

SUNGARD®TRADING AND
RISK SYSTEMS

Operational risk solutions

An analysis of the key drivers behind a bank's operational risk system strategy

Operational risk is one of the most nebulous areas of the Basel II Accord. While credit risk has long been understood and incorporated into regulatory and economic capital charges, operational risk stands as a catchall, and controversial, category. Appropriate measurement methods are the subject of lively debate and systems remain in their early stages of development. Given this, what options are available to banks and what is motivating them to move in certain directions?

SunGard Trading and Risk Systems has completed a comprehensive market review of how the financial services market is preparing for operational risk in light of Basel II. Based on these discussions, we have identified three main drivers that are shaping how banks plan to address operational risk. These drivers are not mutually exclusive; banks usually exhibit some mix of these, with one being clearly dominant. One trend we have seen is a tendency for secondary approaches to increase in importance as a bank gains experience in operational risk management.

A key finding is that there is no single blueprint for operational risk. Financial institutions, as well as corporations, will need to develop operational risk solution architectures that support their unique business environment, their needs and philosophy. Banks are also looking at operational risk in a broader context than narrow Basel II compliance. They realise that implementing an operational risk management process and infrastructure will add value by reducing operational risk-related losses, decreasing reputation risk and optimising processes and the internal control system. In order to take full advantage of the range of methods for operational risk management and to avoid a silo approach, institutions should adopt a flexible, modular infrastructure (see diagram).

1. Compliance and cost minimisation

As a baseline, many banks are evaluating the simplest and least expensive route to compliance. This typically involves collecting loss data (LDC). These data can be useful in reducing losses and reputation risk by highlighting areas of recurring or high impact failures. Also, the very discipline of collecting such

While credit risk has long been understood and incorporated into regulatory and economic capital charges, operational risk stands as a catchall, and controversial, category

Financial institutions, as well as corporations, will need to develop operational risk solution architectures that support their unique business environment, their needs and philosophy

data improves processes by raising awareness of the financial impact of operational failures. Furthermore, loss data collection is a necessary prerequisite to performing statistical analysis for estimation of loss distributions. Finally, this approach is explicitly recognised by Basel II as a sound practice and a necessary component of an advanced measurement approach.

Once the data are collected, banks can implement some variation of the loss distribution approach (LDA). This involves identifying and separating expected losses, unexpected losses and stress losses. The latter two often rely on external loss data, since there may not be sufficient internal losses of this type to be statistically useful. Also, having collected loss data, banks can use them to shape extreme but plausible scenarios to supplement purely statistical analysis with a judgemental exercise in "thinking the unthinkable."

One advantage of the compliance and cost minimisation approach is that it is easier to get buy-in from senior management because it is a 'must-have'. There will be tough questions to answer if this is all that a bank does since it will have a limited impact on actually improving operational process controls. But it is likely to be the minimum a bank will need to do to keep the regulators happy.

2. Influence behaviour/change the organisation

A second motivation - which we have found is often present alongside the first - is to make fundamental improvements in a bank's operational risk management processes rather than simply seeking to meet the specific regulatory requirements. Here the aim is to avoid negative publicity on the front page of the Wall Street Journal or the Financial Times, with the belief that effective operational risk management involves far more than keeping regulators happy. Rather it is about substantial performance improvement and the determination to make consistent high quality service delivery a core competence.

With such goals in mind, banks often adopt control and risk self-assessment as a starting point. This typically involves a series of facilitated workshops involving both line management and internal audit or risk management personnel,

often with an outsider to provide external perspective. This self-assessment enables the bank to map current processes, identify areas of potential operational failures and, ideally, results in agreed improvements in methods and procedures.

Involving operational personnel and their managers directly in the process is important. It means the resulting innovations reflect detailed knowledge of the processes involved and fosters 'ownership' in any agreed innovations on the part of those who must implement them.

The next step is potentially the development of a scorecard approach in which performance metrics are agreed to and tracked through time. These metrics are tied to operational risk capital allocations based either on statistical analysis or judgementally agreed ground rules determined by negotiation between line managers and risk oversight personnel. This gives incentives for desired behaviour as managers seek to improve their performance metrics, thereby reducing their associated capital allocation and increasing their return on capital for any given level of profit.

3. Anticipating future problems

A third motivation is the desire to anticipate and predict potential future events sooner and more consistently. This involves identifying key risk indicators such as settlement failures, staff turnover, computer breakdowns, customer complaints, internal limit violations and breaches of information security such as falling victim to computer worms or viruses. These indicators are then analysed using statistical process control techniques. The goal is to detect unusual patterns that often indicate structural issues needing management attention and correction.

Among these three motivations, this is the one that we have seen least among banks, although it may be gaining ground as a reasonably cost effective way to reduce operational losses rather than simply measuring them.

Banks should approach their operational risk strategies with a clear understanding where they are today and with a view to the future

Common threads

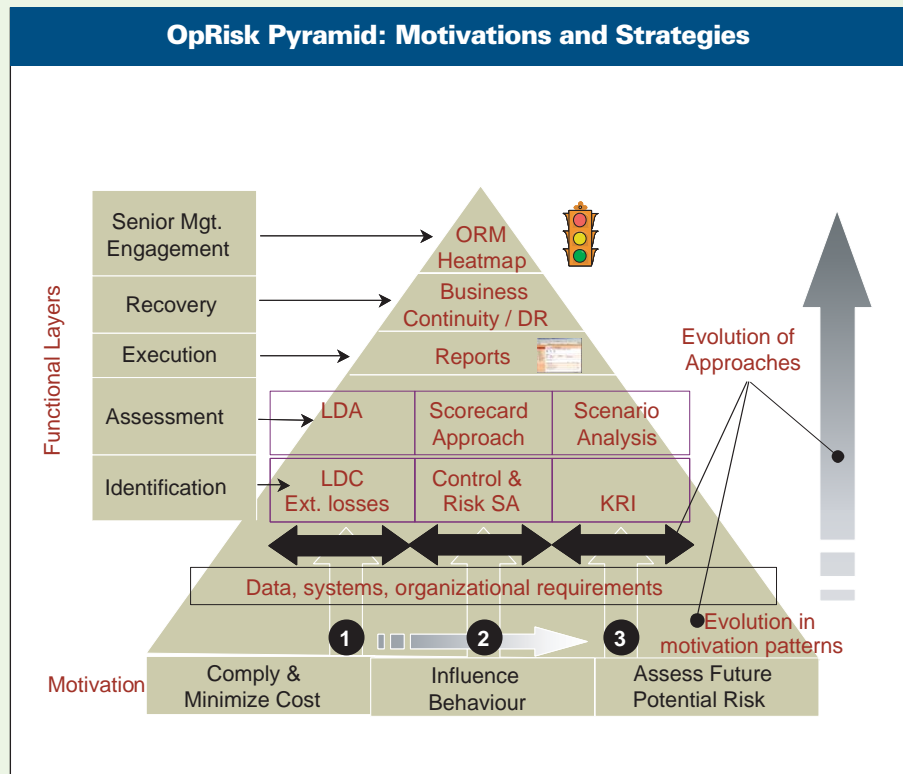
Reporting

Whatever the primary motivation and associated operational risk framework, risk identification and assessment is always followed by execution. This involves tailored reporting both to line managers and senior executives. Line management reports are detailed and focused on specific issues of concern. Senior management reports are generally broader and focus on major problem areas.

They often are presented in the form of a heat map. One of the primary functions of such reports is to maintain top management attention on operational risk issues and to motivate middle managers to avoid showing up as the source of a major problem.

Business continuity

The focus on business continuity has tended to be on backup sites and disaster recovery. However, a good operational risk infrastructure will also have



significant procedural detail - for example, knowing where people are going to report and a central database of non-work contact details for staff. It is important to realise that success in this area requires just as much conscious planning as does improvement in recurring processes.

Operational risk management heatmap

A truly sophisticated operational risk management infrastructure will also provide senior executives with the tools to identify and monitor areas of operational risk across their institution. This can be achieved with an operational risk 'heatmap' that provides executives with high-level indicators of areas of strength and weakness across the organisation.

The holistic approach

Banks should approach their operational risk strategies with a clear understanding where they are today and with a view to the future. Initially focusing too narrowly on a single approach and building an inflexible silo brings the danger that it cannot be extended or integrated with other approaches. System support should be comprehensive enough to integrate the full range of emerging tools and techniques as an institution broadens its approach over time. SunGard's unique breadth of systems, staff capabilities and industry experience with a wide-range of clients makes us a uniquely suitable partner for banks as they develop, finalise and implement their operational risk management processes and systems. ■

CONTACT

SunGard Trading and Risk Systems

Tel: +44 (0) 207 337 6000

e-mail: marketing@risk.sungard.com