit performing capital modelling; this ensures consistency across the company.

Scenario assessments should consider direct financial impact when assessing the severity and probability of any given risk. This means that the indirect impact with associated costs, such as damage to reputation, loss of revenue, opportunity costs, etc. should be excluded from the quantification of operational risks However, it is important to note that the indirect costs associated with an operational risk event should be included in the management/mitigation of that risk, but excluded from its overall rating.

The outputs of scenario analysis should be appropriately documented, and challenged. They should be quality reviewed and approved by management to mitigate the risk of expert judgment bias and to assess the plausibility and reasonableness of the results.

B5. Model validation and governance

Operational risk is one of the hardest risk types to measure, although it can be measured through proxies or internally developed models. Proxies in many cases do not truly reflect the operational risk profile of the company. Internally developed risk-based models can reflect the company's risk profile. However, the model needs to take into account relevant data elements like internal operational risk events, expert opinion regarding scenarios and where possible output from risk and control self-assessments.

In order to be used appropriately, the model should be clear and understandable and its different components clearly explained to experts and management. Therefore it is key to develop proper validation governance and to understand the limitations of the models. This encourages a proper use the model within the actual scope for which it has been designed, prevents misuse, and ensures appropriate confidence in its results.

This section will present different governance elements to ensure stakeholders are appropriately aware of the main aspects relating to operational risk models and suggest various data elements to be considered to aid a proper implementation of an operational risk model. Validation governance should ensure that inputs, methodology, mathematical and aggregation assumptions and subsequently results of the model are understood and independently validated.

Validation of the inputs

Traditionally, operational risk models (for insurance firms) have been designed and built with incomplete historical data. In most cases, operational risk models are heavily dependent on expert opinions, and it is the experts judgement that has become one of the strengths in the process.

Insurers should aspire to organize a defined set of risk data that is relevant to them and that serves as a valuable input to feed their model. Because insurers may have different levels of operational risk maturity in gathering internal losses they should complement their internal loss data collection with external data. This will enable key stakeholders to have a broader view of the operational risk environment. However, past experience will not predict future losses and past data is often not available on most catastrophic events, it is therefore the expert opinion that will be required to assess the frequency and impact of major operational risks.

The methodology developed to collect expert judgement should be clearly defined to minimise bias as far as possible. As part of validation governance, a second opinion and external studies should be gathered and where possible consulted to strengthen and challenge the assessment on major assumptions.

Validation of the model: mathematic and aggregation assumptions

Actuarial methods with calibration assumptions are used to estimate the capital allocation needed to cover operational risk. For regulatory purposes, assumptions and parameters used in the models must be clearly defined and justified. Model assumptions should also make sense to management, operational risk management and other constituencies to provide credence to the statistical estimations.

As part of model calibration, correlation and aggregation assumptions must be taken, thus instituting a model that is more sensitive to adjust for changes. Considering correlations, the main challenges regarding this approach is identifying and assessing the different components and the impact on the different operational risk categories, and being able to isolate potential dependencies. A validation phase with experts is an option to assess the value of the correlation coefficients. Throughout the process this methodology should be explained to relevant participants to minimize shortcomings as a result of misunderstandings of the overall model input.

It is essential to review the results of scenario analysis to ensure that consistent and defensible estimates and outcomes are delivered. A well-structured and systematic review and validation approach for scenario analysis is crucial to minimize and control any bias driven by the subjectivity of the process.

Validation of the results

An important part of the quality assurance for the operational risk model is an efficient validation process, in particular in light of the aforementioned challenges. Validation of the operational risk model needs to be evidenced and presented to the appropriate level of management with a clear and fair disclosure of the assumptions taken.

The following techniques can be used to give management the relevant insight on the results:

- *Plausibility checks*: The results of the scenario analysis and their annual changes are verified against the backdrop of changes in the business profile and company structure.
- *Sensitivity analysis*: The sensitivity of the operational risk model against the scenario results is assessed in order to find the main drivers of the capital requirement. These findings have to be justified in collaboration with the involved experts (SMEs).

- *Back testing*: Observed historic losses mapped to the defined operational risk categories are used to validate the scenario results. Ideally the internal data basis should be enhanced by relevant external data. If sufficient such a data pool could serve for a correlation analysis as well.

If appropriate the results from the risk assessments within the 'Internal Control System' can be used to validate the scenario results - at least major inconsistencies could be detected.

Different elements can be used at various steps of the model validation process. However senior management should exercise its oversight and challenge role to ensure relevance and accountability is achieved resulting in a comprehensive risk profile.

B6. Application of operational risk management and measurement

Risk measurement can be utilised as a tool to help spread risk culture and awareness into the firm in the pursuit of embedding an effective risk management framework. It should be taken into account in the decision making process for strategic change initiatives, new products or reorganisations. It could also be used to support a company's 'business as usual' processes such as product pricing, capital assessment and resource allocation.

Management decisions should also take into account the mitigating actions and proactive investments that may be in place in order to prevent failures of internal processes, systems, people and external events.

Risk measurement allows the assessment of the effectiveness of potential risk transfer solutions to reduce some risks appropriately to within risk tolerance. Furthermore it allows the comparison of cost and effectiveness of any risk mitigation activity or risk transfer.

Quantifying operational risk is not about finding the ultimate answer, as the underlying data is not based on an exact science. It is about finding a reasoned numerical assessment of the exposure of the organisation to its identified risk profile.

Both the management and measurement of operational risk require continued development of the process and the framework. It requires that risk management teams are appropriately skilled and understand both the business as well as the management of the operational risks. These risk management 'skillsets' should then be utilised to ensure there is a clear alignment between the qualitative framework that has been embedded and the measurement (and subsequent quantification) of the identified risks the organisation is exposed to.

Glossary of terms

Term	Definition
AMSB	Administrative, Management and Supervisory Body. Covers the single board in a one-tier system and the management or the supervisory board of a two-tier board system.
Assurance	Providing an independent assessment based on evaluating the effectiveness of governance, risk management, and control processes. (IIA's 'International Standards for the Professional Practice of Internal Auditing').
Assurance Functions	Functions which provide oversight to ensure an effective internal control framework such as compliance or underwriting quality assurance.
Audit	A formal assessment of a part of the internal control system and other elements of the system of governance, carried out by an independent, qualified function that applies a systematic and disciplined approach, including quality control, according to standards for internal auditing. Audits assess control design and control effectiveness and the related risk management processes.
Board	Board means the board of directors for companies with one tier governance structure and supervisory board for companies with two tier governance structure.
Compliance	Compliance serves in a dual capacity as (i) an enabling function supporting business activities regarding ethical and regulatory compliance, and (ii) a control and governance function providing independent assurance on compliance risk matters to senior management and the boards of directors.
Compliance risk	The risk of civil, criminal or regulatory sanctions resulting in a financial loss, loss of ability to conduct business, or loss of reputation, due to a failure to comply with laws, regulations, rules, related self-regulatory organisation standards, or the Code of Conduct.
Conduct impact	The risk to customers of insurers' controls and operations failing.
Control	Identified activities designed to mitigate intentional and/or unintentional errors or failures in process. Controls may be detective or preventative in design.
Fraud	Fraud encompasses a wide range of irregularities and illegal acts, all of which are characterised by intentional deception.
Internal Audit	Internal Audit is an independent, objective assurance and consulting function that assesses the adequacy and effectiveness of the company's internal control system and other elements of the system of governance, and adds value through identifying opportunities to improve the group's operations. Internal audit helps the company accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. Internal audit provides assurance to the board of directors and, secondarily, to business management (1st line of defence).
Inherent Risk	Inherent risk is the expected and unexpected economic impact of operational events before the effect of internal controls.
Insurance Boundary Event	Insurance boundary events are being defined as insurance events, which are partly or completely caused by operational risk failures or insurance event with an increased financial impact caused by an operational risk failure.
Issue	An identified risk or concern that requires senior management attention, such as monitoring and/or mitigation.
Key Risk Indicators	A monitoring tool to alert senior management to risk levels, control performance, and

Term	Definition
(KRIs)	trending changes that may be indicative of risk concerns.
Operational Risk Management	ORM, as a function, is a second line of defence oversight function. As the independent controller for operational risks arising from the business activities or the external environment, ORM has the mandate to provide assurance for operational risks and controls and to consult and support management in raising awareness about risks and for improving the internal control environment. ORM has responsibilities for risk assessment, assurance planning, review of risk-taking activities, issue monitoring and mitigating action verification, monitoring, reporting and coordination and is the process manager for the measurement of the control related behaviour.
Process	A series of actions supporting the insurance company conducted by either business areas maintaining the day-to-day business operation or the peripheral supporting of control functions.
Residual Risk	Residual risk is the expected and unexpected economic impact of operational events considering the mitigation effect of internal controls.
Risk	Exposure to adverse consequences arising from internal or external changes, actions, events, decisions, and/or circumstances which have the potential to reduce shareholder value.
Risk Acceptance	A transparent and well-informed decision by senior management to accept a level of residual risk, given the control measures in place and resources available. In accepting risk, senior management acknowledges that it is impossible to completely eliminate risk, and at the same time asserts that it has made the best use of existing resources to address its most critical risks.
Risk and Control Self-Assessment (RCSA)	A qualitative assessment of risks related to significant processes on a business-as-usual basis.
Risk Avoidance	A risk management technique whereby risk of loss is prevented in its entirety by not engaging in activities that present the risk (e.g., exiting a product or market).
Risk Controller	Tasked by the risk owner with the oversight of risk-taking activities to mitigate potential conflicts of interest between risk owner and risk taker; as part of his fundamental role, the risk controller is responsible for escalating to the risk owner or a higher level risk controller any decision or issue that he or she might be concerned about.
Risk Event	The materialization of an operational risk that leads directly to (or has the potential to result in) one or more financial or non-financial impacts.
Risk Event Capture	The structured reporting, documentation, and compilation of operational risk event data, thus allowing timely analysis and dissemination of information.
Risk Governance	Risk management governance; that is the act or manner of governing risk management activities.
Risk Mitigation	A series of steps designed to reduce the exposure of an issue and/or the potential re-occurrence of an incident.
Risk Owner	Establishes a strategy and assumes responsibility for achieving the objectives.
Risk Taker	Takes steps to achieve the objectives within a clearly specified authority delegated by the risk owner; it is the duty of each risk taker to inform the relevant risk controller of all facts relevant for the discharge of their duties.
Risk Transfer	Shifting some or all residual risk from one party to another; examples include purchasing insurance coverage or issuing debt.

Term	Definition
Scenario Analysis	An analysis that utilizes the expertise of experienced senior management to identify and estimate financial exposure to low probability events that may have severe impacts (i.e., "tail-end events").
Senior management	The CEO and his direct report, often described as executive committee. For companies with two tier structure, this role will be performed by the "management board".

Disclaimer:

The CRO Forum is supported by a Secretariat that is run by
KPMG Advisory N.V.

Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands

www.thecroforum.org