



A series designed to introduce readers to the tools used in the management of operational risk in today's financial services industry.

Self-Assessment of Operational Risk

by Mark Balfan, Phil Gledhill,
and Michael Haubenstein

Few would argue the merits of an enterprise-wide assessment of operational risks. But why self-assessment? This instalment of OR presents the value and implementation of self-assessment.

Operational risk management challenges are very different from those posed by market risk and credit risk. One fundamental difference is that there is no “position” to measure. Consequently, we need to apply a combination of different approaches to understand the current risk profile of the organization and how it might be changing.

An operational risk management framework¹ puts risk in the context of business strategy and risk appetite, establishes processes of risk assessment and measurement, and links the results to performance measures and shareholder value. But how do we know that all operational risks are understood and that they are being effectively monitored and improved? The answer lies in *self-assessment*—one of the critical components in ORM framework.

Self-assessment (also called control self-assessment, or CSA) is a process whereby business areas identify and evaluate the risks incurred, the level of control the areas have over these risks, and action points for improvement. The starting point for CSA is a comprehensive set of *risk definitions*—usually a set of major categories and detailed subcategories. The next step, *identification* of the risks incurred, typically takes the form of a risk map that shows risks by business area and their relative frequency and severity. Additional sources of information can enrich the analysis:

- An examination of the history of loss events and near misses highlights risk areas and provides insight into relative frequency and severity.

- The risk indicators used to monitor risk drivers and controls provide insight into the risk profile.
- A review of best practices and regulatory requirements for controls highlights additional risk areas.
- Audits and regulatory exams also will reveal potential weaknesses.

The Case for Self-Assessment

Self-assessment requires an investment in time and often technology. Organizations are committed to it because they realize self-assessment is necessary to:

- **Create accountability in the line organizations.** Line business areas are the “risk-takers” for operational risk and bear the profit-and-loss impact of any problems. A CSA process makes the risk analysis explicit, and line managers are therefore accountable for the results.
- **Reinforce a culture of openness and transparency.** Risk needs an open discussion to improve awareness and to allocate appropriate resources. CSA creates the forum to discuss the issues.
- **Implement a proactive rather than reactive process.** Businesses run better when they anticipate and correct problems before they occur. Preventing financial losses is also an important goal. CSA provides a method for identifying control weaknesses within the current process and developing action plans to eliminate the weaknesses.

© 2002 by RMA. Balfan is SVP, Market and Operational Risk, and Gledhill is VP and manager, Operational Risk Management Department, at Bank of Tokyo-Mitsubishi North America. Haubenstein is an independent consultant and former partner of PricewaterhouseCoopers, specializing in operational risk management. They can be reached at Mbalfan@btmna.com, Pgedhill@btmna.com and Mhauby@aol.com. The RMA Journal is grateful to Haubenstein for creating and overseeing this series of articles.

- **Engage various parts of the organization.** Operational risk touches all parts of the organization and has many interdependencies between line and support areas, such as information technology. Self-assessment helps break down the silos to discuss risk across the organization and to discuss interdependencies. It may also help justify budgets for needed improvements.
- **Increase awareness and ensure that all risks are considered.** Operational risks cannot be specifically measured at a detailed level. There is no substitute for a complete understanding of risk. While many risk indicators exist, they are not comprehensive, and capital measures operate at too high a level to provide detailed insight into individual exposures. The qualitative analysis in self-assessment complements other quantitative measures to ensure that the full scope of operational risks are analyzed.
- **Identify gaps and action items.** Regardless of the source, the self-assessment process results in identification of control gaps and resulting action items. It consolidates the information from all sources into specific plans for improvement, accountability, and target dates.
- **Enhance oversight and improve decision making.** The results are reviewed by senior management in order to understand the organization's risk exposures and resulting plans. The expectation is support for the plans with the resources required to implement them.
- **Improve audit efficiency.** As the reliability of the CSA results improves, auditors may become more focused on the real issues facing the organization, rather than merely testing transaction details for errors. Consequently audit time and time spent with auditors may decline.

Primary Alternatives in Self-Assessment

There is no one approach to self-assessment. The processes tend to evolve over time and often change purposefully to maintain interest and bring new insights into the risk profile. The alternative approaches are checklists, narratives, and facilitated workshops.

Checklists. Probably the most common approach, checklists are structured questionnaires

distributed to business areas for them to identify the level of risk and related controls. Some are very short with broad categories of risk (such as governance, compliance, processing, people, technology), while others provide a more detailed list that includes expected controls to be in place. Business leaders typically respond with a level of applicability to their process, often some indication of frequency and severity/impact, and the degree of control. Some organizations attempt to indicate the level of inherent risk (prior to control) and the level of risk after current controls are in effect. Any control weaknesses demand some type of corrective action (or a specific statement to accept the exposure), responsibility, and planned completion date.

Narratives. The starting point of narratives is different from the checklist approach, but the end result is similar. Narratives usually start with business areas defining their own objectives and the risks attached to each. Instead of checking off expected controls, they must defend how they control these risks. Gaps are addressed in a similar way. This approach requires more effort and more thinking about the business outside of the framework of defined risks and controls.

Facilitated workshops. This approach tries to skip the paperwork and get people to talk about their risks, controls, and required improvements. Workshops are typically facilitated by an independent person and contain a cross-section of line and staff people familiar with the selected topic. Differing points of view are debated to get better consensus and validation on the issues. Workshops may be used in conjunction with checklists and narratives to initially raise key issues.

How to Ensure Objective Results

When the CSA process is led by business areas, there is a clear risk of inconsistency in interpretation and attitude towards openness across the business areas. The following steps can help keep the results objective.

Involve risk specialists. A successful CSA program requires involvement of most functions in the organization. At the forefront, senior and executive

management must endorse the program completely, proactively review the results, and look for trends in observed weaknesses that might lead to better-managed goals and objectives. Business line managers directly perform the process. Generally, business line managers will deconstruct the elements of their business process in an effort to identify specific control weaknesses that can be addressed through the implementation of clearly defined action plans. The ORM department typically drives the effort by determining the CSA process, facilitating the effort, and aggregating the results. *Risk specialists*, that is, the heads of support departments, assist in the implementation of the CSA process, review self-assessment results from the perspective of their area of specialization, and render opinions on the business assessment of risk types, quantification, and frequency. Internal Audit shares information collected over the years regarding the control environments for each business and operational unit within the organization.

Verify the results. To ensure consistency and fairness, assessments prepared by the businesses must be verified. Operational Risk Management is the first line of defense against inferior CSAs. ORM provides the initial control over the results of the CSA and will make the initial review for completeness and consistency. To do this, ORM must have a thorough understanding of each department's business line, process, and objectives; any responses that stray from this understanding must be questioned and possibly returned to the department for clarification. Risk specialists are responsible for scrutinizing the development of the CSA as well as the results from the departments, especially as these relate to their area of expertise. Specifically, the risk specialist in charge of technology concentrates on technology issues that have been identified by the business units; the human resources risk specialist concentrates on "people" issues, and so on. Each of these individuals has the authority to reject a self-assessment if the reported results are inconsistent or inaccurate. Using the risk specialists within the organization is a good way to ensure that CSA results and issues raised are scrutinized at a high level of authority and expertise.

The role of Internal Audit. As the self-assessment is being developed, Internal Audit's

expertise is helpful in identifying each department's past control issues. Once the CSA is complete, Internal Audit becomes part of the validation process. Internal Audit can use the results of the self-assessment in planning future reviews of individual departments, especially focusing on progress made in correcting internal control weaknesses that were uncovered. The validity of a given CSA will be further confirmed if Internal Audit finds no additional control weaknesses within the department during the review. In addition, Internal Audit should be reviewing the entire CSA program as a process, evaluating whether the program is comprehensive and consistent, whether people are participating, and whether the program is a reliably effective management tool.

Lessons Learned and Key Success Factors

Several factors can help make the self-assessment process successful.

Executive management support. Organizations that attempt to initiate a CSA program without senior management support will find difficulty in achieving meaningful results, since the responsible individuals may not take the time and the assessments may not be as open, honest, and accurate as possible. Executive management's endorsement of the CSA process provides the appropriate incentive for business managers to carefully review the risks facing their businesses and determine whether the controls mitigating the risks are working successfully or not.

Not a one-time event. To be an effective and useful tool for the organization, the CSA must be designed as an ongoing process, not a singular event. Businesses should use it as part of a continuous evaluation of the organization's operational efficiency and internal control environment. CSAs should be performed frequently—at least semi-annually and often quarterly—to capture the improvements or deterioration in controls as well as any changes in a business that might impact productivity and earnings.

Identification of major risk and subrisk categories. The first step in creating a useful CSA program is identifying the major risk categories across the entire organization. It is important to keep these as broad as possible and to limit them to a manageable number (the fewer the better). Identifying more

OR: Self-Assessment of
Operational Risk

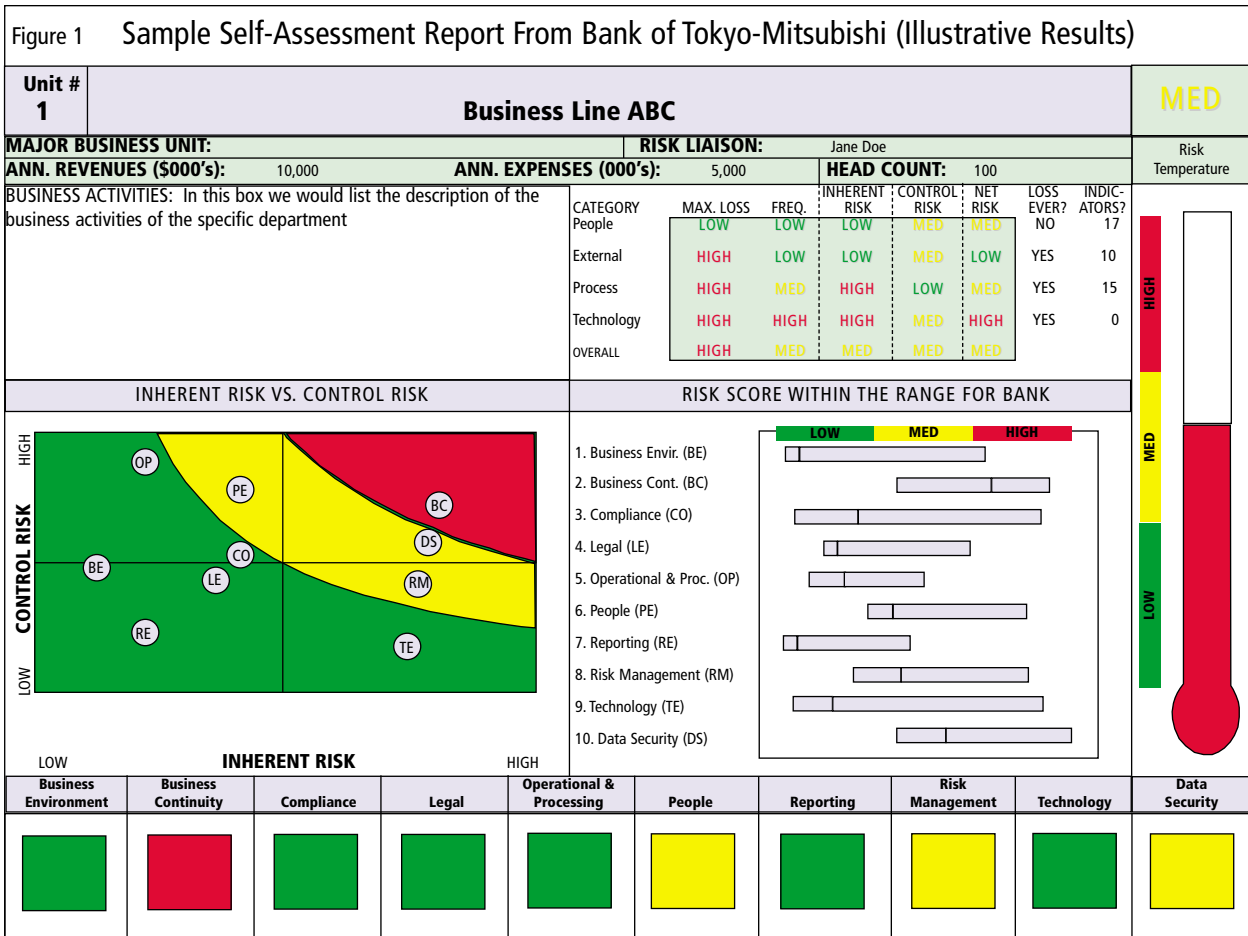
than 12 major risks would complicate the self-assessment dramatically. The program should include major event categories and other key control areas and ensure that each can be applied to all of the business lines within the institution.

Once the major risks have been identified, sub-risks that further define the risk can be developed. Once again, subrisks are to be limited to a manageable number, perhaps no more than four per major risk. In this case, subrisks may not necessarily apply to all business lines, as they have a tendency to be more specific. The major risk categories used at Bank of Tokyo-Mitsubishi are listed in Figure 1.

Customize, customize, customize. Regardless of the size of an organization, there are many parts. Distinctions can be drawn between departments that generate new business and sales, provide operational processing services, and supply technology support. Consequently, a CSA program that fits one business unit will probably not fit another, especially since

the severity and application of the risks facing each are going to be different. Even if the risks affecting one business unit are the same as those affecting another, the controls implemented by the individual units may be highly specialized and specific to each unit's needs. To capture these unique characteristics, each unit's CSA should be crafted so that risks affecting the department are analyzed completely, with control procedures used by the department. Thus, although the major risks and subrisks cut across all functions within the organization, business managers will be responding to the CSA in terms of the specific control procedures that exist (or should exist) within their department.

Sell the benefits of CSA. Managers who are completing the CSA must recognize the value of the process to the organization as well as to themselves. By digging deeply into the business lines process and control environment, managers identify ways to make their operation better. This can only serve to



improve profitability and efficiency, with the attendant rewards of better-managed businesses. They recognize quickly that CSA provides them with a comprehensive vehicle to manage their identified weaknesses and deficiencies, enabling a method to develop succinct corrective action plans and manage the completion of the plans.

Recognize that self-assessment is only one tool. CSA is part of a solution set that also includes risk strategy, governance, risk indicators, databases, and quantification. Each has its role and each complements another.

Keep audit independent. To encourage honesty, accuracy, and a deeply probing evaluation of departmental processes, policy must dictate that identified weaknesses will not be escalated into future audit findings. Department managers must be comfortable that their analysis will not be used against them. One potential policy is that only those weaknesses not mitigated or controlled by the departments within a reasonable time frame are subsequently open for criticism by Internal Audit.

Communicating the Results

Of course, final results will be distributed to executive management, providing them with a barometer of the level of risk within the institution. The challenge is how to communicate the operational risk profile of the organization. Executive management is interested in risk trends, as well as whether these trends are being addressed adequately and in a timely manner. Examples of reports from the CSA process include:

- **Top-10 risk lists.** As a result of all the assessments, these lists indicate the top issues across the organization that create exposure, the nature of the problems, and what is being done about them.
- **Heat maps.** These are color-coded reports, usually red/green/yellow, that highlight the overall “score” of control effectiveness for each business area and risk. These reports are often combined with comparisons to prior periods and highlights of the identified issues for the yellow and red areas.
- **Issue identification.** These are lists of open issues, with descriptions and assigned account-

abilities. These lists are reviewed for content, resources, and planned resolution.

- **Late issues.** Late issues are exception reports of uncompleted issues that have gone beyond their planned resolution date. If any fall past due, the business line managers must offer valid reasons for the delays.

The report shown in Figure 1 is prepared for each major business group. In the upper right, the major risks are rated for frequency, inherent risk, and quality of controls. The results are then placed on a risk map (middle left) to focus attention on the major issues. The CSA process results in a score for each major risk in each business unit. The scores from each business unit are displayed (middle right) in comparison to the high and low scores for other business areas across the bank. Overall ratings for each of the bank’s risk categories are highlighted in the color-coded charts on the bottom and summarized in the risk “thermometer” on the right. The graphic results convey a snapshot of the risk profile to senior management.

The ORM committee can coordinate all of these efforts on behalf of executive management by providing reports, maintaining contact with the business line managers, and constructing databases that keep track of the control weaknesses, corrective action plans, and target dates. □

¹ Michael Haubenstock, “The Evolving Framework for Operational Risk,” *The RMA Journal*, December, 2001.