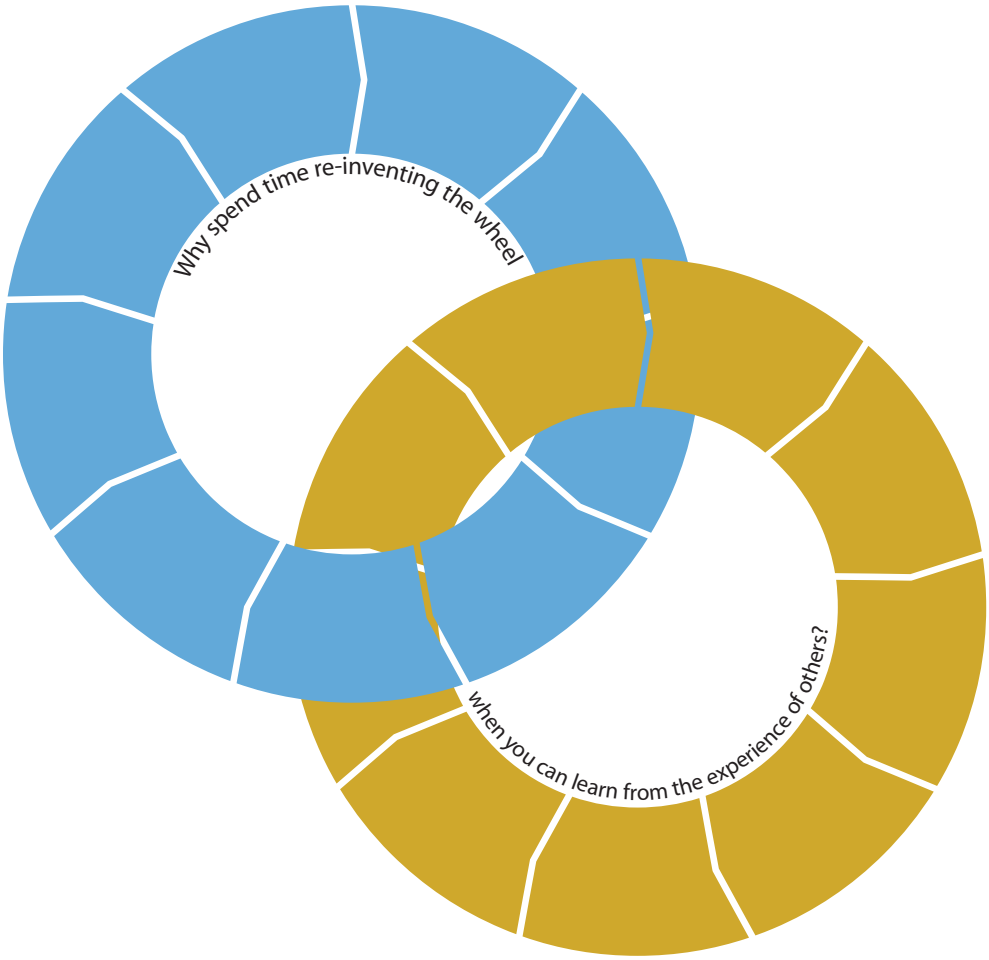
BPIR Management Brief - Volume 5, Issue 8

Enterprise Risk Management



BPIR.com
Business Performance Improvement Resource

NEW ZEALAND BUSINESS EXCELLENCE FOUNDATION

The BPIR Improvement Cycle

- *Identify/Select an Area for Improvement*
- *Measure Performance*
- *Benchmark Performance*
- *Identify a Relevant Improvement Approach or Strategy*
- *Learn How to Implement*
- *Identify Best Practice Organisations*
- *Research Further Information*
- *Implement a Best Practice Approach*
- *Review and Calibrate*

Welcome to Volume 5, Issue 8, of the BPIR.com Management Brief series

The Management Brief is published for members of the New Zealand Business Excellence Foundation (NZBEF).

The Management Brief provides best practices, innovative ideas and research data on topics and tools that will help you to stay up-to-date on the latest international business trends and practices.

NZBEF corporate members have password access (one password only) to its Business Performance Improvement Resource (BPIR) at www.nzbef.bpir.com. Further passwords, for organisational-wide access, can be obtained at a 20% discount from this site. For information on the NZBEF visit www.nzbef.org.nz.

Enterprise Risk Management (ERM): The Definition

Enterprise Risk Management (ERM) is a discipline that consolidates risk management throughout an organisation. It should be considered as a key component of organisational strategy, as it reduces the likelihood of potential catastrophic failures and increases the likelihood of organisational success.

The Stage

The leaders of today's most successful organisations are risk shapers rather than risk takers. Successful organisations do not shy away from addressing risk, regarding it as a source of growth and future business rewards. Today's global economy means that organisations have to use ERM if they want to master risk. Otherwise, they may well be enslaved by it. [1]

Author: Neil Crawford, BPIR.com Limited
Research Assistance: Kevin McKenna, BPIR.com Limited
Editors: Dr Robin Mann, Centre for Organisational Excellence Research, & Michael Adams, maag Consulting (Canada)

Expert Opinion

According to professional risk manager Mark Jablonowski, the real value of ERM is not found in short-term profitability gains. [2] ERM's essential value comes from the development of a wider corporate view of responsibility, which influences an organisation's managers, employees, and shareholders, as well as the community it serves. ERM forms part of the glue that holds corporate governance together. It contributes to an organisation's sustainable growth and long-term profitability.

Introduction to Risk Management

Risk management is an unconscious part of our daily lives – both in terms of avoiding possible negative consequences and seizing new opportunities. Quoting Carl Pritchard, Minnesh Kaliprasad, a cost engineer with Murray & Roberts Engineering Solutions in South Africa, states that effective risk management "means taking deliberate action to shift odds in your favour to increase the odds of good outcomes, and reducing the odds of bad outcomes." [3] [4]

The fundamental elements associated with a given risk are:

- the risk event itself
- the probability of its occurrence, and
- the impact of that risk occurring.

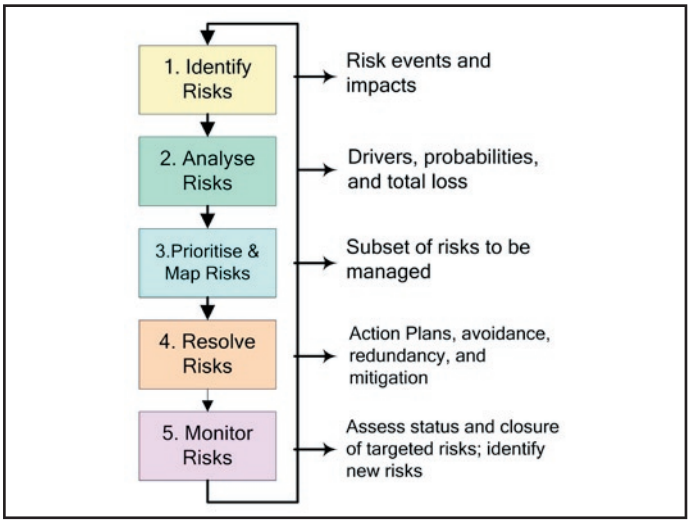


Figure 1: Risk Management Process (adapted from Smith and Merritt) [5]

The five-step risk management process depicted in Figure 1, see opposite, has been successfully used by major telecommunications and defence communication equipment manufacturers to mitigate project losses.

Step 1: Identify risks, beginning with structured brainstorming to list perceived risks that are likely to have a negative impact on a project.

Step 2: Analysis to classify the risk's relative threat to the project.

Step 3: Selecting and prioritising the most threatening risks for active management.

Step 4: Resolving risks through the creation of action plans.

Step 5: Monitoring risks to ensure that the identified risks have been adequately resolved, and that any new risks are incorporated into management processes. [5]

Mapping and Classifying Risks

According to the British journal *Financial Management*, the following steps should be involved when mapping and responding to risks:

1. Record risks in a register. List all identified risks together with their likelihood and associated consequences. A comprehensive register enables constant evaluation, and mapping helps to ensure that the significant risks receive appropriate attention.
2. Evaluate risks in accordance with the organisation's risk appetite (a risk appetite is the degree of risk that an organisation is prepared to embrace in the pursuit of its goals). The evaluation of risks is usually the responsibility of senior management, and involves setting parameters for the acceptance, rejection or management of risk.
3. Treat the risks, e.g. avoid, reduce, transfer or accept them as follows:
   i. avoidance, by withdrawing from high-risk activities
   ii. reduction, by introducing internal control mechanisms
   iii. transference, by using outsourcing, insurance or hedging
   iv. acceptance, i.e. deciding to take no action.

4. Report the risks. Inform the whole organisation about risks and the intended responses to them. Explain how risks are identified, assessed, and managed. [6]

Figure 2, below, prepared by Shannon Anderson and colleagues at Rice University in Houston, Texas, in the United States, lists some common organisational risk classifications and categories. [7]

1. Strategic Risk, relating to high-level goals associated with the support of an organisation's mission
▪ innovation risk ▪ intellectual property risk ▪ product/service failure risk ▪ misalignment of incentives risk ▪ partnering lock-in risk ▪ outside scope risk
2. Operational Risk, relating to the effective efficient use of an organisation's resources
▪ input supply risk ▪ surge capacity risk ▪ quality performance risk ▪ cost/price renegotiation risk ▪ coordination risk ▪ financial viability risk ▪ contribution valuation risk ▪ financial commitment risk
3. Reporting Risk, relating to the reliability of the organisation's reporting procedures
▪ verification and evaluation risk ▪ misalignment of incentives risk ▪ number of choices/average response time ▪ % of supply chain target costs achieved
4. Compliance Risk, relating to the organisation's compliance with applicable laws and regulations
▪ compliance risk ▪ regulatory risks

Figure 2: Common Organisational Risk Classifications and Categories

Professor Thomas Barton and colleagues, at the University of North Florida in the United States, write that many of the current global risks may be classed as "high impact but rare" events, yet the management of high-impact, rare-event risks is an aspect of ERM that is often overlooked.[8] The management of this category of risk is absolutely critical to the functioning of an effective ERM programme. It is sometimes tempting to view such rare events as being manageable only in a generalised way, and the lack of specificity associated with these events can, unfortunately, engender a lax and undisciplined approach to their management. Under an ERM framework, it would be unacceptable to categorise such events as being "not manageable" - and just to focus on more predictable, and potentially less-severe risks.

In ERM implementations, organisations designate rare events on risk maps (similar to Figure 3, below) as low-likelihood, high-impact events. A possible action plan for dealing with high-impact rare events includes the following:

- hiring risk consultants to bring a fresh perspective and to "think outside the box" for potentially unlikely but significant events
- assessing the impact and probability of identified risks
- determining the real root issues behind risks
- identifying strategic risks (i.e. external events) that might damage a company's growth trajectory, and decrease shareholder value. Risks may also be identified using scenario-analysis methodologies, by which managers are able to create and analyse a number of diverse possible futures to bring unexpected insights. Since analysis can never be totally accurate, ERM processes should be integrated with crisis management and business continuity planning. *(See BPIR Management Brief: Vol. 3, Issue 6 – Business Continuity Planning.)*

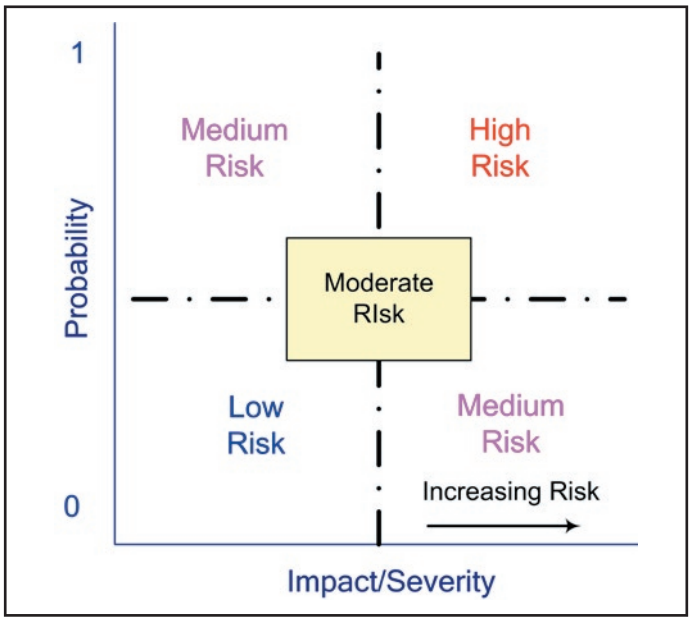


Figure 3: Risk Map Conceptual Diagram

The elements of risk associated with ERM may be divided into the following categories:

- the inherent level of risk (or the underlying level of risk) affecting an organisation, from which no corrective actions are contemplated
- the trend of risk events over a defined period, e.g. 12 months

- risk mitigation procedures, i.e. the steps taken to reduce potential risk to an acceptable level
- residual risk, i.e. the level of risk remaining after risk response strategies have been implemented.

Adapted from Dorminey and Mohn, the following residual risk density map (see Figure 4, below) shows three key zones associated with residual risks that remain after corrective actions have been applied. [9] These are:

1. Potentially over-mitigated, where the residual risk is very low and response strategies may have overcompensated, and allocated more resources than actually necessary.
2. Tolerance, where residual risk levels are deemed to be acceptable and no further action is envisaged.
3. Potentially under-mitigated, where residual risk remains unacceptably high. Each of these zones is directly related to an organisation's risk appetite.

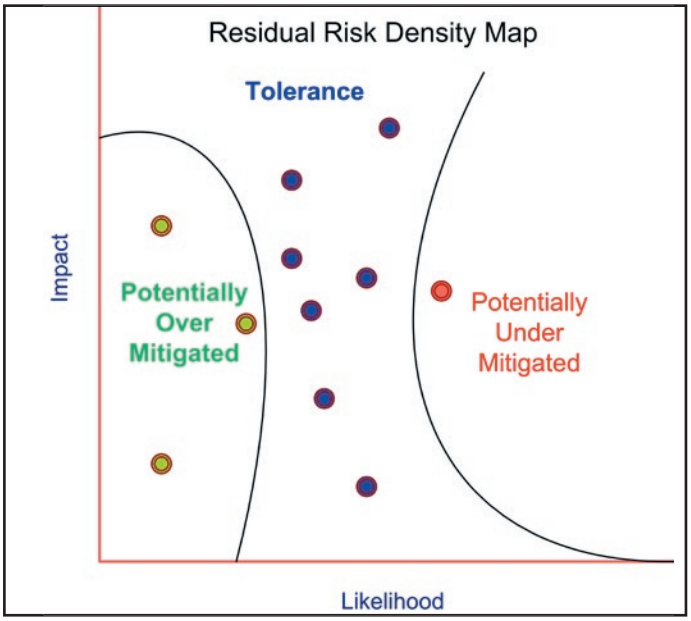


Figure 4: Residual Risk Density Map (adapted from Dorminey and Mohn) [9]

What are the Main Components of ERM?

In Figure 5, see next column, Gary Adams and Mary Campbell, of GR Consulting in Philadelphia, Pennsylvania, in the United States, describe the interrelated components that make up ERM: [10]

1. Culture	Establishing the basis for how risk is viewed within an organisation, including its risk management philosophy, risk appetite, integrity and ethical values.
2. Setting objectives	To ensure that processes are established for drafting and supporting, and also for aligning proposed objectives with the organisation's mission.
3. Event identification	Internal/external events that have an impact on the organisation's objectives should be identified, and opportunities channelled back into strategy/objective-setting processes.
4. Risk assessment	The analysis of the likelihood and impact of risks.
5. Risk responses selected	For example, avoiding, accepting, reducing or sharing risk, in accordance with the organisation's risk tolerances and risk appetite.
6. Control activities	Establishing policies and procedures, and implementing these to ensure that appropriate risk responses are effectively carried out.
7. Information and communication	Identifying, capturing, and communicating relevant information in a form/timeframe that enables staff to carry out their responsibilities.
8. Monitoring	Maintaining oversight of the entire ERM framework, and making modifications as necessary.

Figure 5: The Interrelated Components of ERM (adapted from Adams and Campbell) [10]

Given the wide range and complexity of risks to which organisations are exposed, it is not surprising that business leaders have sought to find effective infrastructures and tools for risk management. ERM systems keep CEOs and top leadership better informed of the impact of enterprise-wide risks, making it possible to set realistic priorities for action. Yves Nadeau, a partner with RSM Richter LLP in Montreal, Canada, writes that ERM frameworks offer a formally structured approach to risk management that enables organisations to:

- close unacceptable performance gaps by establishing risk impact/probability assessment processes and developing solutions
- eliminate organisational silos, and provide leaders with an enterprise-wide view of risk
- react promptly to change by fostering the proactive attitudes needed for identifying, understanding, and adapting to emerging risks
- align available resources for managing risks, controlling costs, and ensuring compliance

- take measured risks, while managing these risks effectively to create a competitive advantage and prepare the organisation to take advantage of new opportunities, and
- strengthen corporate governance, while increasing stakeholder and regulator confidence.

Nadeau also highlights the challenges associated with implementing risk management frameworks:

- difficulty in gaining management acceptance and support
- managing risks in isolation, which may lead to uncoordinated decision making
- responsibilities assigned for managing specific risks are sometimes unclear
- risks being managed only as they arise, leading to a reactive culture and short-term solutions
- poor awareness of potential risks as a result of limited communication between levels of management and functional groups
- risk management processes that focus merely on material losses or regulatory compliance requirements
- risk management activities not being appropriately prioritised or linked to the organisation's strategy and sources of value. [11]

Jack Dorminey and Richard Mohn of the Federal Reserve Bank of Richmond, Virginia, in the United States, describe the elements for successful ERM implementation in not-for-profit and governmental organisations. [9] The motivations and measures for success are somewhat different in not-for-profit organisations than in for-profit organisations, as depicted in Figure 6, below:

Motivations and Behaviours	
For-Profit	***Not-for-Profit/Government***
Profit Objective	Mandate/Mission Objective
Cost/Benefit	Cost/Competition
Efficiency Focus	Effectiveness Focus
Risk Seeking	Risk Avoiding
Value at Risk	Goal/Objective at Risk

Figure 6: ERM in For-Profit and Not-for-Profit Organisations (adapted from Dorminey and Mohn) [9]

Integrated Risk and Value Management

Citing Dr Mark Lawrence of McKinsey & Co., Melissa Wilkinson of *Charter* magazine in Australia, states "there has been an important shift in the nature and scope of risk management. It is no longer just an activity or tool to protect a firm from loss. There is now wide acceptance that it has moved well beyond the domain of compliance, loss avoidance or insurance to a broader consideration of all aspects of risk which affect a company's future performance." [12]

Lawrence believes that strong and effective risk management practices are now increasingly seen as a source of sustainable growth and competitive advantage. There is a need for organisations to be intelligent and conscientious about risk management, and to create enough time to enter into dialogue about the risks they are facing. It is also important not to get too preoccupied with compliance at the expense of thinking about broader issues. Ultimately risk management capabilities and processes must be shaped to fit each organisation's operations, people and performance.

By having a strong culture and awareness of risk, a powerful defence mechanism is created against that risk. The Institute of International Finance's Committee on Market Best Practices has carefully investigated problems experienced during the credit and liquidity crisis that has affected financial markets around the world, and found that the role of organisational culture was a primary driver for effective risk management. The committee's report recommended that organisations clearly state that senior management, and in particular the CEO, were responsible for risk management. In addition, boards should have an essential oversight role of risk management. A robust risk culture should be embedded in the way that organisations operate, and the accountability for risk management should become a priority for everyone – and not just delegated to risk specialists.

Figure 7, below, depicts the path towards integrated risk and value management in financial services organisations since the 1980s:

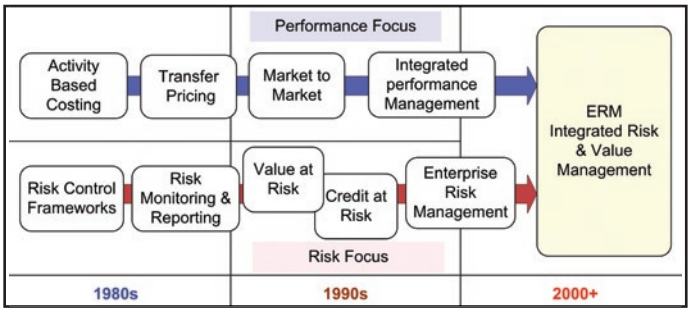


Figure 7: Trends of Performance and Risk Management [12]

Reputation Risk Management

A company's reputation is the way it is perceived by its stakeholders, which include customers, partners, employees, and regulators. According to Ansi Vallens, founder of the New York-based company Signals & Strategies, companies that enjoy a strong positive reputation also have:

- a higher market value
- receive preferential treatment when raising finance
- happier customers
- benefit from a more productive labour force, and
- attract the best talent. [13]

Importantly, when problems arise, organisations with strong reputations appear to get the benefit of the doubt. Standard & Poor's have recently announced that it will start considering ERM as part of the credit-rating process for non-financial companies such as manufacturers, distributors, and service companies. Vallens believes that as much as 75 per cent of a company's value is based on its reputation. A number of techniques may be used to assess and benchmark the reputation of an organisation, including strategic media analysis, surveys of stakeholders, focus groups, and public opinion polls.

Vallens suggests the following steps for reputation risk management:

1. Identify the organisation's key stakeholders, and the issues that are most important to them.
2. Investigate what these stakeholders think, by asking them directly or through focus groups, surveys, media audits, and Internet data mining.
3. Identify and prioritise risks using internal focus groups and role playing.
4. Decide the organisation's reputation risk tolerance, and then develop and implement a reputation risk management plan.
5. Establish an ongoing reputation risk evaluation programme.
6. Evaluate the reputation risk management programme as it relates to the organisation's greater ERM programme.

Implementing ERM in East Asia

Artie Ng, a senior lecturer at the Hong Kong Polytechnic University, believes the private sector is becoming increasingly aware of the need to implement ERM. The concept and application of ERM is still young in the United States; it is in its infancy in many other parts of the world. The increasing convergence of accounting standards needs to be complemented with improved internal controls to ensure that reported financial statements are reliable. This interest in strengthening risk management capacity presents certain challenges for organisations operating in the global marketplace. The traditions and culture of countries can influence attitudes towards risk management. Two of the main challenges to implementing ERM in East Asia lie in the following areas:

1. Experience of risk management. Given the short history of developing ERM, few professionals in East Asia have experience of dealing with its design and implementation. Organisations have begun to hire people in risk management positions and are beginning to develop their own risk registers, which will require clear accountability and continuous risk assessments.
2. Complementarity of corporate governance and culture. Larger East Asian companies are dominated by state-owned enterprises and family-owned conglomerates. These organisations operate from a centralised decision-making culture that manages risk using a top-down, diagnostic approach. They tend to deal with incidents internally, and provide ad hoc solutions instead of using structured methodologies. They may need to change their culture of risk management radically to develop an effective ERM system. [14]

Institutional investors may begin to place greater emphasis on a company's ERM capability when making investment decisions. Organisations that fail to adopt effective ERM would not only fail to comply with regulators' expectations, but come under increased scrutiny from credit rating agencies. The globalisation of processes should lead to increasing numbers of East Asian enterprises exhibiting risk management capabilities.

Survey and Research Data

Risk Management – Top Ten Strategic Risks

An Ernst & Young global survey on strategic business risks obtained the following top 10 strategic risks (preliminary results) from 70 international analysts representing some 20 disciplines, including law, finance, the sciences, business strategy, geopolitics, regulation, medicine, economics, and demographics:

- regulatory and compliance risks
- global financial shocks
- aging consumers and workforce
- emerging markets
- industry consolidation/transition
- energy shocks
- execution of strategic transactions
- cost inflation
- radical greening
- consumer demand shifts. [15]

ERM – Reputation Risk Ranked High in Importance

In 2005, an Economist Intelligence Unit survey of 269 senior risk executives in the United States ranked the relative significance of risks as follows:

- reputation risk (52%)
- regulatory risk (41%)
- human capital risk (41%)
- IT risk (35%)
- market risk (32%), and
- credit risk (29%).

Among those executives surveyed, 28 per cent reported suffering a major financial loss from a reputation event. Fifty-nine per cent of the senior risk executives listed competitive advantage as the principal factor leading to greater awareness and concern for reputation.

Responsibility for reputation risk was thought to reside with the:

- chief executive officer (CEO) (84%)
- board of directors (42%).

Responsibility for quantifying perceived reputation threats was believed to lie with the:

- chief risk officer (CRO) or risk manager (39%)
- CEO (23%)
- communications director (16%). [13]

ERM Adoption Percentages

In 2005, a Research Foundation study reported the following regarding ERM implementation by organisations in the United States. 361 respondents reported the following:

ERM Implementation Status	%
Organisation had not yet considered ERM	13.0
ERM adopted and infrastructure very mature	6.1
ERM adopted recently and infrastructure relatively mature	5.5
ERM recently adopted but infrastructure not yet mature	14.7
Organisation currently in the process of implementing ERM	21.9
Organisation considering ERM along with relevance for enterprise	31.8
Organisation had rejected the ERM concept	1.4
Other	5.0
Response not provided	0.6
Total	**100.0**

Among all the organisations surveyed, the following had primary responsibility for ERM-related activities:

- internal audit team (36%)
- a CRO who was not part of the audit function (27%)
- another executive or function (36%). [16]

ERM – Merger and Acquisition Risk Priorities

The following responses were obtained from a 2007 FTI Consulting survey on ERM within organisations in the United States:

- 45% of directors and 48% of general counsels spent more time on ERM in 2006 than in previous years. However, only 27% of directors and 25% of general counsels reported that they would like their boards to allow more time for ERM in 2007.
- 41% of board directors and 35% of general counsels reported that governance change was the area most requiring attention.
- Approximately one-third of each group said that understanding merger and acquisition risks should be their company's highest ERM priority. [17]

ERM – Implementation Challenges

A Towers Perrin's 2008 U.S. insurance industry ERM survey revealed that:

- Senior finance executives were more concerned about risk management practices (72%) than long-term debt financing (65%) and short-term financing (61%), relationships with their financial institutions (59%), pension plan asset allocation (40%) or their ability to secure equity financing (40%).
- 55 % believed that their organisations were likely to change risk management practices at board and/or employee levels.
- Insurers, in particular, find it challenging to fully implement essential risk and capital management processes that would enable them to realize the full potential of ERM (55% believed that substantial work was needed before they could use economic capital to guide risk-based decision making).
- Despite the acknowledged need for improvement, the survey found that ERM is influencing many important strategic decisions. Since a previous survey, carried out in 2006, respondents had made changes to their company's risk strategy or appetite (36%), asset strategies (35%), and product pricing (31%). [18]

ERM Improves Collaboration

In response to the question, "What value has your organisation's ERM programme created?", respondents to a 2006 KPMG LLP-sponsored survey of 481 global companies reported the following:

- improved risk awareness and collaboration (76%)
- improved regulatory compliance (53%)
- improved operations (50%)
- improved decision making (48%)
- reduced infrastructure, operation or resource costs (29%)
- improved earnings or shareholder value (24%)
- reduced earnings volatility due to hedging (21%)
- improved equity value or reduced debt costs (20%)
- no/little change (8%)
- other (4%). [19]

Example Cases

Valuable lessons can be learned from the following organisations:

Bristol-Myers Squibb, USA
ERM road map

As a result of case studies involving Bristol-Myers Squibb and four other organisations, a road map for the development and execution of ERM programmes was compiled as follows:

1.) Appreciation of the importance of ERM by board members.

2.) Assessment of the gaps and vulnerabilities in existing risk management solutions.

3.) Setting associated mission and programme objectives.

4.) Establishing an ERM infrastructure and the assignment of leadership.

5.) Compiling a risk inventory.

6.) Selecting assessment techniques and defining an acceptable risk appetite and tolerance levels.

7.) Determination of risk-response strategies.

8.) Development of effective internal communications and reporting protocols.

9.) Monitoring of the ERM implementation and its execution.

10.) Choosing compensation policies and performance metrics that promote and track the pursuit of a risk-adjusted corporate strategy.

11.) Integration of ERM with operational systems. [20]

Brisbane City Council, Australia
Internal auditing aligned with ERM

Brisbane City Council improved its internal auditing by integrating the audit department into its corporate risk management framework. This was achieved by directly linking annual audit plans with its divisional and branch risk registers. Numerical values were assigned in accordance with the perceived levels of risk and these were then further categorised and weighted in relation to (a) executive management interest, (b) audit department control perception, and (c) elapsed time between audits. The internal auditors were able to promote risk management throughout the council by aligning risk analysis with the organisation's ERM framework. This alignment challenged and enhanced risk rankings and treatments, improving the identification and evaluation of controls. Additionally, the tying of internal audit risk analysis to the council's risk frameworks clarified the ownership of risks, reduced the number of disputes at the conclusion of audits, and aligned audit reports more effectively with the organisation's objectives. [21]

Large U.S. Retail Corporation
Software proactively flags warnings

At a large retail corporation in the United States, an employee had been taking advantage of a lack of adequate controls associated with her division's budget and expense reviewing procedures. Over a period of two and a half years, she had defrauded the organisation of some US $275,000. With the establishment of internal audit procedures, unusual expense patterns and other discrepancies were picked up and further investigated. This then led to the employee being dismissed and legal action taken. Improvements made to the system included:

- travel and expense reporting became more detailed, and only original copies were accepted as supporting documents
- the use of corporate credit cards provided better delineation and management of expense claims
- audit software was used by the internal audit team and accounts payable to proactively flag warning signs of fraud. The travel and expenses team also developed auditing protocols to increase efficiency in auditing travel and expenses-related data. [22]

Federal Reserve Bank of Richmond, Virginia, USA
Successful ERM at a not-for-profit organisation

The bank successfully implemented a strategically oriented ERM system by focusing on risks that affected corporate goals and objectives. As opposed to a top-down approach, the organisation's ERM profile was built using input from the its functional business units and departments. The implementation is outlined as follows:

- Facilitation: a minimum of two risk analysts met with unit managers with one analyst guiding discussions and the other completing a data collection template.

- Assessment: meetings were held for orientation, setting objectives, and identifying events that might potentially affect a department's ability to complete its core duties.
- Data collection: inherent risk levels were identified along with trends and residual risk. The probability and impact of significant risks were calculated and mitigation strategies rated.
- Reporting: dashboards were used for reporting at both the departmental and corporate levels. [9]

The Nemours Foundation, USA

ERM leads to uniform informed consent

Nemours, a large US health system dedicated to the health of children, implemented an enterprise-wide, integrated risk management model. A key part of the implementation was the development of a uniform informed consent process that ensured families understood the risks and benefits of procedures, and importantly minimised potential liabilities. The existing informed consent procedures were highly variable and dependent on individual practitioner preferences. Some 35 per cent of medical malpractice actions were related to informed consent issues, which could potentially lead to awards of US $1 million or more. An interactive web-based informed consent solution was developed using the help of a third party. Web-based programmes, using animation and simple language, walked patients through upcoming procedures/chronic conditions, and enabled parents/guardians to view the presentations conveniently and at their own pace. Effective informed consent assured Nemours that families understood the risks, and that their expectations of outcomes were realistic. [23]

Sun Life Financial, Canada

ERM framework shaped business

Sun Life developed an ERM framework to provide a comprehensive and consistent view of organisational risk. The framework also included operational risks, e.g. legal, regulatory, and reputation risks. A board risk review committee that was separate from the audit committee met five times a year, and an executive risk committee met monthly. Sun's ERM framework comprised four layers:

- Layer 1 – minimised risks that could threaten the overall solvency/viability of the organisation.
- Layer 2 – managed the volatility inherent in the organisation.
- Layer 3 – shaped the business by deliberately taking risks in areas where the capacity to manage that risk existed, and where appropriate rewards were evident.
- Layer 4 – articulated Sun Life's risk appetite and risk management approach to its stakeholders, which included shareholders, regulators, and rating agencies. [24]

Measure and Evaluate

Measures used within ERM frameworks tend to vary according to the risks that an organisation faces. Appropriate measures should be developed for assessing major risks concerning, for example, reputation, governance, financial management, safety, changes in markets, and environmental issues.

James Kallman, a professor of risk management at Kaplan University in the United States, provides seven proven techniques for identifying risks. [25] As each measurement technique has its associated advantages and disadvantages, Kallman recommends that risk managers should use *all* of these techniques to ensure due diligence:

1. Statistical Analysis: when an adequate amount to relevant data is available, statistical analysis of outcomes is a powerful methodology for forecasting mean values and standard deviations. Actuaries use statistical models to analyse loss data, and managerial accountants use them to project future sales, costs and financial outcomes.
   - Advantages: the results are generally acceptable to decision makers. The data used comes from real operations and reflects past performance. Providing the measuring environment is stable, acceptable future projections can be made.
   - Disadvantages: analysts often do not have a data source that is large enough or data that is sufficiently reliable to create statistically valid inferences. In addition, dynamic business environments may render past data invalid for projecting future outcomes.
2. Contract Analysis: contracts are regularly signed in business, e.g. purchase/sales orders, employment agreements, mergers and acquisitions, and insurance contracts. These contracts should be carefully reviewed by a risk manager or general counsel to ensure that the organisation is not exposed to unacceptable contractual risks. Contractual risks include hold harmless agreements, exculpatory clauses or waivers, some of which could place the organisation in a vulnerable position.
   - Advantages: organisations are forced to carefully read all contracts.
   - Disadvantage: qualified and costly legal counsel may be required to give professional advice.
3. Surveys and Checklists: risk surveys and insurance checklists are commonly used tools. Checklists and surveys represent a good starting point for building an organisational risk register.
   - Advantages: the tools may be provided free of charge and completed by an insuring party.
   - Disadvantage: hazards identified may be limited to those most commonly insurable. Conversely, true risk management surveys tend to be more comprehensive and seek to identify unique risks. However, these cost more and require the investment of more time.
4. Chart Analysis: charts are an excellent visual guide to identifying risks. An organisational flow chart, for example, illustrates the flow of materials, resources and time through the organisation's processes.
   - Advantages: identifying bottlenecks and superfluous processes.
   - Disadvantages: flow charts may only reflect intended flows, with actual flows being modified in practice. For this reason, risk managers should verify charts with the people actually performing the work.
5. Expert interviews: experts may include bankers, accountants, lawyers, auditors, safety engineers, and consultants, or internal staff with specialised knowledge.
   - Advantages: brings a broad base of experience and knowledge to the risk manager. This diverse outlook may enable the risk manager to discover new or unimagined risks.
   - Disadvantages: external experts tend to charge for their services.
6. Financial Statement Analysis: various financial reports are prepared for different purposes, e.g. managerial reports and annual reports.
   - Advantage: these reports can contain critical information about cash flows and significant material disclosures that can be reviewed along with the chief financial officer.
7. Personal inspection: an effective risk identification technique is for risk managers to observe operational risks first hand in the workplace.

Self-Assessments

Self-assessments can be used to find out how effective organisations are at implementing various strategies, tools, and techniques. Figure 8, below, is a self-assessment tool for evaluating ERM frameworks to see where improvements might be made. The assessment could also be carried out by different departments to highlight variations in understanding or application.

Assessment Questions (Mark one box per question with an 'x')	Don't Know	Disagree, or No Plans	Planned	Partly In Place	Implemented Enterprise-wide
A – Internal Environment					
The organisation views risk management as a means of preserving and creating value.					
There is an overall risk management policy set out in a board-approved statement.					
The board considers risk management a regular part of its oversight agenda.					
Managers and personnel at all levels are involved in periodic review or planning exercises, which lead them to identify, source and quantify risks.					
B – Objective Setting					
The risk identification process is designed to make a clear link between the organisation's objectives and the associated risks.					
C – Event Identification					
Data on the business operating environment – political, economic, etc. – events is captured and regularly evaluated in terms of their potential impact upon the organisation's business objectives.					
D – Risk Assessment					
Prior to assessing risks, management examines the impact of potential future events relevant to its business (i.e. entity size, complexity of operation, degree of regulation, etc.)					
Appropriate methodologies are in place to allow the organisation to measure the impact of identified risks on objectives with some degree of accuracy.					
There is a periodic review process to ensure that the organisation's risk assessments remain current.					
E – Risk Response					
The full range of available risk management options – avoid, reduce, share, accept – is considered when formulating risk responses.					
F – Control Activities					
There is an appropriate balance of preventative and detective controls in place, with emphasis on preventative controls when appropriate.					
G – Information/Communication					
Appropriate information is identified and captured to identify, assess, and respond to risk and manage the business, obtained from appropriate internal and external sources, generated manually and electronically and is in appropriate formal and informal formats.					
H – Monitoring					
The required information is available to allow for proper monitoring of risk throughout the organisation.					

Figure 8: How Good is Your Organisation's ERM Framework?

Find out by completing the self-assessment (the full self-assessment can be found in the member's area of BPIR.com). *(Also have a look at our Business Continuity Self-Assessment, which also relates to risk management.)*

Scoring instructions: Take note of where the boxes have been crossed - particularly in the first two columns where no plans are evidenced or further information is required. Brainstorm what actions are required to improve performance.

Summary of Best Practices

The following is a summary of the best practices and/or insights contained within this Management Brief:

1. Strong and effective risk management practices are believed to be a source of sustainable growth and competitive advantage.
2. Corporate boards have an important oversight role of ERM frameworks and practices.
3. An organisation's culture affects how risk is viewed within the organisation, including its:
   - risk management philosophy
   - risk appetite
   - integrity, and
   - ethical values.

   (See also BPIR Management Brief: Vol. 5 Issue 3 – Corporate Culture.)
4. It is believed that as much as 75 per cent of a company's value is based on its reputation. Techniques used to assess and benchmark the reputation of organisations include:
   - strategic media analysis,
   - surveys of stakeholders,
   - focus groups, and
   - public opinion polls.
5. The management of high-impact, rare-event risks is a critical component of an effective ERM programme. Methods for identifying high-impact, rare events include:
   - employing third parties to think outside the box
   - risk mapping
   - root cause analysis, and
   - scenario analysis.

   (See also BPIR Management Brief: Vol. 3 Issue 6 – Business Continuity Planning.)

Conclusion

ERM forms part of the glue that holds corporate governance together. It also contributes to an organisation's long-term profitability and sustainable growth. Effective risk management initiatives need to be both proactive and embedded within the culture of an organisation.

ERM frameworks offer a structured approach to risk management, which enable organisations to:

- establish sound risk impact/probability assessment processes and develop solutions
- provide an enterprise-wide view of risk
- align available resources for managing risks, thus controlling costs and ensuring compliance
- take measured risks, manage them effectively, and create a competitive advantage
- strengthen corporate governance while increasing stakeholder and regulator confidence.

Risk maps and risk registers are excellent mechanisms for communicating organisational risks throughout an organisation.

Risk management capabilities and processes must be shaped to fit each organisation's operations, people, and performance. A strong culture and awareness of risk is a powerful defence mechanism against risk. An organisation's reputation relates to how it is perceived by its stakeholders, including its customers, partners, employees, and regulators, providing a powerful stimulus for establishing effective reputation risk evaluation programmes.

Note

The techniques and case studies mentioned or summarised in this article may be found in greater detail at *www.BPIR.com*, together with the full text of most of the articles and reports cited in the following reference list.

The BPIR Management Brief is a monthly publication delivered as one of the many membership benefits of the Business Performance Improvement Resource (BPIR). To enquire about upcoming Management Brief topics or BPIR membership, e-mail *membership@BPIR.com* or visit the homepage at *www.BPIR.com*.

References

The full text of these articles and reports can be found at www.BPIR.com.

[1] Teresko, J., (2007), **Risky Business Pays Off**, Industry Week, Vol. 256, Iss. 7, pp 44-47, Penton Media, Inc., Cleveland.

[2] Jablonowski, M., (2007), **The Real Value of ERM**, Risk Management, pp 16-20, Risk Management Society Publishing, Inc., New York.

[3] Kaliprasad, M., (2006), **Proactive Risk Management**, Cost Engineering, Vol. 48, Iss. 12, pp 26-36, American Association of Cost Engineers, Morgantown.

[4] Pritchard, C.L., (2001), **Risk Management: Concepts and Guidance**, p 9, ESI International, Virginia.

[5] Smith, PG., and G.M. Merritt, (2002), **Proactive Risk Management**: Controlling Uncertainty in Product Development, pp 30, Productivity Press.

[6] Anonymous, (2006), **Management Accounting – Risk and Control Strategy**, Financial Management, pp 42-43, Chartered Institute of Management Accountants, London.

[7] Anderson, S. W., Christ, M. H., Sedatole, K. L., (2006), **Risky Business**, The Internal Auditor, Vol. 63, Iss. 6, pp 47-53, Institute of Internal Auditors, Incorporated, Altamonte Springs.

[8] Barton, T. L., Shenkir, W. G., Walker, P. L., (2009), **Managing the Unthinkable Event**, Financial Executive, Vol. 24, Iss. 10, pp 24-27, Financial Executives International, Florham Park.

[9] Dorminey, J., Mohn, R., (2007), **A Model for Not-for-Profit Enterprise Risk Management: ERM at the Federal Reserve Bank of Richmond**, The Journal of Government Financial Management, Vol. 56, Iss. 1, pp 50-57, Association of Government Accountants, Alexandria.

[10] Adams, G. W., Campbell, M., (2007), **Where Are You On The Journey To ERM?**, Risk Management, pp 32-36, Risk Management Society Publishing, Inc., New York.

[11] Nadeau, Y., (2007), **A critical function**, CA Magazine, Vol. 140, Iss. 9, pp 60-62, Canadian Institute of Chartered Accountants, Toronto.

[12] Wilkinson, M., (2008), **Risk Revolution**, Charter, Vol. 79, Iss. 9, pp 38-41, Institute of Chartered Accountants in Australia, Sydney.

[13] Vallens, A., (2008), **The Importance Of Reputation**, Risk Management, Vol. 55, Iss. 4, pp 36-42, Risk and Insurance Management Society, Inc., New York.

[14] Ng, A., (2008), **Enterprise Risk Management**, Financial Management, Pp 44-45, Chartered Institute of Management Accountants, London.

[15] Pellet, J., (2007), **Top 10 Enterprise Risks**, Chief Executive, Iss. 229, pp 48-53, Chief Executive Magazine, Incorporated, New York.

[16] Gramling, A. A., Patricia, M. M., (2006), **Internal auditing's role in ERM**, The Internal Auditor, Vol. 63, Iss. 2, pp 52-58, Institute of Internal Auditors, Incorporated, Altamonte Springs.

[17] Marshall, J., Heffes, E. M., (2007), **ERM Seen Emerging As Key Board Issue**, Financial Executive, Vol. 23, Iss. 8, p 12, Financial Executives International, Florham Park.

[18] Brousseau, M., (2008), **Financial Losses Shine Spotlight on Risk Management**, Today, Vol. 31, Iss. 6, pp 31, Association for Work Process Improvement, Boston.

[19] Farrell, J., (2007), **New Use For an Accepted Process**, Financial Executive, Vol. 23, Iss. 4, pp 48-51, Financial Executives International, Florham Park.

[20] Tonello, M., (2007), **Risk Governance and Governance Risk,** Directorship, Vol. 33, Iss. 5, pp 64-66, NewsMarkets LLC, Boston.

[21] MacLeod, A., Overell, B., (2005), **A Change of Focus**, The Internal Auditor, Vol. 62, Iss. 4, pp 97-99, Institute of Internal Auditors, Incorporated, Altamonte Springs.

[22] Kessler, B., (2007), **Fashioning a Fraud**, Journal of Accountancy, Vol. 204, Iss. 4, pp 60-63, American Institute of Certified Public Accountants, New York.

[23] Pilla, L. A., (2008), **Visual Confirmation**, Health Management Technology, Sep. 2008. Vol. 29, Iss. 9, pp 34-36, Nelson Publishing, Nokomis.

[24] O'Rourke, M., (2007), **Scaling The Heights Of ERM**, Risk Management, pp 52-56, Risk and Insurance Management Society, Inc., New York.

[25] Kallman, J., (2007), **Identifying Risk**, Risk Management, Vol. 54, Iss. 9, pp 58-59, Risk Management Society Publishing, Inc., New York.

The Management Brief is published for members of the New Zealand Business Excellence Foundation (NZBEF).

To access the Business Performance Improvement Resource (BPIR) visit www.nzbef.bpir.com.

Issues of the BPIR Management Brief

- Action Planning
- Activity Based Management
- Benchmarking
- Business Continuity Planning
- Business Excellence
- Call Centre Representatives
- Change Management
- Compensation Schemes
- Corporate Culture
- Corporate Performance Management
- Customer Complaints Resolution
- Customer Knowledge Management
- Customer Loyalty
- Customer Market Segmentation
- Customer Order Management
- Customer Profitability Management
- Customer Satisfaction Surveys
- Customer Support and Service
- Diversity Planning
- Emotional Intelligence
- Employee Development
- Employee Motivation
- Employee Suggestion Schemes
- Ethical Business Practices
- Flexible Work Arrangements
- Knowledge Creation
- Leadership Development
- Lean Techniques
- Managing Innovation
- New Product Development - Innovation Strategy
- New Product Development Tools
- On the Job Training
- Performance Management
- Product Lifecycle Management
- Project Management
- Recruitment and Selection
- Relationship Management
- Six Sigma
- Strategic Deployment Metrics
- Strategic Planning
- Succession Planning
- Supply Chain Management
- Sustainable Development
- Total Quality Management
- Work and Life Balance
- Workplace Conflict

The NZ Business Excellence Foundation is proudly supported by our Patrons