By Grant Purdy

How Good Is Our Risk Management?

How Boards Should Find Out

In the past, boards were largely content if management told them what they thought were the major risks that their organization faced and described what they were doing to manage these risks. Now, directors want and need to know more. Recent corporate governance codes—such as the second edition of the *UK Corporate Governance Code*,[1] the South African King III report[2] and, in Australia, the second edition of the *ASX Corporate Governance Principles*[3]—all stress that boards need to gain assurance as to the quality and effectiveness of the risk management processes operating in their company. Boards need this before they can be in a position to say whether the profile of risks they have been informed about is reliable, and that the risk treatment being adopted is suitable and appropriate.

Last year, the first global standard on risk management was published. ISO 31000:2009[4] is different from most other codes in that it concentrates on how—and in practical terms—risk management can be implemented and continually improved. Clause 4.5 provides a clear example.

> In order to ensure that risk management is effective and continues to support organizational performance, the organization should:
> - measure risk management performance against indicators, which are periodically reviewed for appropriateness;
> - periodically measure progress against, and deviation from, the risk management plan; and
> - review the effectiveness of the risk management framework.

In other words, it requires organizations to adopt a performance management approach to risk management. Annex A.3.1 of the ISO 31000:2009 reinforces this message when it says that a required attribute of enhanced risk management is where "an emphasis is placed on continual improvement in risk management through the setting of organizational performance goals, measurement, review, and the subsequent modification of processes, systems, resources, capability, and skills."[5]

The preferred means for measuring performance in risk management is to use "lead indicators" that are concerned with processes that support the achievement of desired outcomes. Examples used include the:

- proportion of treatment tasks for high risks that have been completed this month;
- proportion of the actions in the risk management plan for the year actually completed;
- number of people trained in risk management this quarter against target;
- number of contracts that have been subjected to risk assessment this month against target;
- number of root cause analyses conducted in a project this quarter to learn lessons from successes and failures; and
- number of control self-assessments conducted this month against target.

Many organizations also find it valuable to review the performance of the risk management framework as a whole, typically by comparing how it performs in comparison with those in peer organizations or other benchmarks. This form of maturity evaluation is becoming increasingly popular because:

- it requires managers to evaluate their own areas against a set of criteria, thereby building ownership of the current level of maturity and the need for improvement;
- the process can generate an improvement plan that is the core of a risk management plan;
- it can be used to focus on organization-specific issues or functions that need improvement or that must be performed to a high standard;
- the results can be validated by internal audit, and this activity and the underlying protocol provide a tangible basis for audit assurance activities;

- the process can provide numerical measures that can be compared to personal or organizational performance goals;
- it can be used for benchmarking and best practice transfer within an organization or between organizations; and
- the protocol and measuring system can be changed periodically to "raise the bar" or change the focus, if required.

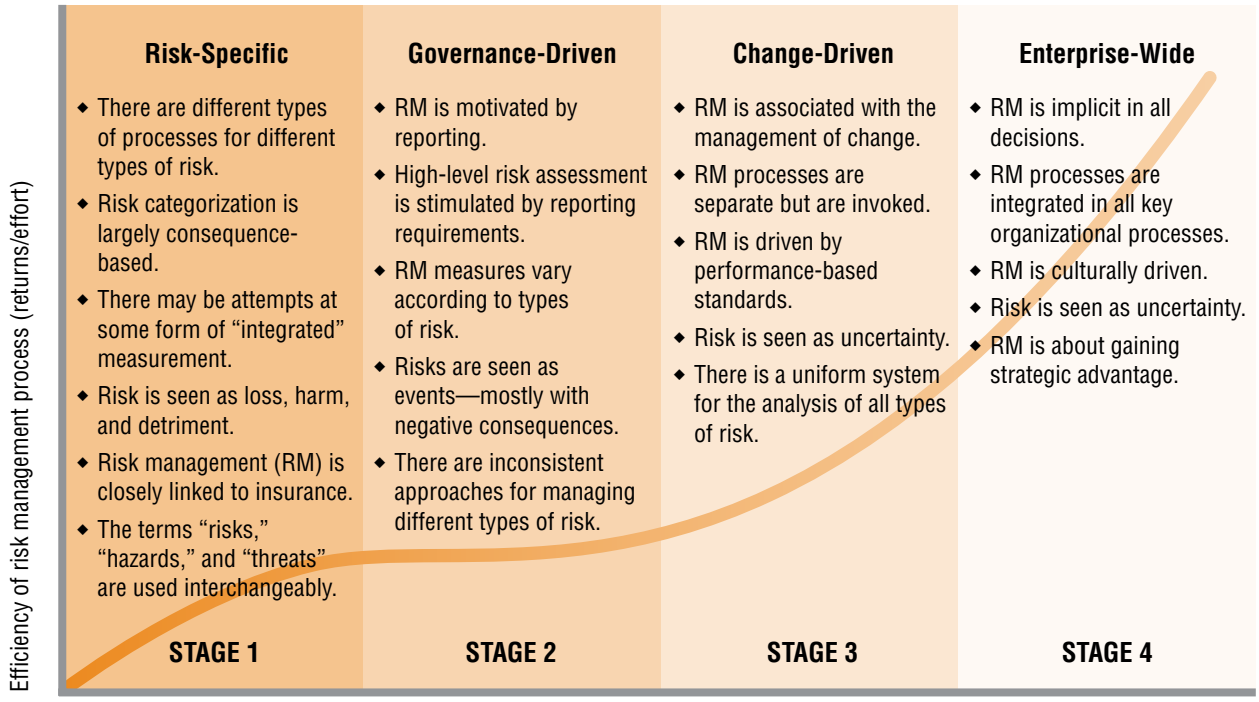
Such evaluations also provide a succinct and reliable summary of the effectiveness of risk management, and show the progress that has been made in improving performance. This sort of output is ideal for boards to use in fulfilling their oversight responsibilities.

The underlying premise of risk management maturity evaluation is that organizations are on a journey that leads to effective and fully integrated risk management. They all start this journey from different points—and even within organizations, different parts are likely to be at different levels of maturity. All organizations require the same basic components of risk management to be in place, but after that these components can be improved and others can be added.

Exhibit 1 illustrates how organizations typically mature. The efficiency of the risk management process is plotted—reflecting the perceived return achieved on the investment in effort that is made—against the degree of integration of the risk management process. This also correlates with the extent to which accountability for risk management is transferred from risk management specialists to all managers and employees.

Evaluation systems that measure where an organization sits on the maturity curve can be based simply on the principles and attributes in ISO 31000. However,

Exhibit 1
Risk Management Maturity Model



Source: Broadleaf Capital International Pty Ltd.

it is often more effective to produce a tailored evaluation protocol that better aligns to the risk profile, context, and needs of a particular organization. The currently available codes and guides for risk management governance all seem to contain some or all of the following 12 summary principles, each of which focuses on a key aspect of effective risk management:

1. **Culture**: Risk management is a core organizational process.
2. **Process**: The risk management process is well-structured.
3. **Outcomes**: There is a good understanding of the risks the organization faces.
4. **Accountability**: Nominated managers are primarily accountable for risk management, and the roles of the executive and board are clearly defined.
5. **Controls**: There is an effective control environment.
6. **Strategy**: Risk management is integrated with strategy development.
7. **Performance**: Risk and control management performance is monitored and reported.
8. **Learning**: The organization learns from successes and failures.
9. **Application**: Major changes trigger risk assessments.
10. **Resilience**: Business resilience and disruption response plans are in place.
11. **Infrastructure**: There are appropriate resources and support for risk management.
12. **Reporting**: There are efficient and reliable processes for the reporting of risks and risk management.

From this list, it is possible to select and tailor sets of principles and associated performance criteria to create customized evaluation protocols that exactly match the needs of a particular organization.

Normally, the management team "score" the performance of their part of the organization on each criterion in terms of the level of management commitment (intent) and the actual level of compliance (practice). The two scores are added together for each criterion and are averaged for each principle and overall. Comparing and contrasting the overall scores and those for each principle and criterion for different parts of the organization (e.g., departments), and for the organization as a whole, helps focus the allocation of resources and promotes internal benchmarking and the exchange of best practices.

Capturing the results of the evaluation on a spreadsheet or in an information system produces useful output, particularly when the current results are compared with those from a previous period, as shown in Exhibit 2.

These types of output can form part of governance reporting to senior management and the board to enable them to fulfill their duties in terms of providing assurance as to the effectiveness of the approaches the organization adopts for the management of the risks it faces.

When presented with such reports, directors are then able to ask some further penetrating questions such as:

- Is accountability for risks and controls clearly established and accepted? How do you know?
- Is risk management part of all key decision-making? Show me.
- Is risk management being embedded into all key business processes? Show me how.
- How did you integrate risk management into strategic plan development? Where are the outputs?
- Is risk management performance really improving? How do you know?

Performance management and reporting help boards and senior management understand how effective their risk management framework and associated processes are. They stimulate continual improvement in risk management and provide the means to focus attention on where potential improvements are possible and then gain ownership of the actions required. This also allows companies to comply with governance requirements that require reports to be provided to senior management and boards on risk management effectiveness.

This process works best when integrated into the organization's existing strategic planning and performance measurement and reporting processes.

Grant Purdy
Associate Director
Broadleaf Capital International Pty Ltd.

Grant Purdy *has worked in risk management globally for over 32 years and specializes in its practical application. Working with executive teams and boards, he ensures they adopt sound governance practices for major decisions and receive appropriate reports and information. Before joining Broadleaf, Mr. Purdy was Global Manager for Risk Management at BHP Billiton and led the team that developed and implemented an approach to enterprise risk management that is recognized as "world best practice" within the resources sector. He is Chair of the Standards Australia and Standards New Zealand Risk Management Committee that was responsible for AS/NZS 4360, and is a co-author of the*

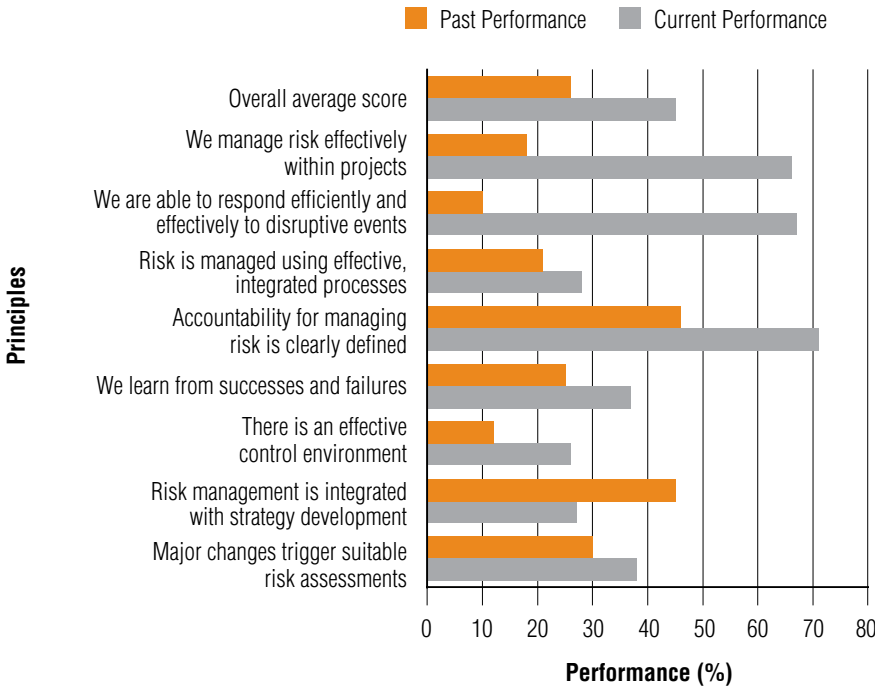
Exhibit 2
Risk Management Maturity Evaluation

Broadleaf

Entity name:_____ Current date: 13/10/2010

Test case:_____ Previous date: 12/11/2008

Principle	Average Results: Current Performance	Average Results: Past Performance
Major changes trigger suitable risk assessments	38	30
Risk management is integrated with strategy development	27	45
There is an effective control environment	26	12
We learn from successes and failures	37	25
Accountability for managing risk is clearly defined	71	46
Risk is managed using effective, integrated processes	28	21
We are able to respond efficiently and effectively to disruptive events	67	10
We manage risk effectively within projects	66	18
Overall average score	**45**	**26**



Source: Broadleaf Capital International Pty Ltd.

2004 version of that standard and the associated handbook of best practice. He is also the nominated expert on the ISO Working Group on Risk Management that wrote ISO 31000:2009. He has co-authored a number of other risk management publications.

1 Financial Reporting Council, *The UK Corporate Governance Code* (London: Financial Reporting Council, June 2010).

2 Institute of Directors in Southern Africa, *King Code of Governance for South Africa 2009* (Johannesburg: IoDSA, September 2009).

3 ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations*, 2nd Edition (Sydney: ASC Corporate Governance Council, August 2007).

4 International Standards Organization, ISO 31000:2009, Risk Management—Principles and Guidelines, 1st Edition (Geneva: ISO, 2009).

5 Ibid., Annex A (informative) "Attributes of Enhanced Risk Management."