Operational risk management

Embedding operational risk management: The real use test

Use test: the need for banks to demonstrate that risk management processes are truly integrated into the management of the business.

The real use test: giving the business a risk framework that they can actually use.

Operational risk management is at a crucial point in its development. Numerous approaches have been developed across the industry, but many institutions are struggling to make them fully effective by really embedding them into the day-to-day management of the business.

In order to overcome this challenge, it is first essential to define clearly the relationship between operational risk processes and the overall control environment (see Figure1), and to establish crucial links between different operational risk processes.

The effectiveness of operational risk management has been impeded by the common failure to embed operational risk truly into the overall management of risk and control. Group risk functions must demonstrate to business unit staff the full potential of using operational risk processes, developed under the group framework to manage the actual risks in the business. Our experience is that without this, business units resort to developing their own processes for managing operational risk and control, while paying lip service to the group framework for internal compliance purposes. The principal reasons for this are:

- Key risk indicators are often insufficiently linked to underlying risk assessment to provide effective risk monitoring.
- Risk assessment processes often fail to provide an effective means of understanding the operational risk profile or a practical tool for driving control improvement actions and consequent reductions in allocated capital.
- Loss data collection often provides a one-way feed into an 'invisible' group model, rather than being used by the business to identify areas of control weakness.
- Operational risk quantification is often viewed as irrelevant to the day-to-day management of risk.

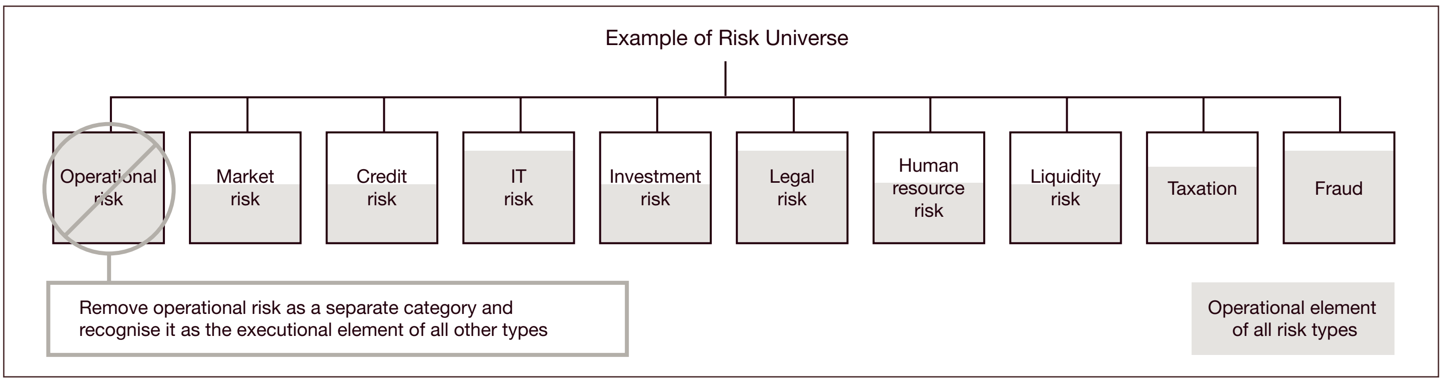
Crucial links

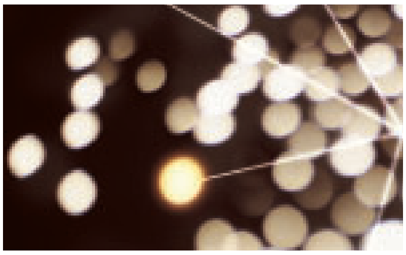
To make operational risk management effective in the business units it is essential to understand:

- **Link 1 – Operational risk is often viewed in isolation from, rather than integral to, all other risk types and those overlaps that are observed in particular with credit and market risk are understated.**
- **Link 2 – The important links between the key operational risk processes.**

Clearly articulating these links is crucial to demonstrating that, when working effectively, operational risk processes can provide a single-minded and coherent approach to managing risk and control, leading to the natural embedding of operational risk into managing the business.

Figure 1 – Embedding operational risk





Operational risk management

Embedding operational risk management: The real use test

How we can help you

The operational risk team at PricewaterhouseCoopers has extensive experience in the design and implementation of operational risk frameworks, from the simplest to the most sophisticated approaches. We place significant importance on creating and demonstrating the links considered here and would be pleased to discuss any of the issues addressed in more detail.

Contact details

Giles Triffitt
Tel: 44 131 260 4061
Email: giles.triffitt@uk.pwc.com

Charles Beach
Tel: 44 207 213 3591
Email: charles.beach@uk.pwc.com

Peter Trout
Tel: 61 2 826 67620
Email: peter.trout@au.pwc.com

Dietmar Serbée
Tel: 1 646 471 7270
Email: dietmar.d.serbee@us.pwc.com

Thijs Peeters
Tel: 31 20 568 4159
Email: thijs.peeters@nl.pwc.com

Link 1 – Operational risk and control environment

A key problem often separating operational risk from the rest of the business is that it is often viewed as a distinct risk type rather than being seen as the executional element of all risk types, i.e. from credit and market risk to those risk types falling within the accepted definition of operational risk such as fraud and business disruption.

This leads to a perception by business staff that operational risk processes are an unnecessary duplication of existing control activities imposed by senior management with little link to reality. This is the principal reason for the failure to embed operational risk management into day-to-day management of risk and control.

The key to solving this problem is to understand that operational risk exists across all risk categories and that operational risk assessment is simply a vehicle for the continual improvement of controls governing the management of all other risk types.

One potentially radical solution is to remove operational risk as a separate risk type and to recognise that it represents the executional element of all other risk types. Risk and control assessment is then positioned as a means to ensure that the effectiveness of these other risk management processes, such as credit risk, fraud, HR, IT, etc, as implemented in the support functions, are continually assessed through a single framework.

In short, operational risk is simply quality assurance over the management of risk and control.

Link 2 – Relationship between operational risk processes

Having established the role of operational risk processes in the context of the control environment, the next step is to make the processes themselves smarter.

The most effective way to do this is to establish the links that are often absent between risk processes in many current operational risk frameworks, to enable them to work together in a dynamic risk management cycle rather than, as they are in many institutions, separate processes (see Figure 2). This brings operational risk closer to the approach adopted in credit and market risk in which forward-looking assessments are used to develop metrics for monitoring and then back-tested against loss experience. By creating these links, we can create a self-improving and dynamic operational risk framework.

Figure 2 – Creating the links between operational risk processes

Current state Disjointed	**Risk and control assessment** • Many banks have various approaches to risk and control assessment in place • Different internal and regulatory objectives, e.g. Basel II v SOX • Lack of consistency/duplication destroys business buy-in	**Risk monitoring** • KRI development often separated from risk assessment process • Often use libraries of indicators from industry consortia • Tendency to monitor too many indicators	**Loss event reporting** • Often reported 'one way' to group for quantitative analysis only • Not used by the business to identify control improvement opportunities • No link to risk assessment and monitoring to test effectiveness
Target state Connected	**Risk and control assessment** Create a single risk assessment process covering all risk and control-related objectives: • Significantly improves risk assessment effectiveness • Reduces cost of risk processes	**Risk monitoring** Embed development of KRIs into risk and control assessment: • Avoids proliferation of irrelevant indicators • Focuses on monitoring only key risks	**Loss event reporting** • Loss events tracked primarily for effective incident response and control improvement • Loss data also analysed by the business to help focus controls • Inputs to any quantitative model are a natural by-product of this process