Most of us own an automobile and probably risk manage its operation without too much thought. Consider the following questions:

- Have you serviced the car in the last 12 months?
- Does the car have a dashboard that contains various warnings (temperature gauge, oil light)?
- Does it have a logbook?

Hopefully you have answered yes to these questions as this is the accepted way of managing the ongoing risk of a vehicle. Now ask the same questions about your business:

- Do you self-assess the future potential risks of each business unit?
- Do you collect and monitor a set of key risk indicators?
- Do you record past loss events in a systematic manner?

Yes answers are less likely. This implies that we are prepared to run our businesses without the fundamental risk management functions we associate with our car, which seems incongruous with the stakeholders’ value we are entrusted with.

Operational risk management has been brought sharply into focus for financial institutions around the world thanks to the new Basel II Regulatory framework. However, the principles of operational risk management have relevance to all corporate, government and financial institutions regardless of whether their prudential watchdog requires it or not.

Ultimately sound operational risk management will encourage a risk conscious culture within any organisation that can reduce the likelihood and mitigate the negative consequences of operational risk events occurring. Business should be doing sound operational risk management anyway.

This article discusses the key components of an operational risk framework with particular emphasis on identification, measurement and reporting concepts. These concepts are developing as ‘Best practice’ among financial institutions worldwide and provide a good benchmark when developing methodologies.

We are fortunate in Australia to have one of the best risk management standards in the world, the AUS/NZ 4360 Risk Management standard. This standard considers the following framework for managing risk:

1. Establishing the Context
2. Risk Identification
3. Risk Analysis and Measurement
4. Evaluating the Risks
5. Treating the Risks
6. Monitoring and Reviewing
7. Communicating and Consulting.

ESTABLISHING THE CONTEXT

In conjunction with considering the organisation’s structure, culture and overall objectives it should also consider the objectives of operational risk management being to:

- Minimise the negative impact of operational risk events on the organisation;
• Minimise the level of operational risk to an economically viable level;
• Meet the expected risk levels of regulators, shareholders and other external bodies;
• Reduce the level of capital required to cover operational risk; and
• Develop a strong risk culture within the organisation.

RISK IDENTIFICATION, ANALYSIS AND MEASUREMENT
The key risk identification and analysis methods are:
• Risk and control self assessment.
• Monitoring of key risk indicators
• Analysing past risk events that have occurred (loss database).

As these processes aim to identify risks as well as measure and analyse those risks we will consider these two framework steps together. We will also consider a practical application of these methods to a common business unit in most organisations, the human resources (HR) department (see figure 1).

Risk and Control Self-assessment
Self-assessment looks at future or potential risk events that could take place in an organisation. A detailed approach to self-assessment for each business unit would contain the following steps:
• Identify the objectives, critical success factors and key processes of the business unit;
• Identify key risks for the business unit;
• Assess the controls aimed at mitigating the risks from occurring or their consequence if they did occur;
• Assess the residual likelihood and consequence of the risk after controls;
• Assess the importance and effectiveness of the controls; and
• Accept the residual risk or take further action to treat or limit the risk.

We now apply these concepts to a human resources department: (See figure 2).

As a result of the assessment, management may decide that for positions that are potentially exposed to fraudulent activities, HR will be required to obtain a criminal history check for any candidate during their parole period. Having assessed the importance of controls, compliance or the internal audit function is then in a better position to focus on key controls in its testing programs and boards are able to gain greater comfort that risks are being considered across all areas of the organisation in a systematic manner.

Key Risk Indicators
Recording of Key risk indicators (KRI) to forewarn the institution of higher levels of operational risk is similar to the concept of key performance indicators being used to assess the financial performance of an organisation. As an example, the human resources department may have KRI’s that relate to the level of overtime, staff turnover, complaints, dismissals and new employees. Over time, as information relating to each indicator is stored in a systematic manner, the organisation is able to identify any deviations from long-term trends. Such deviations may be indicative that operational risk levels are changing within that department either due to new staff, a tighter labour market or growth pressures.

Issues to consider when establishing appropriate key risk indicators are:
• Is the data to complete the KRI readily available?
• What is the strength of relationships to the key risks identified in the self-assessment phase?

![Diagram of Risk Management Process](image_url)
Figure 2

**IDENTIFY OBJECTIVES, CRITICAL SUCCESS FACTORS, PROCESSES**

<table>
<thead>
<tr>
<th>OBJECTIVES</th>
<th>CRITICAL SUCCESS FACTORS</th>
<th>PROCESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure staff have the appropriate skill sets to perform duties.</td>
<td>Adequate budget for staff training.</td>
<td>Requests for staff from business unit managers.</td>
</tr>
<tr>
<td>Hire staff that will perform their duties with integrity.</td>
<td>Adequate budget for payroll to attract appropriate candidates.</td>
<td>Understanding the vacant role and its responsibilities.</td>
</tr>
<tr>
<td></td>
<td>Adequate staff to assess candidates.</td>
<td>Advertise the role.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identifying and interviewing key candidates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Checking references.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contract offering and acceptance.</td>
</tr>
</tbody>
</table>

**IDENTIFY KEY RISKS**

- Potential candidates misrepresent their skill sets.
- Potential candidates have fraudulent intent.

**ASSESS CONTROLS RELEVANT TO EACH RISK**

<table>
<thead>
<tr>
<th>Risk assessed</th>
<th>Controls</th>
<th>Degree to which control reduces likelihood</th>
<th>Degree to which control reduces consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misrepresent skill set</td>
<td>Minimum two written references required.</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Verbal contact with prior employer as to duties performed.</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Fraudulent intent</td>
<td>Minimum two written references required.</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

**ACCEPT RESIDUAL RISK OR ADDITIONAL TREATMENT?**

- What is the operating norm for the KRI values?

**Loss Event Database**

Regardless of the strength of controls and treatment methods, operational losses will occur. At present, many of these losses cause heart palpitations for those involved in the short term and are documented in an ad hoc manner for board reporting and then simply filed in the long-term memory of the senior executives involved. An effective operational risk framework will, however, look to record and report these losses in a consistent, efficient and accessible manner to both the board and senior executives.

Loss event recording should:
- Record the event and its cause in a systematic manner;
- Record the net direct cost to the organisation after considering any insurance claims;
- Record any indirect effects on staff, reputation and customers; and
- Provide the user with the ability to recommend action or improvements that will reduce the likelihood of the event from occurring again, or its consequence.

Prior losses can then be analysed to identify key risks events that are consistently occurring in the organisation.

**EVALUATING AND TREATING THE RISKS**

Having identified and assessed the risks across the business units through the above methods, the organisation can then:
- Set trigger/escalation points for the level of risk undertaken;
- Accept the residual risk as part of doing business but be fully aware of potential consequences;
- Avoid the risk by exiting the activity;
- Reduce the risk
  - Reduce the likelihood of the risk occurring by increasing controls as was the case in the HR example;
  - Mitigate the consequence by creating contingency plans;
- Transfer the risk through insurance or hedging activities; and
- Transform the risk through outsourcing activities.
MONITORING, REVIEWING AND REPORTING
Having established a Self-assessment, KRI and loss event framework, consideration then needs to be given to reporting relevant information through to senior management and the board in an easy to understand and ongoing manner.

Self-assessment Reporting
For Self-Assessment at the business unit level, likelihood and consequence maps (Heat Maps) can be considered that highlight the reduction in risk as a result of controls. Management focus would be on those risks in the hot and upper warm zones. Compliance would focus on controls that were assessed as reducing the impact of risks to a large degree. An example report could be:

Key Risk Indicator Reporting
For KRIs, historical trend lines could be used to identify expected long-term values. Dashboard or scorecard-based reporting that looks at movements in the relevant KRI each month and maps them to low, medium or high risk zones based on expected values can also be considered as per the HR example (figure 4) below.

Loss Event Reporting
Loss event information can be reported in a number of ways but should, as a minimum, report net losses at the business unit level and by key risk event categories. Other issues to consider in the reporting process are:
- Whether the events are still open to incur further losses;
- Any substantial indirect effects; and
- The capacity to review suggested improvements.

CONCLUSION
Let your board and management team know – operational risk management is here and it involves everyone. If embraced, it can only serve to enhance risk awareness in your organisation and reduce unnecessary operational losses from impacting your bottom line.

David Bergmark, Protecht Advisory, david.bergmark@protecht.net
David Tattam, Protecht Advisory, david.tattam@protecht.net