# EMBEDDING RISK MANAGEMENT PRACTICES FOR IMPROVED ORGANISATIONAL PERFORMANCE

By: Patrick Ow

Improving business results require risk management practices to be simplified and embedded seamlessly into normal business operations, planning and budgeting processes, and organisational culture. It is no longer an add-on or a management fad. Private and public sector organisations alike have struggled to understand risk management implementation steps and techniques. For those who have overcome it, they are reaping the fruits of their labour

High performing organisations, having developed strategies through a sound strategic planning process, must ruthlessly implement strategies by removing performance barriers or risk through enterprise-wide risk management practices.

Organisations can implement their strategy and perform well if:

* Everyone understands strategic, unit and departmental objectives, measures and targets and key priorities (clarity).
* Everyone is connected emotionally and engaged to strategic themes, key objectives and organisational priorities (commitment).
* There is clear “line-of-sight” for each individual, department, and unit so that they are closely aligned to the organisation’s key priorities (translation).
* Structure, system and cultural barriers are removed through embedded enterprise- wide risk management process (enabling).
* Everyone works together to arrive at better ways to achieve objectives and targets, removing “it’s not my job” thinking (synergy).
* Individuals are responsible for achieving targets (accountability).
* Everyone is a de facto risk manager (responsibility).

Risk is the likelihood of something happening (either positive or negative) that will have a consequence or impact (arising from the event) upon the achievement of objectives. Risk management standard AS/NZ 4360:2004 defines risk as “the chance of something happening that will have an impact on objectives.”

**Risk = Likelihood X Consequence**

Like the risk management process itself, an enterprise-wide approach (or commonly known as enterprise risk management, ERM) to manage risks arose from the business sector and it is being adopted by public and not for-profit organisations around the world.

The Committee of Sponsoring Organisations of the Treadway Commission (COSO) has broadly defined ERM as “a process, affected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage

**Table 1** Risk & Control Cycle

| Risk/Control Cycle | Description | Key Questions |
|---|---|---|
| Set/Confirm Objectives | Clarify what the organisation seeks to achieve, starting with its vision and strategic objectives. | • What are we trying to achieve? |
| Identify Events/Risk to Achieving those Objectives | Identify all events and risks that may affect/ impact the achievement of these objectives. | • What could go wrong?<br>• What could happen that would affect our objectives? |
| Assess Risks | Assess *likelihood* that each risk will materialise and calculate the *consequences* arising from the risk. | • What is the *likelihood* or probability that the risk will occur?<br>• What is its *consequence* or impact if the risk does eventuate? |
| Identify Risk Responses | Identify and select cost-effective responses to managing risk, based on a Board – approved risk appetite. | • What are the risk responses or options available to us to address risk? |
| Execute Control Activities To Address Risk | Implement cost-effective risk control activities to address or mitigate risks, as encapsulated in a risk management plan. | • How do we rate the control effectiveness?<br>• In the light of risk control assessment and prioritisation, what is the most cost-effective way to address/mitigate the risk? |
| Develop Effective Information and Communication | Develop cost-effective information and communication systems and processes to enable the organisation in meeting its objectives, and for timely reporting of risks and decision-making. | • How can we integrate risk as well as performance information and indicators into our everyday business performance reporting and decision-making processes? |
| Implement On-going Monitoring Activities to Ensure Controls are Effective | Once risk controls are established, develop and implement on-going cost effective monitoring activities to ensure that risk management and control practices continue to operate effectively and efficiently as an integral part of organisational culture and business processes. | • How do we use information management systems and technologies/IT to maintain or enhance our on-going risk monitoring and performance reporting capability? |

risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." The enterprise-wide approach to risk management does not necessarily negate or replace the traditional risk management process and mitigating risk controls, which is summarised in Table 1. Controls are policies, procedures, practices and organisational structures designed to provide reasonable assurance that operations are effective and efficient, organisational reporting is complete, reliable, accurate and timely, and that all applicable laws and regulations are complied with.

Effective risk management calls for a collaborative approach involving all parts of the organisation. Taking an enterprise-wide approach to risk management is vital as risk in different units may be within the risk appetite of that individual unit. Taken together, that unit's risk might exceed the risk appetite of the organisation as a whole – in which case, different risks responses may be required to bring the individual unit's risk in line with the organisation's risk appetite.

The starting point is the organisation's objectives, encapsulated by their vision and strategy.

realistic, and timed) performance measures and quantifiable targets are developed. Measures and targets are important as what gets measured gets managed and done.

From the highest level, guided by organisational structure, organisational vision and strategies are cascaded down and forms the strategic objectives, and performance measures and targets, which in turn cascades down, is weighted and forms each business and supporting units' objectives, and performance measures and targets. Then it cascades down further as departmental and project objectives where applicable. Ultimately, all objectives must be cascaded into everyone's individual performance objectives, as measured by their annual performance plan. (See Diagram 1).

Prioritise objectives throughout each level of the organisation. For prioritisation, develop strategic themes (or value drivers) that align to the organisational vision and strategy. Examples of strategic themes include revenue growth, sustainable outcomes and efficiency. Eliminate organisational activities or initiatives that do not support strategy implementation. The prioritisation process ensures clear focus or line-of-sight performance for everyone within the organisation.

**Diagram 2** Cascading Corporate Measures using the Balanced Scorecard Approach

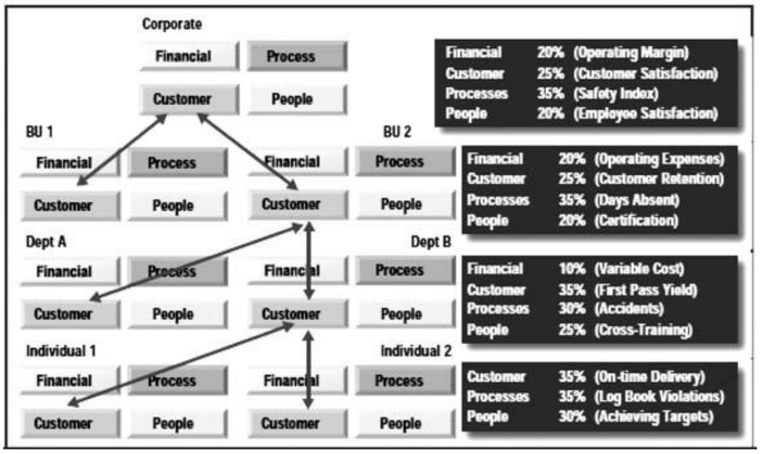
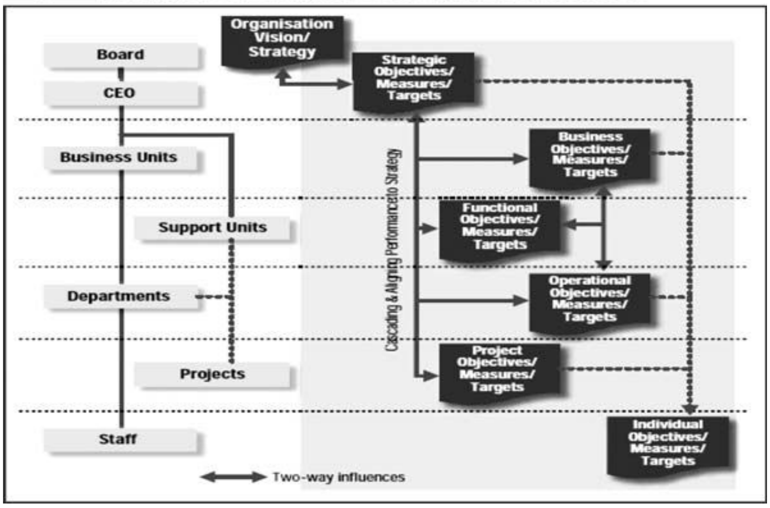


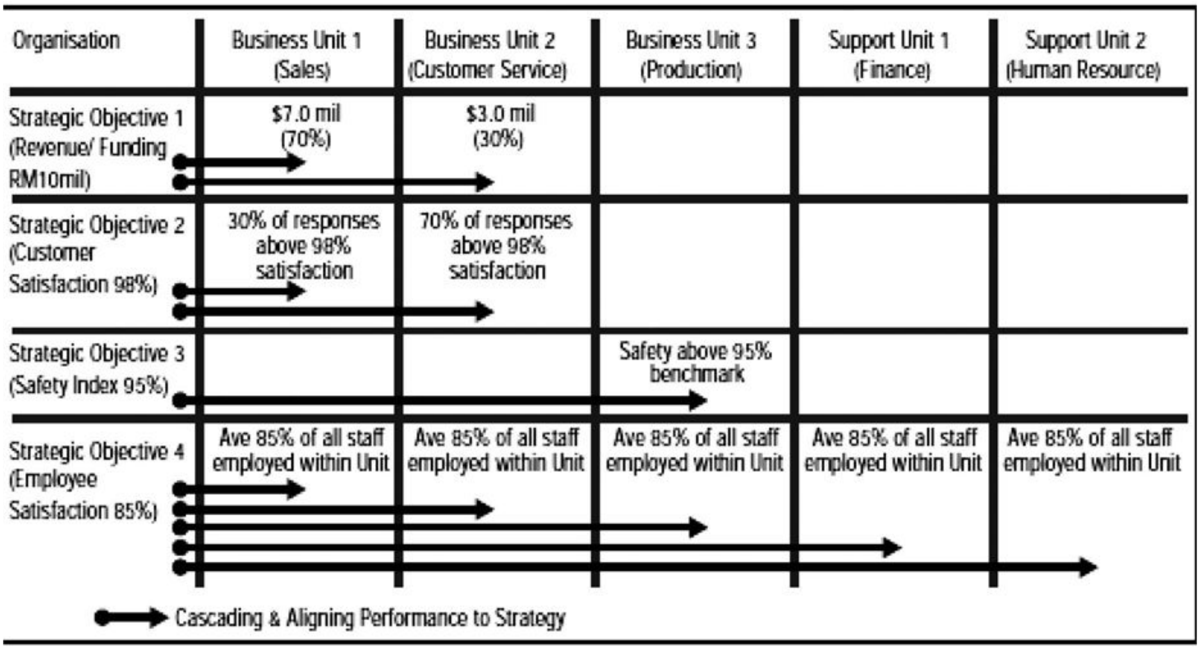

**Diagram 1** Mapping the Cascading Process to Organisational Structure




From objectives, SMART (specific, measurable, achievable, Use management tools like the balanced scorecard to cascade down top-level objectives, and performance measures and targets systematically throughout the organisation, right down to each individual, which is based on four perspectives (financial, customer, processes, and people).1 (See Diagram 2)

1 "Beyond Measurement Alone – Optimising Corporate Performance," Accountants Today, November 2005, page 48.

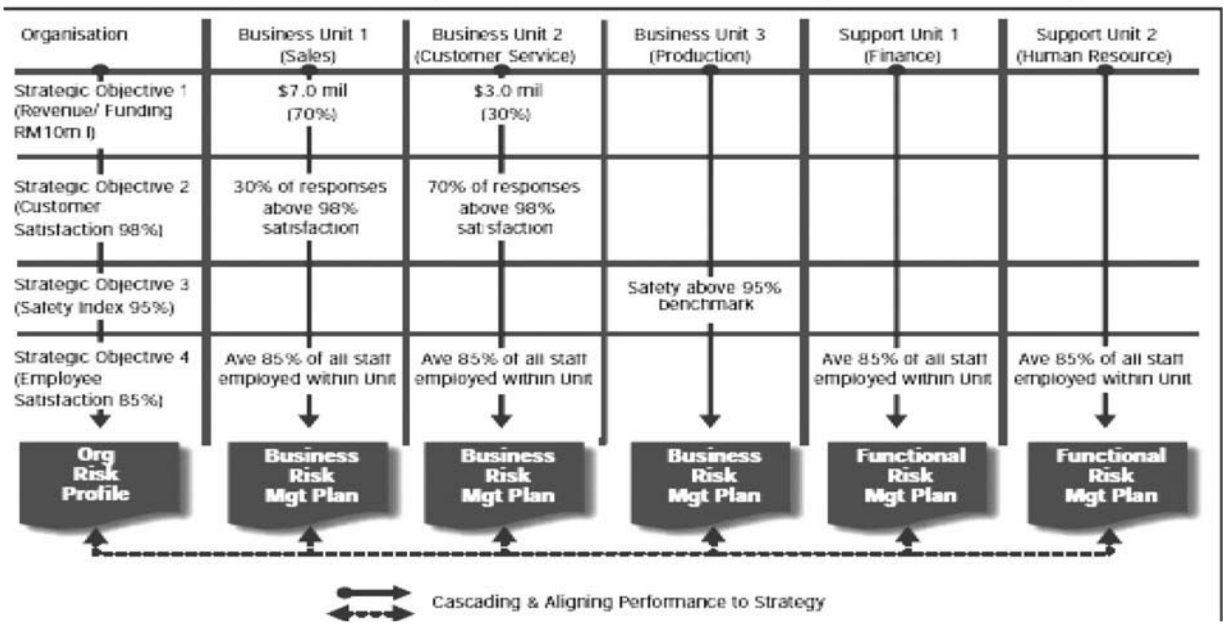
**Diagram 3** Cascading and Aligning Corporate Measures Enterprise-Wide




Map and allocate each strategic objective into business and support units' objectives as shown in Diagram 3. Not all strategic objectives are applicable to all units. "Weight" the achievement of each unit for clarity so that individuals managing their own unit are clear about their unit performance, avoiding any finger pointing. Eliminate joint responsibilities.

Thereafter, develop risk management plans for each level of objectives (whether strategic, business, functional, operational and project) as an integral part of organisational culture, planning and budgeting processes, and performance management practices. (Shown in Diagram 4)

**Diagram 4** Developing and Integrating Individual Risk Management Plans Enterprise-Wide



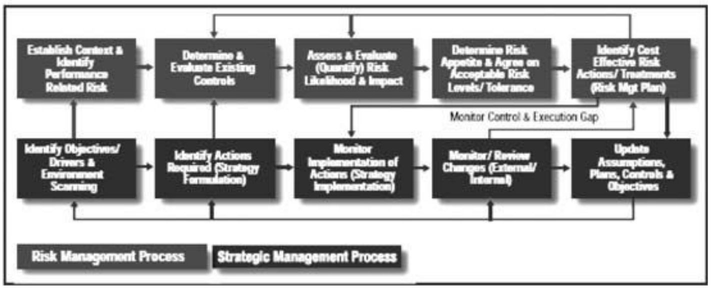
All risk management plans interact with each other constantly, "passing" risk items up and down through different organisational levels based on its implementation capability over the risk items. Criteria for passing risk are categorisation, materiality and/or impact upon the organisation - similar to perhaps the criteria for passing information to the Board.

For example, if a unit cannot address risk solely by itself because they do not have control, influence and/or authority over the implementation of the risk control, that unit's risk must be passed up as a risk item into the organisational risk profile for corporate action.

Alternatively, if the risk control was operational in nature within that unit, the Unit Head would pass down that risk item into the department's risk management plan for the Department Head's attention. The Department Head would then be responsible for that risk. This interaction process ensures that someone will act upon risk identified from any part of the organisation.

Integrate the risk management process into the strategic management process if organisational culture and processes permits as shown in Diagram 5.

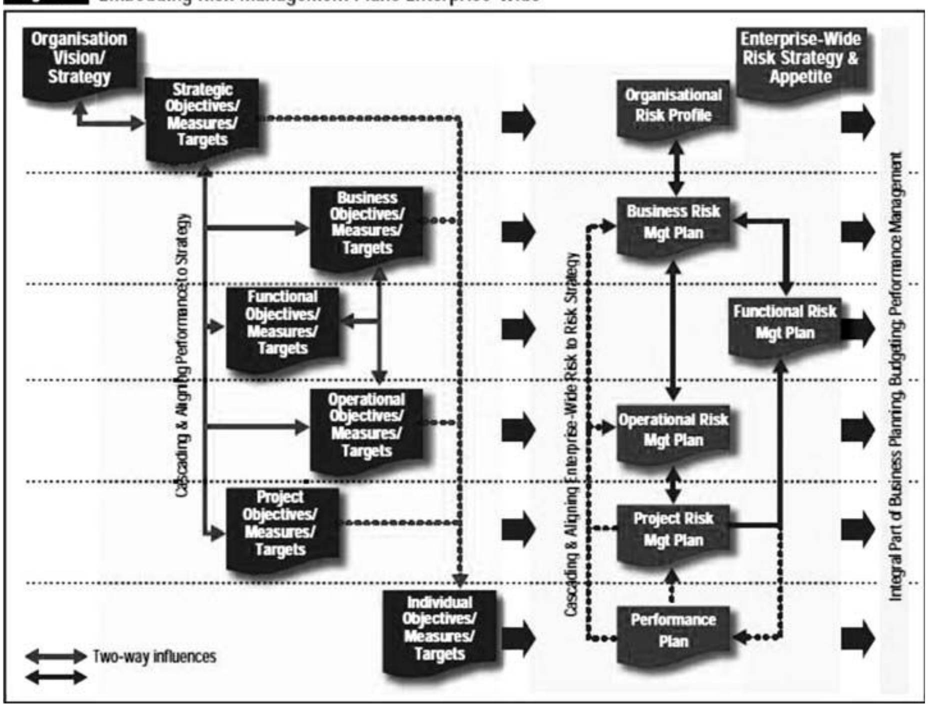
**Diagram 5** Integrating Risk Management into Strategic Planning Process[2]




For example, accompany business proposals with a sub-section on risk management. The risk management sub-section clearly sets out all key risks affecting the achievement of the business proposal, clearly identifying responsibility and accountability for risk control, what funding is allocated from existing (or future) budgets to address these risks and whether the business proposal clearly promotes the achievement of organisational strategy through clear measurable output and/ or outcomes.

As part of a manager's monthly performance report, include a section on risk management, identifying issues or risk potentially affecting the manager's performance for their unit or department. This way, risk management is not about box ticking but becomes an integral part of performance reporting and management. Therefore, risk management must NOT be an add-on or separated as an independent activity. Risk management must be part of organisational culture, embedded as part of everyday organisational life as shown in Diagram 6. The risk management plan is therefore a "living document" embedded as a sub-set of performance reporting and budget reviews, where risk and achievements are constantly monitored and evaluated against strategy and objectives.

**Diagram 6** Embedding Risk Management Plans Enterprise-Wide



Take note of the following: 1. Avoid silo-based risk management practices as changes to one part of any system or organisation will affect other parts since the whole can exceed the sum of its parts. 2. Supporting units' objectives must support the achievement of business units' objectives. 3. Adequately resource risk controls activities from budgets but prioritise against strategic themes. Otherwise, risk management plans become meaningless. 4. Monitor and report on risk activities through performance reports, rather than specific risk reports. Integrate risk reporting into performance ormonthly reports as it aids the achievement of business results, providing management with assurance that a responsible person is continuously monitoring or implementing risk controls. 5. Rename your Risk and Audit Department to Business Assurance Department. 6. Avoid "risk manager" job titles since risk ownership is a collective matter. Using one of the many approaches shown in Table 2, inputs, activities, outputs, and outcomes are chain of events that describe organisational, unit and departmental performance. Inputs (e.g. qualified trainers recruited) lead to activities (e.g. training activities), which lead short-term out puts (e.g. number of training sessions conducted). At some point, the customer or beneficiaries served by organisational activities will either achieve or not achieve the long-term outcomes (e.g. improvement in staff competencies and behaviours as the long-term result of the training).

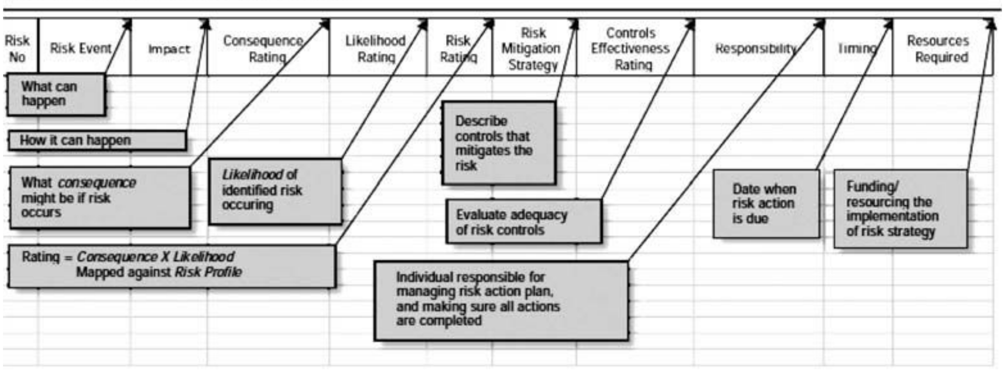
Inputs and activities answer the question "Are we doing things right?" whereas outputs and outcomes answer the question "Are we doing the right things?" By measuring/ quantifying the chain of events, we are able to determine the performance barriers or risk, which would feed into risk management plans. Knowing the measures help in the risk identification process.

Subsequently, risk management plans (Diagram 7) can be developed from the inputs, activities, outputs, and outcomes chain of events. The risk management plan sets out cost-effective risk controls required to achieve objectives, evaluation of risk likelihood and consequences, and determine inherent risks the organisation is prepared to accept in line with the Board-approved risk appetite as encapsulated it its Enterprise-wide Risk Strategy.

**Table 2** Risk & Control Cycle

| Item | Description | Sample Performance Indicators/ Measures |
|---|---|---|
| Objectives | • Goal, planned or intended outcome. | • Improve quality of learning and student performance. |
| Inputs | • Resources consumed by the system, including cost/workforce.<br>• Financial/staffing. | • Government Funds — \$30.0 mil.<br>• 100 qualified trainers. |
| Activities | • Steps to produce the output.<br>• Quality, quantity, timeliness, efficiency. | • 2,000 training hours.<br>• 1,000 workshop hours. |
| Outputs | • Products & services produced.<br>• Productivity (units of work). | • 20,000 trained teachers.<br>• 4.3 million new textbooks.<br>• 90% trainer satisfaction. |
| Outcomes | • Results that accomplish the mission; impacts.<br>• Behaviour changes.<br>• Programme/service effectiveness. | • 20% increase in student test scores.<br>• 10% increase in future earnings of primary school graduates. |
| Risk and Critical Assumptions | • Assumptions are risk and enabling factors. They are external conditions that are outside the direct control of the organisation.<br>• Achieving objectives can depend on whether assumptions hold true.<br>• Assumptions are made about the degree of uncertainty (degree of risk) between different levels of objectives. | • Inadequate provision of Government funding.<br>• Selected trainer is competent.<br>• Students have the ability to concentrate. |

**Diagram 7** Sample Risk Management Plan




Cont'd on page 24