Asian Banks: Setting Operational Risk Limits

Successful Asian banks are establishing risk limits as part of an effort to synchronize the integration of their operational risk models with their existing business units. But what steps are these banks following to set operational risk limits? And what are the potential benefits of embedding operational risk into a bank's day-to-day operations? Niklas Hageback investigates.

For a large number of Asian financial institutions that are in the process of implementing a Basel II-compliant operational risk framework, integrating the operational risk initiatives with the overall business objectives and strategies is a major challenge. If the operational risk tools and techniques are not embedded in the day-to-day management of the bank, much of the perceived value and business benefits of an operational risk framework is lost – due to its silo foundation.

To address this issue, leading Asian financial institutions are using operational risk limits to bridge and synchronize the integration of the operational risk framework with existing business practices. The aim of this article is to introduce the concept of operational risk limits and to outline a blueprint for the emerging best practice for establishing a limit structure.

As part of introducing a Basel II operational risk framework, one of the most complex issues is to ensure that operational risk initiatives align with corporate aims and objectives in a meaningful way. These initiatives must also be integrated with a bank's day-to-day management; otherwise, Basel II can potentially become nothing more than an exercise in "regulatory window dressing."

Properly integrated, an operational risk framework provides a number of business benefits that can lead to significant cost savings – as well as an information advantage that leads to a more efficient decision-making process than those of less sophisticated competitors. But the real key to success is to embed operational risk tools and techniques into the business practice, so that they can support and enhance the daily management of the bank in a meaningful and value-added way.

Operational Risk Limit: A Definition

Leading banks in Asia have bridged the gap between their operation risk frameworks and their business operations and strategies via the introduction of operational risk limits. Limits need to be outlined through a structured and logical foundation to ensure a consistent implementation; hence, establishing a clear roadmap is pivotal. However, to start with, it is important to understand what an operational risk limit really is and how it can be used.

The purpose of operational risk management is not to eliminate risk but to ensure that it remains within tolerable boundaries. Hence, risk tolerances or limits express how much risk the bank is willing to take for a certain risk exposure and can be articulated in both quantitative and

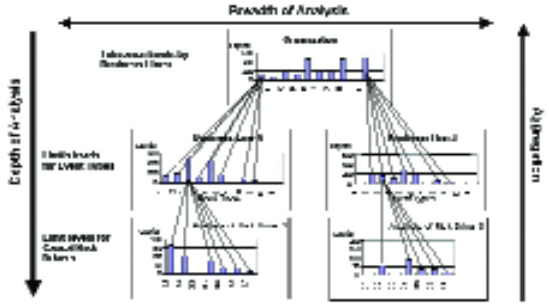
qualitative expressions.

Tolerances and limits are largely synonymous but are applied on different levels of the bank, and tolerances normally constitute aggregations of related limits. Tolerances are applied on a firm-wide perspective for operational risk loss-event categories and/or business lines; they should also be aligned with perceived rating targets and strategic objectives, such as risk-adjusted performance levels. Subsequently, the tolerance levels need to be expressed in monetary amounts – to reflect the capital the board is willing to risk in pursuit of the bank's business.

However, from a business line perspective, tolerance levels can appear too abstract, so to tie in tolerances to more pragmatic and practical targets, limits are introduced. The tolerance levels, hence, are cascaded throughout the bank through limits that help serve as the board's instrument to communicate the quantitative levels of strategies and objectives – as well as the firm-wide bank culture of risk awareness.

Limits are normally linked to individual risks or controls that – from a bottom-up perspective – correspond to the matching risk tolerances; limits also play an important part in the day-to-day management and monitoring of the risk and control environment of the business.

Cascading Effect: Tolerances and Limits



A Blueprint for Operational Risk Limits

A comprehensive plan for establishing operational risk limits comprises five primary steps: 1) setting risk tolerances; 2) linking limits to tolerances; 3) creating a limit design; 4) integrating limits into the business framework; and 5) testing and calibration.

The establishment of risk limits follows a top-down approach. Subsequently, it should start from the board of directors level, where tolerances are established not only for operational risk bank-wide but also by categories – which could include loss-event types and Basel business lines.

In an effort to align tolerance levels with the bank's rating and risk-adjusted return targets, the board needs to consider the maximum size of operational risk it is willing to accept. To communicate the board's views on the quantitative levels of strategies and objectives throughout the bank, tolerances also need to be broken down to more manageable and meaningful targets: i.e., limits. For example, when the board has estimated a capital tolerance level for IT-related risks, this risk category should be broken into key factors that are monitored periodically – including system downtime, number of virus and hacker attacks, IT-related staff training and usage capacity for business-critical systems.

Niklas Hageback

For each of the selected factors, one or many Key Risk Indicators (KRIs) should be linked to periodically measure any changes in the levels of risk for each factor. The selection of relevant risk factors is normally done through causal analysis of historical loss data and is supported by statistical analysis – such as regression – to better understand the interdependencies.

After the limits and tolerances have been rolled out and implemented as part of the business practice, evaluating the effectiveness of these tools should be an ongoing exercise. To better understand how well the limits relate to actual loss exposures, back-testing of the limit levels versus actual loss outcome should be conducted. The back-testing and analysis of causal drivers behind losses constitute a key part in assessing suitable limit levels.

In addition, as part of Management Information (MI), the number of limit breaches should be tracked over time; this tracking process will pinpoint trends for further analysis and highlight areas where risk exposures are not contained within tolerable limits.

The testing of applied limits versus actual risk metrics – which helps ensure that risks remain within tolerable boundaries – is also an important part of establishing and maintaining a credible operational risk framework.

Early Warning System: A Byproduct of Limits?

Articulating, setting and calibrating risk limits has implications not only for an operational risk management functional model but also a number of other elements, including: governance; risk management policies; risk measurement; management information and performance reporting; training and education; and external reporting.

Banks that establish limits will also find it easier to set up other risk mitigation systems, such as a so-called Early Warning System. The objective of an Early Warning System is to prevent/reduce the levels of operational risk losses by linking preventive actions to the identification of predictive indicators and patterns.

Since early warning signals aim to highlight changes in the risk environment and the effectiveness of controls, they provide banks with an opportunity to intervene early and avert problems before they become a source of financial loss or reputation damage.

An early warning signal would typically represent the breach of an operational risk limit, which indicates that the level of operational risk has significantly increased and the likelihood of a loss occurring is on the rise.

The breach of a limit should initiate some type of action, such as an investigation of the causes behind the breach or the launch of a proactive plan to reduce the risk of an operational loss.

Basel II Connection

Limits can also potentially affect the capital charges banks will be subject to under the Basel II capital accord. Basel II's Advanced Measurement Approach for calculating operational risk capital includes a "forward-looking adjustments" component. This component requires a bank to consider not only historical loss data but also potential historical loss scenarios when calculating an operational risk capital charge.

Forward-looking adjustments are normally done through KRIs and control scores. If the levels of operational risk exposures increase, as captured through the KRIs and control scores, these exposures will subsequently be reflected through an increased capital charge; on the other hand, decreased operational risk exposure levels will lead to a lower capital charge.

The link between the AMA capital methodology and risk limits is tied to the forward-looking adjustment. The number of limit breaches, tracked on an ongoing basis, can serve as an indicator of the level of risk. Subsequently, an increased number of limit breaches, from one time period to another, will lead to an increased capital charge.

Business units that breach agreed limits will be penalized through increased capital charges, which of course can negatively affect a unit's performance measurement, budgets and bonuses. Undoubtedly, such potentially negative ramifications serve as an incentive for effective implementation of limits at banks.

Benefits of Op Risk Integration

In addition to meeting regulatory requirements, Asian banks that have gone through the process of embedding their operational risk framework into the organizational structure have profited from a number of business benefits, including: improved and consistent MI and reporting; a better understanding of a firm's specific operational risks; a reduction of costs; and mitigation of potential losses.

Firms that embed operational risk into their business structure typically introduce a "health check" system that provides early warning signals about potential operational risk problems, mitigating the potential for losses; this is one component of improved MI and reporting.

> "When a bank fully comprehends its operational risks, it can ensure that these risks are priced into products and services through an economic capital program."

When a bank fully comprehends its operational risks, it can ensure that these risks are priced into products and services through an economic capital program; it can also optimize its investment in mitigation tools – such as controls, insurance and business continuity – in terms of cost benefits.

Integrating Operational Risk Limits: **Five Key Questions**

1) What is the make up of existing IT support systems and infrastructure?

2) Has there been appropriate documentation of tolerance/limit management procedures?

3) How are limits embedded into Management Information and reporting?

4) How is the limit monitoring best structured? (By whom and how often?)

5) How does the firm adhere to treatment of escalation breaches regarding existing preventive action plans, responsibilities, communication lines, materiality and experience?

Ultimately, it is important for banks – not only is Asia but across the globe – to develop a holistic and consistent framework for managing heterogeneous operational risk types. On both an ad-hoc and a regular basis, this framework should be able to provide senior management with answers to four key questions: 1) What are our top operational risk concerns? 2) Is there a comprehensive and robust methodology put in place to measure operational risk exposures with significantly different characteristics? 3) Who takes ownership of the different operational risk exposures, through ongoing monitoring and management? and 4) What is being done to reduce existing operational risk exposures?

Basel II requires banks to establish an operational risk framework. But implementing operational risk tools and techniques should not be done just to ensure regulatory compliance, as a lot of business benefits can be accomplished through prudent operational risk management.

> "I like to play with toys that resemble financial models. Such objects keep me reminded of the fact that life is a game, and it should be played with."

Leading Asian banks have experienced cost savings in terms of lowered levels of operational risk losses and improved reporting, which ensures information advantages over less sophisticated competitors. However, to achieve these benefits, the operational risk framework needs to be fully embedded within the bank's operations. The bridge between the two is operational risk limits. Establishing limits within an organization takes a very clear understanding of what limits are, as well as a structured implementation blueprint. A trial-and-error implementation process is filled with potential pitfalls and can be costly, so it's best to have a fundamentally sound plan in place before you tackle the operational risk dilemma. ■

A Guide to Tolerances

When devising a plan for operational risk, there are many different types of tolerances to consider. Zero tolerances, for example, are typically related to fraud and criminal activities and apply to activities for which a single incident is automatically a recorded issue. But what are the other key tolerances? Here's a quick rundown:

Frequency Based: These tolerances are business context-dependent and are measured in terms of either the maximum permitted percentage of similar actions that fail or the maximum permitted percentage of time that an error condition may prevail. For example, in the payments processing back-office function, the risk tolerance for "incorrect transaction handling" may be stated as 1‰ – meaning that no more than one payment per thousand can be incorrectly handled without a warning flag automatically being raised. Frequency is measured through the periodic values of the appropriate Key Risk Indicator (KRI), which will typically be updated on a monthly basis.

Amount Based: Stated in monetary terms per annum, regardless of the number of incidents, these tolerances are typically found in activities with low-processing volumes; the cost of individual insurance and premiums paid for insurance policies to cover for loss of or damage to assets is an example of an amount-based tolerance.

Control and Risk Self Assessment (CRSA): This type of operational risk tolerance calls for qualitative assessment of risk; risks are rated, on a scale of 1-5 (insignificant to catastrophic), according to frequency and severity.

Capital Based: This type of risk tolerance is calculated using a capital-at-risk methodology, whereby the bank holds a minimum economic capital base level that will cover unexpected loss within a defined confidence level, holding period and observation period. For regulatory purposes, funding and other structural and business cycle reasons, a bank might want to maintain a buffer above this minimum capital base. However, if the full cost of effective and robust risk controls is expensed and/or capitalized within a financial reporting period by each business line, prudent provisions can be made for all expected loss incurred in the normal course of business; these provisions are made as a cost of undertaking that business – and the risk tolerance for that business expressed as a percentage of risk-adjusted capital.

References:

1) Alexander, C. "Operational Risk: Regulation, Analysis and Management." Financial Times Prentice Hall, 2003.

2) Cruz, M. "Modelling, Measuring and Hedging Operational Risk." New York: John Wiley & Sons, 2002.

3) Ong, M. "The Basel Handbook – A Guide for Financial Practitioners." London, Risk Books, 2004.

4) The Basel Committee on Banking Supervision, 2003. The New Basel Capital Accord, Third Consultative Paper.

✎ **Niklas Hageback** is a director at KPMG's Bank & Finance Group in the Asia Pacific region. He can be reached at niklashageback@kr.kpmg.com.