

An operational risk scorecard approach

Operational risk scorecards have been in the spotlight since the Basel Committee on Banking Supervision's 2001 paper on op risk treatment under Basel II. In the first of two articles, Ulrich Anders and Michael Sandstedt of Dresdner Bank examine what, specifically, these systems seek to accomplish – and what implementing them entails

The analysis of operational risk is a relatively new area, though it is increasingly essential. From market and credit risk it can easily be understood what risk is and how it can be assessed – market risk results from the market portfolio of the company, credit risk results from the credit portfolio of the company.

But what do we want to assess in operational risk? Operational risk is the risk of a loss resulting from inadequacies or failures in processes due to technology, personnel, organisation or external factors.¹ What is being assessed, therefore, is the business processes of the company that are operational therein. Compared with the market or credit portfolios of the company, the business processes of the company could also be called the operational portfolio.

Once we have assessed the business processes of the company, we need to report on the results. The appropriate way to do this is via an operational risk scorecard.

Many reports are called scorecards. They all use scores to reflect a particular situation. For example, the famous Balanced Scorecard² is, in simple terms, a report that scores how a company has implemented its vision and strategy in the areas of finance, business processes, learning and growth, and customers.

An operational risk scorecard is a report that shows the operational risk profile of a company or parts of that company, with the help of appropriate scores. This

scorecard must achieve several goals:

□ Reflect the level of operational risk: this is the primary goal that gives the op risk scorecard its name. The level of risk is determined via an assessment.

□ Explain from where in the organisation the operational risk comes: the scorecard should reveal what the op risk scores are related to, that is, to which part of the organisation, in connection to which products or business lines, which organisational units and which locations of the company.

□ Present what the causes of operational risk are: only when the causes of op risk are presented in the scorecard do people understand how the level of op risk is determined, why it is at the level at which it is reported in the scorecard and how it can be reduced.

□ Reflect the operational quality: the level of risk in an organisation depends on its operational quality, which includes the quality of the control environment. If the operational quality is low, the organisation will face a higher risk of losses.

□ Focus management attention: the scorecard should not only give a status of the op risk and quality level, but also encourage management to undertake actions to mitigate the risk via quality improvements. Therefore, the scorecard must relate the levels of op risk and quality to each other so management can set priorities for their actions.

It is useful to supplement the information provided by the scorecard with loss data³ resulting from operational risk and key op risk indicators⁴ to compare op risk assessments, losses and indicators. This task is usually performed by an operational risk management information system.

Risk and quality

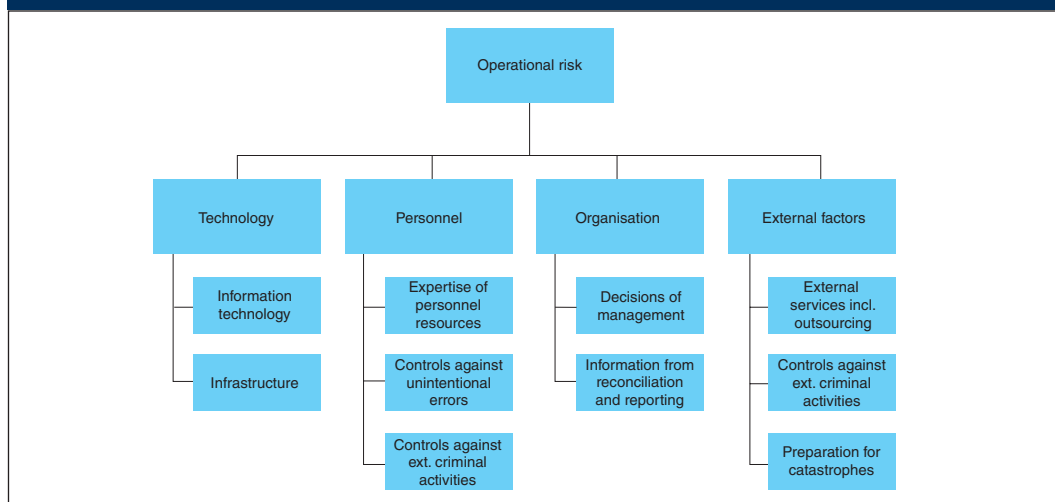
The assessment of operational risk and quality is a difficult task. To explain it we will first consider what risk is and how it is assessed, then what quality is and how it is assessed, before we apply these concepts to the assessment of operational risk and operational quality.

What do we mean when we talk about risk? We mean we could lose something with a certain probability. How much we could lose is called severity, the probability of losing it is called frequency.

If we want to compare risks we must compare the dimensions of risk. For example, driving a motorbike is more risky than driving a car, since on the motorbike the severity of personal damage is usually higher, and accidents also occur more frequently. The risk of one situation compared with another is higher if the loss severity is higher given that loss frequencies are equal, or where the loss frequency is higher given that the loss severities are equal, or if both loss frequency and loss severity are higher.

The measuring units for risk are obvious. The severity dimension needs to be measured in monetary units such as the euro. The frequency dimension can most conveniently be measured in number of

1. Factors affecting business processes



¹ This definition is in principle similar to the Basel II definition, but it distinguishes between where op risk occurs (in processes) and why op risk occurs (due to technology, staff, organisation, external factors)

² Kaplan R and D Norton, 1996, *The Balanced Scorecard: Translating Strategy into Action*, Harvard Business School Press

³ Losses are defined as all extra (out-of-pocket) expenses and financial liabilities as a result of a loss event. Losses due to op risk are caused by inadequacies or failures of technology, personnel, organisation and external factors (such as external suppliers)

⁴ Key risk indicators are defined as parameters resulting from business processes or areas, and are assumed to be predictive for changes in the op risk profile of these processes or areas

⁵ ISO 9000:2000, *Quality management systems – Fundamentals and vocabulary*

times per year. Assessing the risk means understanding (a) how much we would lose if something happens that affects what we own or are liable for, and (b) how frequently this 'something' would happen. Therefore, risk is always assessed by scenario analysis, that is, by evaluating the potential loss severities and frequencies of possible events.

Quality is a concept that is open to a variety of definitions. One widely agreed definition of quality is that 'the totality of features and characteristics... that bear on

its ability to satisfy stated or implied needs'.⁵ Quality can be viewed in both objective and subjective lights. Objective quality is the degree of compliance of a thing with a pre-determined set of criteria that are presumed essential to the ultimate value of the thing. On the other hand, we also have subjective quality, which is the level of perceived value reported by a person who benefits from this thing. The judgement of quality is then reported as good or bad quality value.

To achieve a consistent judgement about operational quality across an organ-

isation, it is key to determine the dimensions in which quality is to be assessed. For operational quality, the following three dimensions have proved useful: suitability and functionality, security and reliability, and availability and accessibility. These dimensions tell us whether the overall quality is high or low. For example, a good-quality car scores high in the dimensions suitability, reliability, security, etc. A poor-quality car does not. A good quality IT system satisfies the user needs, is suitable for the task at hand, is reliable, ensures data security and is always available.

Quality can be measured in two ways: that of something gained or that of something lost. Either way, the tangible results of the quality should be a measure of the degree to which stated or implied needs are fulfilled. To assess the quality, a rating on a so-called Lickert scale – such as excellent, good, fair, weak, poor – for each of the quality dimensions is therefore most appropriate.

Concept application

In operational risk, we want to assess the risk of loss arising from failures in the business processes of the organisation. For this, we need to understand what we mean by business processes.

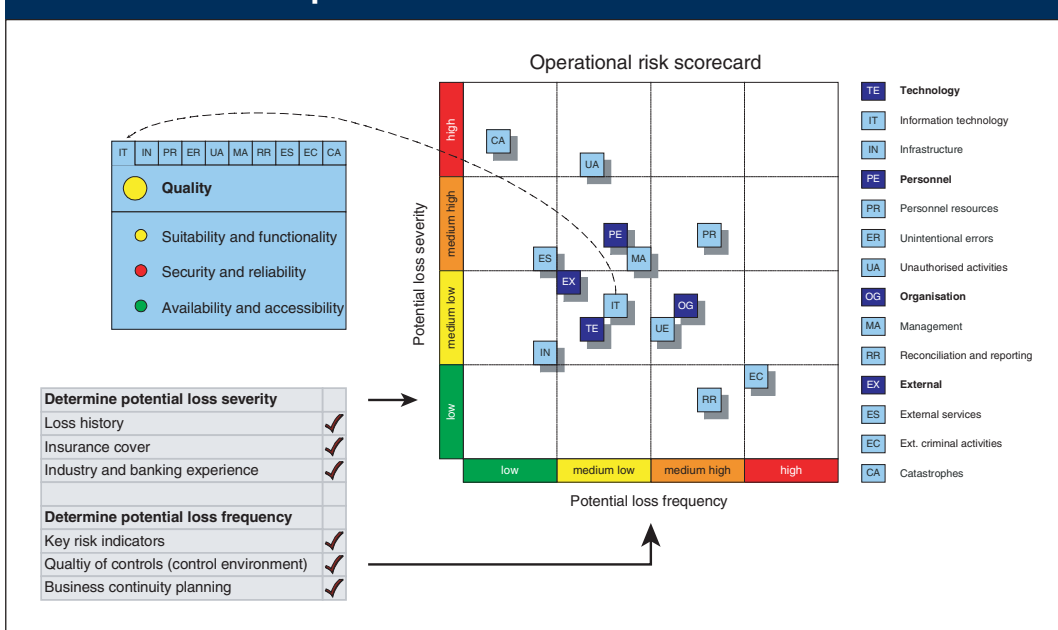
If we want to understand op risk in more detail, we need to understand what we mean by business processes. A (business) process is defined as a set of (business) activities that produce an output from a given input.

The activities of business processes are, to varying degrees, dependent upon certain factors such as information technology, infrastructure, expertise of personnel resources, controls against unintentional errors, controls against unauthorised activities, management decisions, information from reporting and reconciliation, external services, controls against external criminal activities and preparation for catastrophes (see figure 1). The factors underlying a business process can also be called risk factors since their inadequacy or failure may result in a situation in which the activities in the process cannot be performed, and therefore the process cannot fulfil its purpose. This could potentially lead to an op risk loss. The risk factors can be assigned to risk causation categories such as technology, personnel, organisational or external factors.

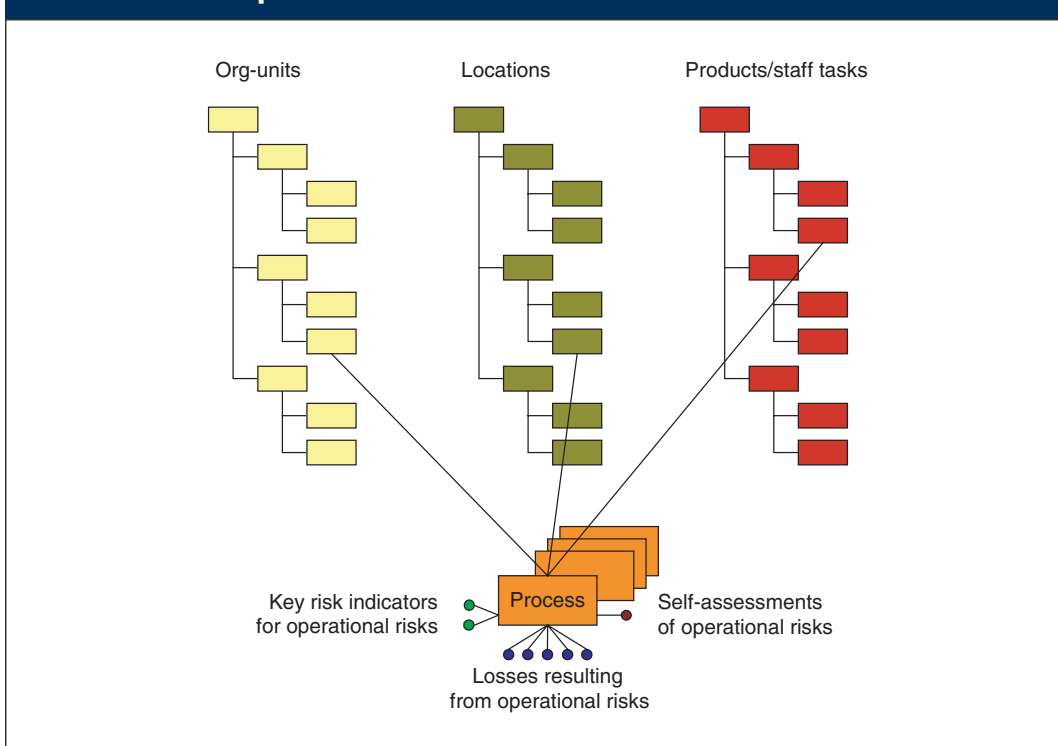
Below are two examples concerning business processes and inadequacies or failures of their risk factors⁶:

□ The process we could call 'trading in Asia' in Barings Bank would have needed a control against unauthorised activities. It has been stated that this control did not

2. The scorecard report



3. Attributes to processes



exist – or was inadequate – so that Nick Leeson was ultimately not prevented from ruining the whole bank.

□ The process we could call 'hedge fund trading' in Long-Term Capital Management would have needed proper risk reporting and management decision-making. It was analysed that both seem to have failed so that \$4.4 billion was eventually lost.

To evaluate a business process's op risk, one therefore needs to evaluate the risk of a loss due to a failure or inadequacy in one or more risk factors. In short, a failure of a risk factor underlying a process, such as an IT breakdown, might cause an operational risk loss. The severity of such a loss, together with its frequency of occurrence, determines the level of op risk due to this factor.

Furthermore, it is obvious that the quality of the risk factors underlying a process significantly influences the level of risk incurred. Therefore, it is also necessary to evaluate the quality of the risk factors. This analysis allows management to focus attention on situations where the risk of loss in a process due to failure or inadequacy of the underlying risk factors is high, and the quality of the underlying risk factors is low. If the risk incurred by the risk factor in the process is high, but its quality is also high, the risk needs to be insured or accepted. Otherwise the logical consequence would be to close down the process.

Producing a self-assessment scorecard

The result of an assessment of op risk and quality for any particular set of business processes is input into a report called a scorecard report (see figure 2). As operational risk is broken down into the risk categories, each risk category has its own individual risk assessment, which is based on scenario analyses. The scorecard

therefore shows the risks caused by the failure of risk factors scored into a risk matrix in the dimensions of severity (in euro) as well as frequency (in number of times per year). The quality of each risk factor is scored by assessing the quality dimensions of the risk factor (in the form of a rating). This means it reveals: (a) how much is lost in the event that the corresponding risk factor breaks down, is inadequate or is unavailable so that the processes dependent upon it fail or are only able to function with significant limitations; (b) how frequently that will occur; and (c) how good the risk factor for the process is in quality.

To generate a scorecard, the necessary information must be collected from within the organisation. Historic loss data or key risk indicators alone do not seem to be adequate choices for the assessment of op risk in business processes. Historic loss data is usually insufficient and not forward-looking. Key risk indicators need to be interpreted subject to the local context they stem from, and therefore do not possess a simple translation into risk.

The better choice seems to be to make the organisation's experts responsible for evaluating the internal risks based on their understanding of their business processes, their banking and industry experience, their knowledge of embedded controls, insurance cover and loss history, and existing key risk indicators.

The way to make the experts responsible is via a self-assessment exercise. This is not a simple task, since a lot of effort needs to go into debriefing the experts so that their evaluations are consistent, are comparable, can be validated and are as reliable as possible. The exercise therefore has the following prerequisites:

□ If the self-assessment is supposed to be an exercise across the whole organisation, it needs to be applied to all essential business processes within the

organisation. For this, we need a process collection exercise, which is described in more detail below.

□ The experts who will assess the business processes need to be identified. They are selected according to their knowledge of these processes and according to their responsibility for certain products, locations or organisational units. The experts are then trained in workshops or presentations about how to fill in the self-assessment questionnaire. Additionally, they must be guided when filling in the questionnaire by means of help texts, interviewers or through a helpdesk. Once the experts have completed the questionnaire, the answers usually need to be approved by another person. The workflow of the self-assessment is presented in part two of this article next month.

□ Since a self-assessment is usually applied to a wide range of processes, the self-assessment logic needs to be well thought through. It is the basis for the questionnaire design, where the questionnaire must measure what it is supposed to measure, and the questions in the questionnaire must be easy to understand. The answering schemes must also be well explained, otherwise consistent results cannot be expected.

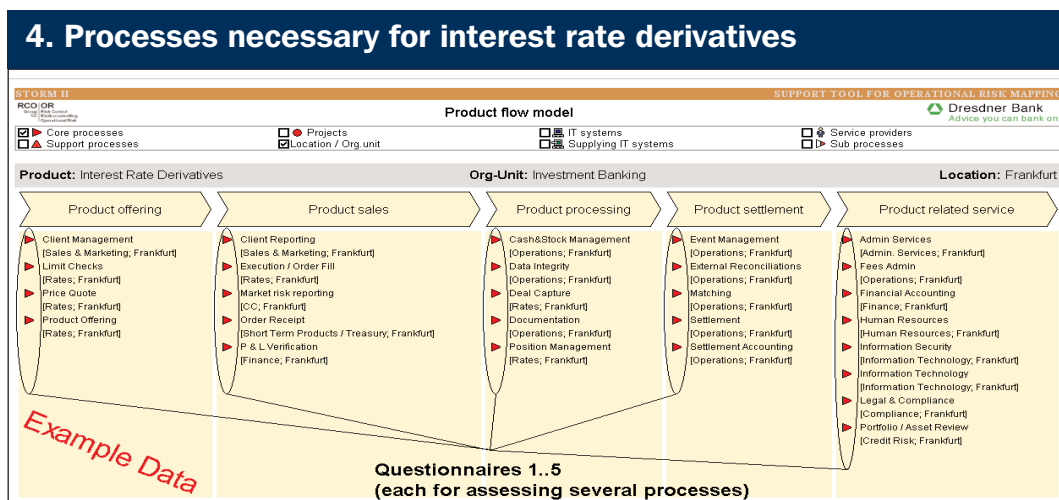
□ Once the self-assessment has been completed and approved, the results of the self-assessment need to be validated. This is performed by an independent operational risk oversight function. The quality of the overall op risk process is additionally reviewed by the internal audit function (as described further on).

Process collection

Before we can actually assess the business processes of the company, we must take stock of them. This means collecting the processes of the organisation so they can be named and listed in a structured format. This task is similar to bringing the market and credit portfolios together in one place before we can actually calculate their risks.

The process collection exercise needs to fulfil three purposes:

□ It needs to ensure that the operational portfolio covers the entire organisation.
 □ It needs to provide a structure for the operational portfolio in order to: (a) find the right experts in the organisation to assess the business processes without overlap; (b) be able to aggregate the reports of the assessments by products, location or organisational unit or combinations thereof; (c) subsequently allow for the comparison of the self-as-



⁶ See www.ic2.zurich.com

assessment of op risks with losses resulting from op risks and key risk indicators pointing to op risks.

It needs to define at what level of process granularity we wish to collect information and to subsequently report on operational risk assessments, losses and indicators. The less granular the processes collected, the fewer the number of specific op risk assessments, losses and indicators that can be assigned to particular processes in the organisation.

We will now suggest a procedure for taking stock of processes that allows all three goals to be achieved. Since the purpose of any business process in the organisation is, ultimately, to enable the organisation to sell a product or fulfil a staff task, it makes sense to start the collection process at the level of products or staff tasks of the organisation. More precisely, any process should help to:

- offer products, close deals, deliver products, get deals settled or administer products, or
- fulfil a staff task, where staff tasks are tasks whose purpose is to fulfil internal or external requirements, for example, to produce a balance sheet, fulfil particular reporting duties, gather the information on which strategic decisions are based, etc.

The idea is now to assign all processes to products or staff tasks. When we have a complete list of products or staff tasks we simply need to follow their product flows through the organisation and collect all processes we find on the way. Using this procedure, we are already able to achieve the goal of a complete coverage of the organisation.

⁷ Porter M, 1985, *Competitive Advantage: Creating and sustaining superior performance*, The Free Press

Furthermore, any business process is usually run at one particular location and within the responsibility of one particular organisational unit. Consequently, each process belongs to: one or more products or staff tasks; one organisational unit; and one location.

What we have said so far is schematically represented in figure 3. The three attributes – products or staff tasks, organisational units, locations – also help us to structure the portfolio, and later also to compare operational risk assessments, losses and indicators that will be attached to individual processes. The level at which processes are assigned to the hierarchies of products or staff tasks, organisational units, and locations also determines the level of granularity of the processes. At the highest hierarchical level, we only have a single process for the entire company that is the set of all activities in the whole organisation, all locations and in connection with all products or staff tasks. This overall process can now be broken down into more granularity in the products or staff tasks, organisational units, and locations. Using this mechanism allows us to specify the granularity of the processes.

Conclusion

Why did we concern ourselves with business processes? The answer is:

- To specify what we are assessing and to ensure full coverage of the organisation.
- To be able to report on the assessments in a structured manner in the different dimensions of products or staff tasks, organisational units or locations.
- To be able to split the task of the assessment between different people in the organisation without overlap and double-counting of risk.
- To be able to compare the assessments

with losses and key risk indicators for operational risk relevant to the same processes.

Figure 4 shows all the processes necessary for a certain product, that is, interest rate derivatives. The processes are marked with red triangles. The product is traded in Frankfurt in the organisational unit called investment banking. The processes show their location and organisational unit in square brackets. The five steps of the product flow (offer, sales, processing, settlement and related services) are similar to the supply chain model of Porter.⁷ (The five-step model does not have a particular necessity in this context, but it helps to structure the collection of the processes for a product.)

The process collection is the basis for the self-assessment. Each self-assessment is the assessment of at least one process. However, processes can also be grouped and evaluated within one overall self-assessment questionnaire. In the example shown, five questionnaires will be set up, where each questionnaire relates to a set of individual processes. Whether processes should be assessed individually or in groups depends on the materiality and complexity of the processes, as well as on the granularity of information the organisation wishes to achieve. Since each process has the three attributes 'organisational unit', 'location', and 'product', the self-assessment resulting in these dimensions can be analysed later and also compared with losses or key risk indicators collected for the same organisational units, locations or products. ■

Ulrich Anders is head of operational risk and Michael Sandstedt is operational risk controller at Dresdner Bank