Five steps to Enterprise Risk Management

by

Val Jonas CEO Risk Decisions Group
Five steps to Enterprise Risk Management

Introduction

With the changing business environment brought on by events such as the global financial crisis, gone are the days of focussing only on operational and tactical risk management. Enterprise Risk Management (ERM), a framework for a business to assess its overall exposure to risk (both threats and opportunities), and hence its ability to make timely and well informed decisions, is now the norm.

Ratings agencies, such as Standard & Poors, are reinforcing this shift towards ERM by rating the effectiveness of a company’s ERM strategy as part of their overall credit assessment. This means that, aside from being best practice, not having an efficient ERM strategy in place will have a detrimental effect on a company’s credit rating.

Not only do large companies need to respond to this new focus, but also the public sector needs to demonstrate efficiency going forward, by ensuring ERM is embedded not only vertically but also horizontally across their organisations. This whitepaper provides help, in the form of five basic steps to implementing a simple and effective ERM solution.

This is first of a series of whitepapers on Enterprise Risk Management. Future papers will expand on each of the steps in this whitepaper as well as continuing to cover Governance and Compliance.

Step 1 – Establish an Enterprise Risk Structure

ERM requires the whole organisation to identify, communicate and proactively manage risk, regardless of position or perspective. Everyone needs to follow a common approach, which includes a consistent policy and process, a single repository for their risks and a common reporting format. However, it is also important to retain existing working practices based on localised risk management perspectives as these reflect the focus of operational risk management.

The corporate risk register will look different from the operational risk register, with a more strategic emphasis on risks to business strategy, reputation and so on, rather than more tactical product, contract and project focused risks. The health and safety manager will identify different kinds of risks from the finance manager, while asset risk management and business continuity are disciplines in their own right. ERM brings together risk registers from different disciplines, allowing visibility, communication and central reporting, while maintaining distributed responsibility.

In addition to the usual vertical risk registers, such as corporate, business units, departments, programmes and projects, the enterprise also needs horizontal, or functional risk registers. These registers allow function and business managers, who are responsible for identifying risks to their own objectives, to identify risks arising from other areas of the organisation.

The enterprise risk structure should match the organisation’s structure: the hierarchy represents vertical (executive) as well as horizontal (functional and business) aspects of the organisation. This challenges the conventional assumption that risks can be rolled up automatically, by placing horizontal structures side by side with vertical executive structures. Risks should be aggregated using a combination of vertical structure and horizontal intelligence. This is a key factor in establishing ERM.
Step 3 – Create an enterprise risk map

Risk budgeting and common sense dictate that risks should reside at their local point of impact, because this is where attention is naturally focused. However, the risk cause, mitigation or exploitation strategy may come from elsewhere in the organisation and often common causes and actions can be identified. In this case, we take a systemic approach, where risks are managed more efficiently when brought together at a higher level. To achieve this, we need to be able to map risks to different parts of the risk management structure.

To create an enterprise risk map, you need:

- a set of global categories to communicate information to the right place
- the facility to define the relationships between risks (parent, child, sibling etc)
- scoring systems with consistent common impact types

Global categories

Functional and business managers should use these global categories to map risks to common themes, such as strategic or business objectives, functional areas and so on. These categories then provide ways to search and filter on these themes and to bring common risks together under a parent risk.

Risk relationships

For example, if skills shortage risks are associated with HR, the HR manager can easily call up a register of all the HR risks, regardless of project, contract, asset, etc. across the organisation and manage them collectively.

Similarly, the impact of a supplier failing on any one contract may be manageable. But across many contracts could be a major business risk. In which case, the supply chain function needs to bring the risks against this supplier together and to manage the problem centrally.

Each Risk Management Cluster will include both global and local categories in a Predict! Group, so that each area of the organisation needs only to review relevant information.

Step 2 – Assign responsibility

Once an appropriate enterprise risk structure is established, assigning responsibility and ownership should be straightforward. Selected nodes in the structure will have specified objectives; each will have an associated manager (executive, functional or business), who will be responsible for achieving those objectives and managing the associated risks. Each node containing a set of risks, along with its owner and leader, is a Risk Management Cluster.*

Vertical managers take executive responsibility not only for their cluster risk register, but also overall leadership responsibility for the Risk Management Clusters below. Responsibility takes two forms: ownership at the higher level and leadership at the lower level. For example, a programme manager will manage his programme risks, but also have responsibility for overseeing risk within each of the programme’s projects.

Budgetary authority (setting and using Management Reserve), approval of risk response actions, communication of risk appetite, management reporting and risk performance measures are defined as part of the Owner and Leader roles as illustrated in Figure 3. This structure is also used to escalate and delegate risks.

Horizontal managers take responsibility for their own functional or business Risk Management Clusters, but also for gathering risks from other areas of the Enterprise Risk Structure related to their discipline. For example, the HR functional manager will be responsible for identifying common skills shortfall risks to bring them under central management. Similarly, the business continuity manager will identify all local risks relating to use of a test facility and manage them under one site management plan. To assist in this, we use an enterprise risk map – see Step 3.

*Risk Management Clusters® are unique to the Predict! risk management software

Figure 3: Vertical management chain of Owners and Leaders

Figure 4: Global categories
baseline, both of which should be recorded against each Risk Management Cluster®.

Enterprise-wide reporting allows senior managers to review risk exposure and trends across the organisation. This is best achieved through metrics reports, such as the risk histogram. For example, you might want to review the risk to key business objectives by cluster. Or how exposed different contracts and projects are to various suppliers.

Furthermore, there is a need to use a common set of reports across the organisation, to avoid time wasted interpreting unfamiliar formats. Such common reports ensure the risk is communicated and well understood by all elements of the organisation, and hence provide timely information on the current risk position and trends, initially top-down, then drilling down to the root cause.

**Step 4 – Decision making through enterprise risk reporting**

The most important aspect of risk management is carrying out appropriate actions to manage the risks. However, you cannot manage every identified risk, so you need to prioritise and make decisions on where to focus management attention and resources. The decision making process is underpinned by establishing risk appetite against objectives and setting a
(as risks) before they arise, you have far more options available to affect a ‘Left Shift: from a costly and overly long process to one better matching the original objectives set!

Most organisations have pockets of good risk management, many have a mechanism to report ‘top N’ risks vertically, but very few have started to implement horizontal, functional or business risk management. Both a bottom up and top down approach is required. An ERM initiative should allow good local practices to continue, provided they are in line with enterprise policy and process (establishing each pocket of good risk management as a Risk Management Cluster will provide continuity).

From a top-down perspective, functional and business focused risk management needs to be kick started. A risk steering group comprising functional heads and business managers is a good place to start. The benefits of such a group getting together to understand inter-discipline risk helps break down stove-piped processes. This can trigger increasingly relaxed cross-discipline discussions and focus on aligning business and personal objectives that leads to rapid progress on understanding and managing risk.

Finally, to ensure that an organisational culture shift is affected, the senior management must be engaged. This engagement is not only aimed at encouraging them to see the benefits of managing risk, but to also help the organisation as a whole see that proactive management of risk (the Left Shift principle) is valued by all.

A Risk Management Masterclass for the executive board and senior managers can provide them with the tools necessary to progress an organisation towards effective ERM.

The benefits

ERM delivers confidence, stability, improved performance and profitability. It provides:

- Access to risk information across the organisation in real time
- Faster decision making and less ‘fire fighting’
- Fewer surprises (managed threats and successful opportunities)
- Improved confidence and trust across the stakeholder community
- Reduced cost, better use of resources and improved morale
- Stronger organisations resilient to change, ready to exploit new opportunities

Over time this will:

- Increase customer satisfaction, enhance reputation and generate new business
- Safeguard life, company assets and the environment
- Achieve best value and maximise profits
- Maintain credit ratings and lower finance costs

Summary

All of the risk management skills and techniques required to implement Enterprise Risk Management can easily be learned and applied. From senior managers to risk practitioners, Masterclasses, training, coaching and process definition can be used to support rollout of Enterprise Risk Management.

Create a practical Enterprise Risk Structure, set clear responsibilities and hold people accountable. Define a simple risk map and provide localised working practices to match perspectives on risk. Be seen to make decisions based on good risk management information.

Enterprise Risk Management should be simple to understand and simple to implement.

Keep it simple! Make it effective!
Appendix 1: References


ISO Guide 73 – Risk management - Vocabulary

All of these publications are listed at www.riskdecisions.com

Appendix 2: Glossary

Where ‘source’ is in brackets, minor amendments have been incorporated to the original definition.

Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Budget</td>
<td>The resource estimate (in £/$s or hours) assigned for the accomplishment of a specific task or group of tasks.</td>
<td>Risk Decisions</td>
</tr>
<tr>
<td>Change Control (Management)</td>
<td>Identifying, documenting, approving or rejecting and controlling change.</td>
<td>(PMBOK)</td>
</tr>
<tr>
<td>Control Account</td>
<td>A management control point at which actual costs can be accumulated and compared to earned value and budgets (resource plans) for management control purposes. A control account is a natural management point for budget/schedule planning and control since it represents the work assigned to one responsible organisational element on one Work Breakdown Structure (WBS) element.</td>
<td>APM EVM guideline</td>
</tr>
<tr>
<td>Cost Benefit Analysis</td>
<td>The comparison of costs before and after taking an action, in order to establish the saving achieved by carrying out that action.</td>
<td>Risk Decisions</td>
</tr>
<tr>
<td>Cost Risk Analysis</td>
<td>Assessment and synthesis of the cost risks and/or estimating uncertainties affecting the project to gain an understanding of their individual significance and their combined impact on the project’s objectives, to determine a range of likely outcomes for project cost.</td>
<td>(PRAM)</td>
</tr>
<tr>
<td>Enterprise Risk Management</td>
<td>The application of risk management across all areas of a business, from contracts, projects, programmes, facilities, assets and plant, to functions, financial, business and corporate risk.</td>
<td>Risk Decisions</td>
</tr>
<tr>
<td>Enterprise Risk Map</td>
<td>The structure used to consolidate risk information across the organisation, to identify central responsibility and common response actions, with the aim of improving top down visibility and managing risks more efficiently.</td>
<td>Risk Decisions</td>
</tr>
<tr>
<td>Left shift</td>
<td>The practice by which an organisation takes proactive action to mitigate risks when they are identified rather than when they occur with the aim of reducing cost and increase efficiency.</td>
<td>Risk Decisions</td>
</tr>
<tr>
<td>Management Reserve (MR)</td>
<td>Management Reserve may be subdivided into:</td>
<td>APM EV/Risk Working Group</td>
</tr>
<tr>
<td>Non-specific Risk Provision</td>
<td>The amount of budget / schedule / resources set aside to cover the impact of emergent risks, should they occur.</td>
<td>APM EV/Risk working group</td>
</tr>
<tr>
<td>Operational Risk</td>
<td>The different types of risks managed across an organisation, typically excluding financial and corporate risks.</td>
<td>Risk Decisions</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
<td>Source</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Opportunity</td>
<td>An ‘upside’, beneficial Risk Event.</td>
<td>PRAM</td>
</tr>
<tr>
<td>Baseline</td>
<td>An approved scope/schedule/budget plan for work, against which execution is compared, to measure and manage performance.</td>
<td>(PMBOK)</td>
</tr>
<tr>
<td>Performance Measurement</td>
<td>The objective measurement of progress against the Baseline</td>
<td>APM EV/Risk Working Group</td>
</tr>
<tr>
<td>Proactive Risk Response</td>
<td>An action or set of actions to reduce the probability or impact of a threat or increase the probability or impact of an opportunity. If approved they are carried out in advance of the occurrence of the risk. They are funded from the project budget.</td>
<td>(PRAM)</td>
</tr>
<tr>
<td>Reactive Risk Response</td>
<td>An action or set of actions to be taken after a risk has occurred in order to reduce or recover from the effect of the threat or to exploit the opportunity. They are funded from Management Reserve.</td>
<td>(PRAM)</td>
</tr>
<tr>
<td>Risk Appetite</td>
<td>The amount of risk exposure an organisation is willing to accept in connection with delivering a set of objectives.</td>
<td>APM EV/Risk Working Group</td>
</tr>
<tr>
<td>Risk Event</td>
<td>An uncertain event or set of circumstances, that should it or they occur, would have an effect on the achievement of one or more objectives.</td>
<td>PRAM</td>
</tr>
<tr>
<td>Risk Exposure</td>
<td>The difference between the total impact of risks should they all occur and the Risk Provision.</td>
<td>APM EV/Risk Working Group</td>
</tr>
<tr>
<td>Risk Management Clusters®</td>
<td>Functionality in Risk Decisions’ Predict! risk management software that enables users to organise different groups of risks to form a single, enterprise-wide risk map.</td>
<td>Risk Decisions</td>
</tr>
<tr>
<td>Risk Provision</td>
<td>The amount of budget / schedule / resources set aside to manage the impact of risks. Risk provision is a component part of Management Reserve.</td>
<td>APM EV/Risk Working Group</td>
</tr>
<tr>
<td>Risk Response Activities</td>
<td>Activities carried out to implement a Proactive Risk Response.</td>
<td>APM EV/Risk Working Group</td>
</tr>
<tr>
<td>Schedule Risk Analysis</td>
<td>Assessment and synthesis of schedule risks and/or estimating uncertainties affecting the project ability to meet key milestones.</td>
<td>(PRAM)</td>
</tr>
<tr>
<td>Schedule Reserve</td>
<td>The schedule component of Management Reserve.</td>
<td>APM EV/Risk Working Group</td>
</tr>
<tr>
<td>Specific Risk Provision</td>
<td>The amount of budget / schedule / resources set aside to cover the impact of known risks, should they occur. It is not advisable to net opportunities against threats and so a separate value is calculated for each.</td>
<td>APM EV/Risk Working Group</td>
</tr>
<tr>
<td>Threat</td>
<td>A downside, adverse Risk Event</td>
<td>PRAM</td>
</tr>
<tr>
<td>Uncertainty</td>
<td>The spread in estimates for schedule, cost, performance arising from the expected range of outcomes. Often termed estimating error.</td>
<td>APM EV/Risk Working Group</td>
</tr>
</tbody>
</table>
About Risk Decisions

Risk Decisions Limited is part of Risk Decisions Group, a pioneering global risk management solutions company, with offices in the UK, USA and Australia. The company specialises in the development and delivery of enterprise solutions and services that enable risk to be managed more effectively on large capital projects as well as helping users to meet strategic business objectives and achieve compliance with corporate governance obligations.

Risk Decisions has introduced many innovative features that have since become standard features in the industry including the risk hierarchy tree, combined threat and opportunity risk impact grids and automated schedule risk analysis. The company plays a significant role in influencing risk management policy, making important contributions to APM, OGC and PMI risk management guides and standards, including guidance on interfacing risk with other disciplines, such as Earned Value and Systems Engineering. In 2010, Risk Decisions registered Risk Management Clusters® as a Trademark.

Clients include Balfour Beatty, Mott MacDonald, National Grid, HSBC Rail, BAE Systems, Selex, Raytheon, AgustaWestland, UK MoD, Australian Defence Materiel Organisation and New Zealand Air Force.

For further information visit: www.riskdecisions.com
or contact Alex Leggatt at: Risk Decisions Ltd,
Whichford House, Parkway Court,
Oxford Business Park South,
Oxford, OX4 2JY
Tel: 01865 718666,
Email: alex@riskdecisions.com