Enterprise Risk Management & Governance
Vol. 7, No. 3

CUTTER CONSORTIUM

Achieving Business Benefits by Implementing Enterprise Risk Management

by Keith Sherringham and Bhuvan Unhelkar,
Senior Consultant, Cutter Consortium

The global financial crisis and the oil spill in the Gulf of Mexico highlight the significance of risk in business and the need to embed capacities and capabilities for the management, mitigation, and response to risk. From the ownership of risk by company directors through management of risk at the source in everyday business operations, this *Executive Report* brings practical experience to the implementation, management, and benefit realization of a risk-based approach to business (aka enterprise risk management).

Executive Report

Access to the Experts

Cutter Consortium is a truly unique IT advisory firm, comprising a group of more than 100 internationally recognized experts who have come together to offer content, consulting, and training to our clients. These experts are committed to delivering top-level, critical, and objective advice. They have done, and are doing, ground-breaking work in organizations worldwide, helping companies deal with issues in the core areas of software development and agile project management, enterprise architecture, business technology trends and strategies, innovation, enterprise risk management, metrics, and sourcing.

Cutter offers a different value proposition than other IT research firms: We give you *Access to the Experts*. You get practitioners' points of view, derived from hands-on experience with the same critical issues you are facing, not the perspective of a desk-bound analyst who can only make predictions and observations on what's happening in the marketplace. With Cutter Consortium, you get the best practices and lessons learned from the world's leading experts — experts who are implementing these techniques at companies like yours right now.

Cutter's clients are able to tap into its expertise in a variety of formats, including print and online advisory services and journals, mentoring, workshops, training, and consulting. And by customizing our information products, training, and consulting services, you get the solutions you need while staying within your budget.

Cutter Consortium's philosophy is that there is no single right solution for all enterprises, or all departments within one enterprise, or even all projects within a department. Cutter believes that the complexity of the business technology issues confronting corporations today demands multiple detailed perspectives from which a company can view its opportunities and risks in order to make the right strategic and tactical decisions. The simplistic pronouncements other analyst firms make do not take into account the unique situation of each organization. This is another reason to present the several sides to each issue: to enable clients to determine the course of action that best fits their unique situation.

Expert Consultants

Cutter Consortium products and services are provided by the top thinkers in IT today — a distinguished group of internationally recognized experts committed to providing top-level, critical, objective advice. They create all the written deliverables and perform all the consulting. That's why we say Cutter Consortium gives you *Access to the Experts*.

For more information, contact Cutter Consortium at +1 781 648 8700 or sales@cutter.com.

The Enterprise Risk Management & Governance Advisory Service Executive Report *is published by the Cutter Consortium, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA. Client Services: Tel: +1 781 641 9876; Fax: +1 781 648 8707; E-mail: service@cutter.com; Web site: www.cutter.com. Group Publisher: Chris Generali, E-mail: cgenerali@cutter.com. Managing Editor: Cindy Swain, E-mail: cswain@cutter.com. Print ISSN: 1554-7035 (*Executive Report, Executive Summary*, and* Executive Update*); online/electronic ISSN: 1554-7043.*

©2010 Cutter Consortium. All rights reserved. Unauthorized reproduction in any form, including photocopying, downloading electronic copies, posting on the Internet, image scanning, and faxing is against the law. Reprints make an excellent training tool. For more information about reprints and/or back issues of Cutter Consortium publications, call +1 781 648 8700 or e-mail service@cutter.com.

Rob Austin · Ron Blitstein · Christine Davis · Tom DeMarco · Lynne Ellyn · Tim Lister · Lou Mazzucchelli · Ken Orr · Robert Scott · Mark Seiden · Ed Yourdon

Cutter Business Technology Council

Achieving Business Benefits by Implementing Enterprise Risk Management

THIS MONTH'S AUTHORS

Keith Sherringham

Bhuvan Unhelkar
Senior Consultant, Cutter Consortium

IN THIS ISSUE

2 Risk Within Business

5 Risk Management Within Business

13 Developing Risk Management Capability

15 Risk and Business Benefit

18 Strategic Risks and Business Change

21 Conclusion

21 Acknowledgments

21 Endnotes

22 About the Authors

23 Appendix: Glossary

> Great love and great achievements involve great risk.
>
> — Dalai Lama, 2000

As reported in the *New York Times* on 6 May 2010: "within a few minutes, the United States stock market appeared to be collapsing. Some of the decline was real, but another part of it was simply trading gone awry ... and appeared to be the result of errors, not intentional sell orders."[1] Around the same time, Icelandic volcanic ash had aircrafts grounded with the airline industry reporting losses of US $200 million per day. This was on top of the global financial crisis and concerns of sovereign debt. As this *Executive Report* goes to press, BP is trying desperately to plug leaking oil in the Gulf of Mexico with expected costs in the billions of dollars, notwithstanding the loss of reputation, a falling share price, litigation, and any potentially hostile takeovers. These events reiterate what business leaders know: risk is an integral part of business and the presence or absence of effective risk management contributes significantly to business success.

Enterprise risk management (ERM) or a risk-based approach to business formalizes risk management across a business because of the important role risk plays in profit and cash-flow management.[2] The relative decline of Kodak due to weak management of the risks to its business from the advent of digital photography is a case in point. ERM includes the identification of risks and their sources, risk management frameworks, risk mitigation and impact minimization activities, effective governance, compliance with standards, and the necessary tools and technologies. Incorporating risk into routine operations, making risk management a norm rather than an exception, enables a business to manage its known risks and to respond effectively to unknown risks by embedding durability and resiliency within a business.[3]

Examples of a risk-based approach to business include:

- **Legal cases.** Standard legal practice is to assess the likely cost of a case and expected compensation payout to determine whether the case is worth fighting or whether settlement is appropriate.

©2010 Cutter Consortium

- **Product recalls.** This involves the ability of a business to successfully manage the recall of products for remediation in response to risks and issues occurring; for example, the recent vehicle recalls by Toyota.
- **Preventative maintenance regime.** The maintenance of road bridges to prolong the life of the asset and to reduce the risk of being sued by the general public for injury is an example of a risk-based approach and the use of effective governance. Conversely, a decision to save costs by reducing a preventative maintenance regime; for example, the Union Carbide chemical plant disaster at Bhopal, India, in 1984, or the BP oil refinery explosion at Texas City, Texas, in 2005, shows how risk affects a business through a lack of governance.
- **Transaction security.** This is a measure taken by banks to ensure integrity of financial transactions over the Internet to reduce risk of financial losses; for example, use of encryption or multiple sources of identity.

Risk is inherent to a business, and a risk-based approach entails the achievement of better outcomes through a formalization of what is often occurring by default for risk. Examples of inherent risk that benefit from formal risk management include:

- **Mergers and acquisitions.** The decision to grow a business through a merger or acquisition of another company is an example of where the risks associated with the acquisition versus the risks of not merging are assessed as part of an overall business decision.
- **Funding.** The loaning of funds to a business to support its growth is a risk-based approach. Security of some form is often provided to the bank to reduce the bank's risk profile, which is a view of the overall risk exposure (see the Appendix for a glossary of terms used in this report), against the lending of funds.
- **Emerging technology.** The advent of new technologies, such as the Web or cloud computing, can provide risks and challenges to the conversion, security, privacy, and volume of data within a business.
- **People.** Large-scale people movements, retraining, or retrenchments are fraught with sociocultural challenges and risks.
- **Insurance.** The business model of insurance is all about a risk-based approach to the number of claims that will need to be paid in a given period.[4]

As Cutter Fellow Robert Charette observed, managing risk is more than the reporting of bad news or the possible cost savings based on events that may not have occurred.[5] Indeed, a risk-based approach to business is a mainstream and comprehensive business solution for conducting business to realize better business outcomes. It is the formal business decision to accept a risk and to manage the consequences should a risk be realized or to invest in risk mitigation and/or impact minimization measures to achieve other business outcomes in the process of managing risk that underpins a risk-based approach to business.

Aimed at a wide business audience, this *Executive Report* brings practical experience to the implementation and management of a risk-based approach to realize a range of business benefits. The report begins by reviewing the occurrence of risk within the business and placing risk in the context of a risk-based approach to business to achieve outcomes. Building on the role of risk within business, the report then addresses the elements and supporting structures for the management of risk. The significance of effective governance in risk management (enterprise risk governance) is also noted. Following on from what is required to manage risk, the report details how to develop and implement the required risk management and risk-based approach. Some of the benefits from a risk-based approach are considered next, particularly the use of risk mitigation activities and measures for impact minimization to achieve other business benefits. The use of ERM as a tool for aiding cash-flow management, achieving cost savings, realizing market opportunities, and improving operational performance is also reviewed. Finally, some strategic changes expected to occur within the business environment that pose risks to a business, the likely business responses, and related benefits are noted.

RISK WITHIN BUSINESS

An appreciation of the role of risk within an organization starts with the four major business drivers — customers, market forces, costs, and regulation — that affect the occurrence of risk within a business, as shown in Figure 1.

Examples of risks within the business drivers include:

- **Customers.** Changes in customer activities affect a business; for example, the demand for cheap airline tickets by customers has seen the growth of low-cost airlines that pose a significant risk to the operations of the full-cost carriers.
- **Costs.** This refers to variations in costs (cost of goods and/or expenses) to a business. The risk of a key

Figure 1 — Illustration of the occurrence of risk within a business.

supplier going bankrupt and a shortage in product supply applies to many businesses. The impact a drought may have to increase food costs that have to be absorbed by a business to prevent a loss of customers to competitors is a risk to be managed by some businesses.

- **Regulation.** The risk of changes in regulation can significantly affect a business. For example, the risk of noncompliance with Sarbanes-Oxley (SOX) can be substantial. An additional example of regulatory risk is the changes to sovereign risk seen with the recent decision of the Australian government to place an unplanned "super tax" on the mining industry. The impacts of this decision to mining companies have included falling share prices, restrictions on access to capital, and deferral of planned investments.

- **Market forces.** Changes in markets bring risks to business; for example, long-term changes in consumer trends as a result of changes in information and communications technology (ICT) or volatility in foreign exchange rates impacting access to capital.

These four drivers influence the setting of objectives and outcomes of a business. For example, the objective of Oracle Corporation to "double profits year on year" in the mid-1990s led to increased risk taking within Oracle's sales operations, including the recording of sales that had yet to be approved by customers, which led to subsequent investigations by regulators.

Long-term trends in the business environment strategically influence the risks for a business (strategic risk). The looming risk to the aviation industry from an expected large-scale adoption of videoconferencing is but one example. The strategic decision of News Corporation to implement a "pay wall" around much of its online news content is part of the company's strategic response to the risks to its business from changes in technology. The decision of travel company Thomas Cook to derive revenue from the growth of the packaged holiday market is another example of risk affecting strategic decision making and of how such decisions change the risk profile of a business. For Thomas Cook to gain the advantage, alliances with airlines, hotels, and tour operators were formed. The risk of brand damage to Thomas Cook from alliance parties not meeting the required standards was weighed against the risk of loss of revenue and loss of market opportunity.

The strategic impacts of risk on businesses are seen in various ways, including:

- **Business insurance.** From professional indemnity to protection against floods and droughts, strategic risk affects the insurance premiums paid by a business; for example, the impact of climate change on increasing premiums.

- **Access to capital.** The strategic risk profile of a business affects its ability to access capital and the price paid; for example, availability of capital for energy

©2010 Cutter Consortium

companies to implement alternative energy sources as known oil reserves decline.

- **Business location.** If a decision is made to develop operations in a politically unstable area, the strategic risk profile for the business affects the profile of the business in other areas; for example, it increases the risk of physical attack on people or assets.

The main occurrence, management, and mitigation of risk within a business is within the daily management of the business functions shown within Figure 1 (from people to third parties listed at the bottom of the figure). Familiar risk examples include credit risk or occupational health and safety (OH&S) risks. Some of the more frequently occurring types of business risk are shown in Table 1.

People, process, information, communication, infrastructure, suppliers, and third parties are the main functional areas of a business. These functional areas are both the source of business risk and the source of risk mitigation. Examples of risk and mitigation in these areas are as follows:

- **People.** Risks relating to people within a business can include, for instance, the ability to access enough skilled tradespeople during a housing boom. It is the calibre and actions of people that mitigate the occurrence and impacts of risks.

- **Process.** These are risks related to current business processes and changes to business processes; for example, the implementation of a new billing system and the risks to cash flow and customer service. A successful revision of business processes should provide a better customer experience and reduce the risk for a loss of customers.

- **Information.** From privacy compliance to providing the right information for shipping of products, information (both electronic and paper records) risks occur across a business. Information risk happens for a range of reasons, including the duplication of information between systems and the effectiveness of backup and recovery procedures. Management of information risk requires a range of ICT solutions integrated with business processes to help standardize the role of knowledge workers.[6]

- **Communication.** Communication risk occurs in business because of the volume and complexity of communication between stakeholders across differing platforms. Risks occur in everything from the connectivity between systems to the misunderstanding of an e-mail sent from a PC leading to extensive instant messaging from mobile devices. Communication risk management includes the use of ICT with the appropriate policies and procedures as well as skilling in the interaction between people.

- **Infrastructure.** The risks here relate to the infrastructure that the business depends upon; for example, buildings or special plants and equipment of an oil refinery. The right infrastructure improves business operations and mitigates risks; for instance, the lowering of the cost of goods because wastage is minimized.

Table 1 — Frequently Occurring Types of Business Risk

Business Risk	Risk Details
Operational risk	Risks in many areas of business operations; for example, safety risk or the plant management operations risk. Operational risk also has a specific meaning within financial services; for example, Basel II or the AS/NZS ISO 31000-2009 Risk Management Standard.
Financial risk	Used to define the financial impacts of risk and the specific financial risks that affect the business; for example, credit risk or securing a loan with assets and impacts to cash flow.
Market risk	Addresses the risks related to the more operational aspects of trends in the market, either financial or the market in which the business operates; for example, changes in exchange rates and the hedging of funds or fuel.
Regulatory risk	The risks related to regulatory and compliance that have an impact on the business; for example, changes to food-handling regulations and the ability of a business to comply.
Program risk	The overall risk of programs and projects to a business; for example, likelihood and impacts of cost overruns.

- **Suppliers.** The risks around the services received from suppliers includes the logistics chain as well as utilities, cost of goods, and expense purchases. Adoption of multisourcing mitigates single supplier risk.
- **Third parties.** A major source of risk to business operations is a dependency upon third parties. The actions of regulatory bodies, for example, health and hygiene inspectors, can see a business shutdown. A dependency upon outsourcing vendor(s) for critical business functions; for instance, payroll processing, has risks for a business.

Risks with potential catastrophic impacts on the business exist within all of the main functional areas; for example, a major loss of people through a strike. These risks having high-impact but low likelihood of occurrence are termed resilience risks (see sidebar "Resilience Risks"), and management of these risks is part of an overall risk-based approach to business.

Therefore, a risk-based approach includes both an understanding of risks within a business and the existence of the capacity and capability for the management of risk across a business.

RISK MANAGEMENT WITHIN BUSINESS

From an appreciation of the role of risk within business comes the ability to manage risk. Some of the common elements of risk management are shown in Figure 2, together with the supporting role of governance, reporting, audit, strategy, and planning. These common elements of risk management are discussed further within this section using the example of a risk posed by the lack of skilled staff as well as other familiar business examples.

Risk Identification

Risk identification is about recognizing risks, likely impacts, and causes of risks as part of business as usual. Identifying the risk to a business related to a lack of skilled staff allows a business to take measures to adjust its operations (e.g., implementation of an apprenticeship scheme).

The identification of risk needs to separate risks from issues and distinguish between risks that need to be readily managed at the source (e.g., putting up a sign to manage risk of slippage on a wet floor) and those that need to be escalated through the management chain (e.g., risks associated with a new product release). Risk identification may include some element of risk classification as a means to an end only. The ability to identify and manage risk at a consistent standard level requires skilling and training (e.g., part of OH&S training on induction and part of annual performance review).

Risk Owner

A risk needs an owner who is accountable for and responsible for managing all aspects of a given risk within the designated business area. The practical management of a risk may be allocated to various parties, but it is the responsibility of the risk owner to fulfill his or her obligations. A process for the management of risk

Figure 2 — Common elements for risk management.

RESILIENCE RISKS

Resilience risk is a term used for those risks that have a low likelihood of occurrence but are of high or catastrophic impact to the business; for example, risk of loss of a building. The management of resilience risks has both an immediate impact on the business as well as a strategic impact. Consequently, resilience risks are often aligned to strategic issues and strategic business decisions.

By their nature, similar resilience risks can occur in any area of the business, though some industry-specific risks exist. Types of resilience risks and examples in three categories are listed below:

1. Industry risks refer to industry-specific risks, such as loss of fleet for the aviation industry or loss of mineral rights due to land-ownership claims for the mining industry.
2. Business risks include:
   - Loss of people, such as a strike action
   - Loss/denial of building, such as the loss of an operations center
   - Loss/denial of information, such as the loss of a billing system
   - Loss/denial of communication, such as the loss of PABX or widespread printing failure
   - Loss of plant and equipment, such as the loss of a satellite dish or loss of a distillation plant
   - Loss of suppliers and/or third parties, such as regulators or outsourcing vendors
   - Loss of infrastructure, such as a railhead
   - Process change, such as a change in outsourcing vendor
3. Event risks include:
   - Global/regional wars
   - Health emergencies, such as the flu, pandemics (e.g., SARS)
   - Physical attack on people or assets, such as riots and civil unrest (e.g., G9 summit or attacks on banks in Greece)
   - Natural disaster, such as a flood or earthquake (e.g., Haiti)

Unique aspects of resilience risks include:

- **Cross-business impacts.** By their nature, resilience risks cut across all areas of the business; for example, loss of a building.
- **Significant impact.** This refers to the significance of their impact on the business; that is, potential catastrophic losses to the business.
- **Mitigation and response.** This is the amount of effort required to mitigate the risks and to respond to the risks.
- **Classification.** Resilience risks cut across other categories of risk. A loss of a building can be seen as a strategic risk or a market risk. Irrespective of in which category a resilience risk resides, it is the management of the cross-business impacts of resilience risks that is significant.
- **Rating.** Unlike other forms of risk that are often highly dynamic, resilience risks seldom change in nature and rating. Resilience risks tend to move quickly from a risk to an issue, often with little notice; for example, a chemical spill causing a building evacuation.

Resilience risks need to be viewed in context, including:

- **Risk details.** This refers to any details around the risk including the factors that are currently serving to increase the risk; for example, renegotiation of employment contracts leading to increased risk of strike action.
- **Critical functions.** Detail any critical business functions that would be impacted. The interest is in the critical functions necessary for a business to keep operating.
- **Critical dependencies.** Related to the risk identified, detail any critical dependencies (system, process, function, or entity) that the critical areas of business depend on.

Like any other form of risk, the consequences of resilience risks becoming an issue can be mitigated. Consider the example of a house burning down. By trimming the branches of the trees around the house and by regularly burning off any excess leaf debris in the area in the winter months, the likelihood of a fire occurring is mitigated. Similarly, actions can be taken to mitigate the occurrence of resilience risks, but at some point further investment of effort and resources is not justified and the risk is accepted.

The impacts of resilience risks can also be minimized. Again, consider the example of the house burning down. The previously described regime acts to mitigate the occurrence of fire and to reduce the consequences should fire occur. Having an insurance policy is an example of an action to minimize the consequences but not to mitigate the risk of fire. Similarly, actions can be taken to minimize the consequences of resilience risks, but at some point, further investment of effort and resources is not justified and the risk is accepted.

owners needs to exist. Risk owners need to be familiar with the respective problem domain and have sufficient strength to call upon the resources available to handle the risk. The demise of Enron illustrates the importance of ethics in ownership of risk.

Risk Rating

This is an assessment of the severity of a risk in terms of likely impacts and likelihood of occurrence; for example, a lack of skilled staff is critical because a loss of key sales staff members will see customers go with them causing a loss of revenue within three months. The risk rating is used to help determine business priorities; for example, an agreement to offer better conditions to retain existing staff is a priority for key business areas.[7]

Standard risk management practice is to rate (classify and categorize) risk for reporting, management, and analysis purposes. The significance of a rating risk lies in the actions taken to mitigate risk and minimize impacts.

Risk classification, as outlined below, is about likelihood of occurrence and likely impact:

- **Occurrence.** A rating of the likelihood that a risk will occur. The occurrence rating could be classified as "rare, unlikely, likely, very likely, expected" or similarly on a quantified scale. Value ranges can be assigned and best judgments made accordingly. Assessment can be based on likely occurrence to a business area or in relation to the overall business significance. Either way, consistency of application and of assessment is required.
- **Impact.** This is an effort to rate the likely impacts should a risk occur; for example, financial or loss of life. Impacts could be rated as "insignificant, minimal, minor, significant, severe" or similarly on a quantified scale. Value ranges can be assigned and best judgments made accordingly. Assessment can be based on likely occurrence to a business area or in relation to the overall business significance. Either way, consistency of application and of assessment is required.
- **Trend.** A final element is the trend or the outlook of a risk in a given period; that is, the risk rating is increasing, decreasing, or steady.

Assessment of risk impacts can be based against the following:

- **Brand.** Risk rated by impact upon brand, either qualitative or quantitative.
- **Safety.** Risk rated by injury or possibly death to employees, customers, and/or stakeholders.
- **Security.** Risk rated by security threat based on its nature and likely impacts.
- **Compliance.** Risk rated by business impact if business is noncomplying.
- **Cost.** Risk rated by likely cost to a business to address impacts resulting from the risk if realized.
- **Loss of plant and equipment.** Risk rated by impact upon loss or damage of plant and equipment. Either cost of replacement if risk realized and/or cost of the disruption to business functions based on business criticality of the impacted function(s).
- **Operational disruption.** Risk rated by impact upon disruption period to business functions and the business criticality of that function(s).
- **Loss of facilities.** Risk rated by impact upon facilities; for example, outage period and loss of production resulting.
- **Loss of revenue.** Risk rated based on estimated loss of revenue. The varying amounts of revenue generated by different business areas can impact a risk rating; that is, smaller revenue generating areas may be rated lower in an overall rating but the risk may be of greater significance to a business. For internal services, the profit center structures and internal cost recovery revenues can be used.

Although a qualitative impact assessment may suffice in some instances, a quantitative approach is preferred.[8] A business may rate risks based on significance to a given business function (ensure management within that business area) and from the impact upon the overall business; that is, accommodate business criticality within the risk rating. Independent peer review of all estimates, especially qualitative estimates, is recommended.

Based on the likelihood of occurrence and the likely impact, an overall risk rating can be determined as part of an overall risk assessment guide (see Figure 3).

An overall risk profile for projects and programs and the impact of delivery on a business would be included within an overall risk assessment guide. The significance of risks with a low rating that may not change frequently is also required in any overall risk assessment. Strategic and resilience risks are obvious examples, but, as the recent oil spill in the Gulf of Mexico shows, a risk with a low rating is still a business priority. Active mitigation to keep the risk of a well blowout low would include a preventative maintenance regime and upgrades of well head technology. Active impact minimization would include

©2010 Cutter Consortium

Impact	Occurrence				
	Rare	*Unlikely*	*Likely*	*Very Likely*	*Expected*
Severe	Moderate	High	High	Extreme	Extreme
Significant	Moderate	Moderate	High	High	High
Minor	Medium	Medium	Moderate	Moderate	Moderate
Minimal	Low	Low	Medium	Medium	Medium
Insignificant	Minor	Minor	Low	Low	Low

Figure 3 — Illustrative risk rating matrix for business risks excluding program management.

desktop exercises and contingency testing (see sidebar "Business Planning with a Risk-Based Approach").

Risk Acceptance, Mitigation, and Impact Minimization

The decision to accept a risk or to take actions to mitigate is the essence of a risk-based approach. A business can decide to:

- **Accept a risk.** This decision is based on business experience, an ROI for mitigation, and the risk rating. Any decision is a combination of these factors together with the amount of risk (risk appetite) that a business is prepared to accept. An acceptance of risk is a decision to undertake no further mitigation or impact minimization activities at a given time. Ongoing monitoring and review is still required. The decision to accept a risk can be made before any mitigation is implemented or after a level of mitigation has been implemented and there has been an acceptance of residual risk.
- **Mitigate a risk.** This is the decision to invest in measures to mitigate the likelihood of the occurrence of a risk, commensurate with risk and business need. Mitigation for the risk of a lack of skilled staff may see a business accept lower recruitment standards and then skill inhouse. A decision to mitigate a risk provides an opportunity to realize other business benefits. Consider the automation of a business process. Reducing the risk to a business process through automation can also achieve cost savings and improved customer service.
- **Minimize impacts.** This is the decision to invest in measures to minimize the consequences should a risk be realized. For a lack of skilled staff risk, a business may develop a plan to headhunt staff from rival businesses and then invoke the plan as required. Including redundancy into an ICT system both mitigates risk and minimizes impacts. Redundant and imaged hard disks aid a rapid systems recovery and minimize any business outage. Similar to risk mitigation, impact minimization measures are an extension of best practice and can be used to realize business benefits; for example, cross training of staff to fill multiple roles.

Measures to mitigate risks need not be expensive or complicated; common effective measures may include:

- **Education and training.** Prevention is better than cure. Implemented as part of other routine activities (e.g., OH&S training) to realize the benefits of a better educated and more productive workforce as well as reduced risk.
- **Process revision.** Revising processes to better service customers can reduce risks by eliminating points of failure and improve customer service.
- **Performance management.** This refers to the inclusion of risk management outcomes within performance metrics.
- **Preventative maintenance.** A regime of preventative maintenance reduces the risk of equipment failure, reducing production outages, and provides a safer working environment (fewer accidents due to equipment failure).
- **Insurance.** Reduce the risk of loss through appropriate insurance policies. An effective risk mitigation regime may reduce insurance policy premiums.
- **Culture.** Develop a culture that values risk mitigation and risk management because "it is the right thing to do." The culture then becomes a self-sustaining feedback cycle that delivers business benefits. Use of people of influence and peer pressure to provide the positive culture is required.
- **Compliance.** Use the need for compliance as a tool for reducing risk and use risk management to aid compliance.

Risk mitigation involves the following activities:

- **Reasoning.** There is a need to reason through the problem before solution and implementation. Where the complexities and interdependencies of risks have

BUSINESS PLANNING WITH A RISK-BASED APPROACH

The recent events of the Icelandic volcanic ash and the global financial crisis have highlighted that crises are part of the business environment.[1] Having a durable and resilient business that accommodates risk requires strategy, preparation, and planning. The significance of strategy and planning are reflected in having guidance and a framework within which people can work flexibly, having infrastructure and capabilities that can be adapted to meet dynamic needs, identifying issues for resolution, understanding the value of thinking something through to the point that others know what they need to do and can develop that further, and gaining advantages by not having to continuously rework an activity.

As seen in Figure A, the strategy and planning considerations within a risk-based approach include:

- **Objectives.** Define what is to be achieved. Objectives need to be clearly defined, be quantifiable, be realistic, and have a time frame attached to them. Multiple objectives often lead to a dilution of effort, increased risk, and uncertainty of priorities. In tough times, objectives may change to focus on cash-flow preservation.

- **Strategy.** Defines how an objective is to be achieved. Strategy sets focus and direction and eliminates options. Only one or two key strategies are necessary for achieving an objective. Strategies need to be clearly defined, quantifiable, and readily articulated by managers (at all levels). While strategies need to be reviewed and adjusted according to changes in circumstances, effective strategies seldom change. Sacrificing peripheral business activities to protect core business is often part of a strategy for surviving tough times.

- **Planning.** Refers to the activities needed to realize strategy, which include:
  - *Business planning.* The familiar business planning but also planning for how an organization survives a major loss of revenue; that is, how to manage a business through tough times.
  - *Business continuity planning.* Addresses what the business is going to do should it experience a major incident.
  - *Contingency planning.* Developing contingencies in the event a risk becomes an incident; for example, how a potential loss of staff from a strike would be managed.
  - *Crisis planning.* Planning for how to manage a given crisis; for instance, a rail accident.
  - *Disaster recovery planning.* Planning for recovery from a disaster and/or for preventing a disaster; for example, the familiar disaster recovery of ICT.
  - *Operational procedures.* Describe how operations are to be conducted. Many crisis procedures are actually operational procedures and should be treated accordingly.

(Sidebar continues on next page.)

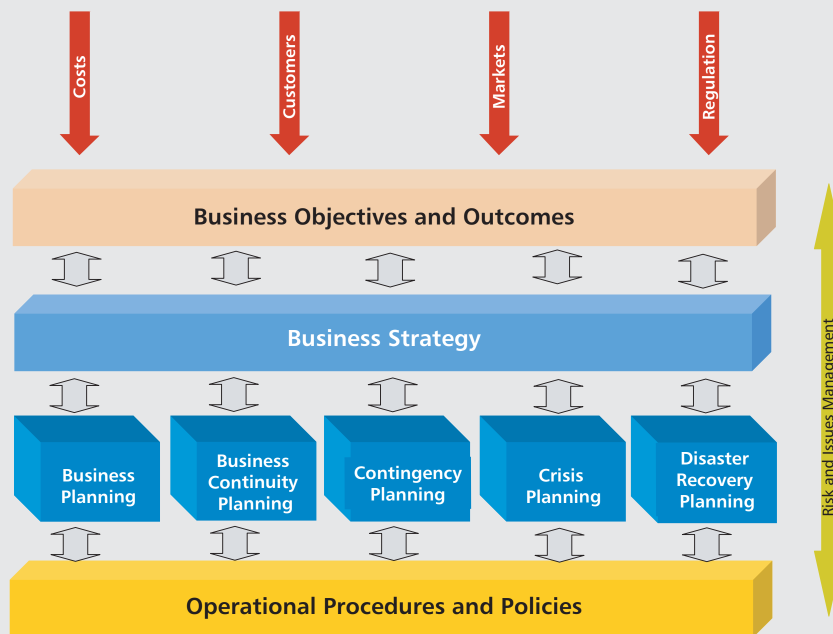


Figure A — Planning with a risk-based approach.

BUSINESS PLANNING WITH A RISK-BASED APPROACH (CONT'D)

With planning, the following are of consideration:

- **Planning process.** The significance of a plan lies in the planning process rather than the plan itself. The planning process is about:
  - *Intent.* Defining what needs to occur.
  - *Issue recognition.* Identifying the issues and how they are to be addressed.
  - *Building infrastructure.* Allows the capabilities and infrastructure developed to be used as required to meet needs in a changing environment.
  - *People aligned.* Involves effective communication between all parties so they know what they need to do.
- **Implementation.** This is the plan covering what to do when an event occurs; for example, what actually needs to occur when staff relocates to another building.
- **Preparation.** This is the plan for all the preparation that is required so the implementation will actually work; for example, preparing a building so that it can be used if staff needs to be relocated.

Plans are most effective when they are regularly: reviewed to ensure they are current such as for annual review and postincident reviews; updated at times of review to reflect the changing business environment; and exercised, or tested, so that the plan remains relevant, is valued, and ensures staff knows what to do in the event of an emergency.

A regime that includes the following elements develops the robustness, durability, and resilience of a business:

- Risk management
- Regular building evacuation procedure testing
- Clear crisis management structures and exercising of these capabilities
- Desktop exercises (facilitated hypotheticals using risk-based priorities) conducted regularly to build expertise and capabilities
- Testing of the crisis management callout structures
- Regular review and testing of plans and policies and procedures
- Practical recovery exercises; for example, loss of key systems with an invocation of manual contingencies
- Postevent reviews and revisions
- Regular reporting of outcomes to executive

[1]Sherringham, Keith. "Business in Tough Times: Seven Fundamentals." Alinement Network, 5 April 2010 (www.alinement.net/component/content/article/8-styles/40-seven-fundamentals-for-tough-times).

a significant impact on a business, taking some time to reason through the problem is often more cost effective than moving rapidly to solution mode (where major expenditure may occur). Consider changes in technology driving consumer trends to use e-books while printing and distribution costs are increasing. In such a case, the best response for shareholders may entail a publishing house selling off parts of its operation while adjusting the core of the business to publishing on new technologies.

- **Opt out of that function.** No longer having an involvement in that area of business or business function can be used to reduce risks; for example, James Hardie Industries and its asbestos liabilities led to relocation in the Netherlands and a liquidation of business areas with a high risk of asbestos claims.
- **Watching brief.** Sometimes a decision to do nothing and just accept a risk for a period, with a watching brief, is appropriate because business circumstances change to reveal other opportunities.
- **Risk sharing.** This involves the recognition of who else has this risk and the possibility of sharing the solution; for example, freight companies share the same terminal to manage risk of increasing capital costs.

Mitigation of resilience and/or strategic risks is often more complex, requiring a significant business commitment over an extended period. An alignment of risk mitigation to the business planning and budgeting process is also required. A culture of active risk management and taking measures to mitigate risks can be used to drive out operational gains, but like many preemptive measures, the cost of being preemptive with risk can be seen and is therefore prone to cost cutting. The cost of tardiness around risk management is often significantly higher, but unfortunately, the cost of tardiness is seen only after the fact when funds must be allocated.

Risk Reporting and Review

An ongoing review of risks should guide business decisions. Risk management requires quality risk reporting. It is the setting of risk information in context for decision

making that provides value beyond the standard reporting of different types of rated risk on a quarterly report. Since most businesses go through a careful planning process to set budget and objectives and then link performance, the reporting of risks against performance metrics provides context, illustrates impacts, and clarifies priorities. Context is also provided by reporting the following:

- **Risk trend.** This is the outlook for the risk: increasing, decreasing, or steady. An increasing risk should be accompanied by proposed measures for risk mitigation or minimizing impact.
- **Risk details.** Specific details of the risk; for example, loss of skilled staff risk, the increasing of salaries by rivals means some five key managers in the operations area are at risk of leaving.
- **Recommended actions.** These are recommendations about any actions for risk mitigation and/or minimizing impact required; for instance, for a loss of skilled staff risk.
- **Issues.** Details on risks that have been realized as issues and what has been done to manage them are also significant. Issues that have reverted back to a risk should also be detailed.
- **Exceptions.** Focus information for decision making and implementation by reporting exceptions; for instance, the problem areas and progress made to resolution.
- **Risk profile.** A view of the overall risks for a business (the risk profile) allows managers to know where priorities are; for example, actions required around an ICT system to address business integration.
- **Program risk.** The risk profile approach should also apply to a program of work and its business impact; for example, the loss of revenue from delays in the development of a new product offering. The impact of the program on the various affected business areas and the business itself is part of the respective risk profile reported.

Risk reporting is more than the production of routine reports from ICT solutions. Effective risk reporting requires people with business expertise to make pragmatic decisions and value add to the reports. Best practice keeps reports current and makes use of reporting as an ongoing monitoring tool.

Issues Management

This is the management of realized risks to minimize business impacts. Though part of a risk-based approach is the ability to manage issues, effective risk management should drive out problems for resolution before risks escalate into issues. Issues management includes preparations and contingencies for minimizing impact as well as the capacity and capability to effectively and efficiently resolve issues. It is the active, effective, and efficient management of issues that is pivotal to overall business performance.

Managing Strategic Risk

The management of strategic risk provides its own unique challenges and opportunities to a business. Ambiguity within business objectives and strategy (again, see sidebar "Business Planning with a Risk-Based Approach") leads to uncertainty in the management of strategic risks. Strategic risks may have an impact over an extended period and have a high degree of interdependencies between other risks. Major changes within a business are often required to meet strategic risks. Consider two examples: changes to regulations in a tax regime and market changes due to trends in ICT.

With regard to a regulation tax change, a government usually consults with impacted parties when it is planning regulation changes and the business finds out that options are being considered. A planned change in regulation is a risk because of any impact it may have upon the strategic direction of a business. Measures a business may take to influence the government not to regulate or to regulate in a different way are part of risk mitigation. Impact minimization may include measures to change the business in advance of the regulation; for example, a proposed broad-based consumption tax used by the government would see a business move to an accounting package that already supports differential sales tax rate functionality. When a government regulates, the risk has now become an issue and is affecting the business. The response of the organization to this issue may have been planned or plans may need to be developed (contingency planning; see sidebar "Business Planning with a Risk-Based Approach").

Regarding market changes due to ICT, the consumer adoption of ICT is having many impacts on business and markets. Consider the case of Bankers Trust and the introduction of ATMs. Rather than invest significant amounts in ICT to try and catch up with competitors, Bankers Trust made a decision to sell off its retail banking operations. As well as returning shareholder value through the sale, Bankers Trust significantly reduced the strategic risk profile of the company and saved expenditure.

©2010 Cutter Consortium

Other Features of Risk Management

Management of risk includes everything from the company directors having accountability and ownership for the overall risk profile of a business through to risk being managed at the source as part of everyday activities across a business. Using the risk posed by a lack of skilled staff, some other features around risk management include:

- **Issue management.** When a risk such as lack of skilled staff is affecting a business, it is no longer a risk (e.g., a strike). It is an issue to be managed accordingly. Issue management may create other risks and issues to be managed.
- **Risks and issues exist together.** Across the business, the risk of a lack of skilled staff may be a risk in one or more areas and to the business overall, but once the risk is affecting business operations, it is an issue for that respective area of the business. How risks and issues manifest in risk reporting across the business will depend upon the reporting, governance, and management regime adopted by a business.
- **Issue to risk to issue.** The realization of a lack of skilled staff risk as an issue does not mean that the risk has changed and/or disappeared. Once the immediate issue(s) around lack of skilled staff has been addressed, the issue may go back to being a risk. Similarly, the risk can be converted to an issue and back again.
- **Risk likelihood.** Although the risk of a lack of skilled staff may have become an issue, this may not change the likelihood of this risk occurring again.
- **Slow burn.** A cut in government funding for traineeships eventually leading to a lack of skilled staff for a business is an example of slow burn risk. There is a high likelihood of this risk becoming an issue, but the impacts are not immediate. The business has time to respond in a variety of ways. Slow burn risks are usually related to strategic and resilience risks.

Enterprise Risk Governance

Whether operated centrally in a command-and-control model or implemented along distributed lines with empowered accountability, governance is required within business to ensure accountability. Therefore, governance in the form of enterprise risk governance[9] is an important tool in a risk-based approach to business.

The purpose of governance is to ensure accountability and ownership; that is, effective governance determines the regime and culture. Governance should ensure that the "spirit of the intention" becomes part of business as usual — business areas do it for their own benefit. Aspects of effective governance to consider include:

- **Process alignment.** Governance should align with existing processes and serve as a tool to improve processes.
- **Standard regime.** A common governance regime that is flexible to meet specific business needs is required across a business; for example, use of ITIL or COBIT to assist in SOX compliance.
- **Management of behavior for outcomes.** A governance regime is about instilling the right behaviors to realize or exceed required outcomes.
- **Ownership.** Governance should include clear ownership of risk and accountability for risk. The empowerment of the respective owners is required, aligning with other authorization limits, accountabilities, and performance management.
- **Audit capability.** This refers to the audit of risk management capacities, capabilities, and outcomes as part of a routine internal/external audit.
- **Multilayer approach.** Management of risk through a multilayered approach of risk controls at each level of implementation. Consider a software development project where risk management controls would be applied using standard methodologies or frameworks as shown in Table 2.

Audit in Risk Management

An effective audit function forms part of any successful risk governance. Audit capability would include the auditing of:

- **Risk profile.** Assessment of the risk profile of business areas and programs, together with an overall risk profile for the business.
- **Mitigation.** Assessment of risk mitigation achieved.
- **Standards.** Use of and alignment to relevant standards.
- **Compliance.** Ensuring the relevant compliance of risk management.
- **Reporting.** Assessment of the completeness of risk reporting and its effectiveness.
- **Effectiveness.** The effectiveness of the risk regime determined by agreed-upon metrics.
- **Programs.** Independent audit of programs and their risks, especially the business impacts around the program.

DEVELOPING RISK MANAGEMENT CAPABILITY

While the detailed implementation of risk management capacity and capability may vary according to business type, size, or location, much commonality exists across a business.[10] The requirements for the development of a risk management capacity and capability within a business are shown in Figure 4. The four business drivers are affecting the need and strategy for achieving risk management. The risks and the ability to sustain business also influence the strategy and decision to support any implementation.

Implementing a risk-based approach includes:

- **Executive strategy and support.** There needs to be an overall champion within the executive leadership team who has the drive, vision, and the necessary strategy for implementation. Board and executive

Table 2 — Methodologies and Frameworks for Risk Mitigation in Software Development Projects

Activity	Risk Mitigation
Gathering of business requirements	Adoption of UML and use cases
Definition of processes	Processes measured against Six Sigma
Coding of software	Use of standard ISO/IEC 9003: 2004 for QA
Testing	Standardized testing procedures benchmarked on ISO/IEC 29119
Alignment to enterprise architecture	Assuring architectural integrity through Zachman Framework
Project management	Programs and projects managed to a common methodology PMBOK or Prince 2
Management of the application and services provided	Service definition and management through ITIL

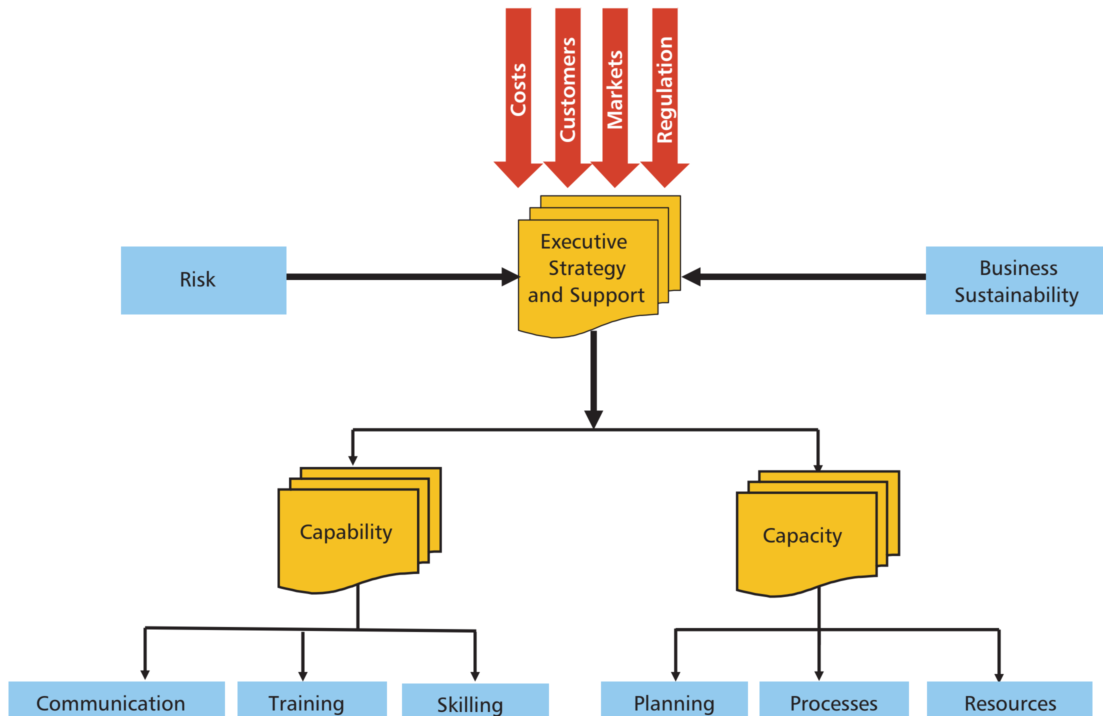


Figure 4 — Developing capacity and capability for risk management in an organization.

support is a necessary component for successful implementation because of the leadership it provides and the influence it has upon busy people to prioritize a risk-based approach to business.

- **Risk.** This means the risk around implementation: what happens if the implementation is unsuccessful and what are the recovery points? The risk of not having a risk-based approach to business is also part of the implementation risk.
- **Business sustainability.** This refers to the ability of the business to sustain operations while the changes are implemented into the business. A risk-based approach is implemented progressively, in a manageable way, to achieve business outcomes.
- **Planning.** This addresses the detailed planning for the risk management regime (e.g., classification, reporting, and governance) and its implementation.
- **Processes.** This refers to the definition of the processes required for risk management and the process for their implementation. Include alignment of risk management into business processes.
- **Resources.** This involves resolution of the availability of resources to implement the program of work required, including budget. The ability of key staff to spend time away from other business-as-usual activities is critical.
- **Communication.** This involves the required communication activities to affected stakeholders to ensure implementation. Communication should include how a risk-based approach will be used in their business operations for their benefit.
- **Training.** This refers to the training required; for example, training on risk identification and reporting as well as roles and responsibilities.
- **Skilling.** This involves the reskilling of people required to adopt the change and the use of risk in business. This includes ethics and the willingness to actively manage risk.

Implementation of risk management is a change management program in its own right,[11] implemented according to standard program management practices. A business can manage only a certain amount of change at a given time, and trying to implement too much change too fast significantly increases the risk for implementation and of benefit realization. The maturity of risk management is an ongoing business activity, but distinct programs for development of the capability are often required. Cultural change achieved through a risk-based approach is one of the main benefits to be realized.

A risk management regime requires:

- **Board ownership.** Risk needs to be owned by the board. The board uses risk to manage and drive a business. The board is responsible and accountable for risk within a business.
- **Executive for risk.** A member of the executive leadership needs to be responsible for risk (chief risk office).
- **Governance body.** This is a risk governance and management board or committee that is charged by the company board with overseeing a risk-based approach to business. This entity includes the executive responsible for risk, together with other executives and board members, and is accountable to the company's board.
- **Reporting.** A regime for the effective reporting of risk, for action, and for decision making is needed. The reporting starts in the lines of business and cascades up, reporting by exceptions, to the board.
- **Risk facility.** This refers to tools for the management of risk, including guidelines, standards, processes, polices, procedures, governance, and audit.
- **Accountability culture.** This requires the appropriate governance and audit function and the inclusions of risk within the management capability of a business. Accountability also occurs when risk is included in performance metrics and when the performance metrics of the individual are aligned to the best long-term interests of a business.[12]
- **Mitigation activities.** An empowered culture is required to take measures to mitigate risk and to be proactive in the management of risk. This includes changes to role descriptions as well as skilling and training.
- **Facilitation group.** A small group is charged with the facilitation of risk management within the business. This group advises and provides assistance and expertise to all areas of business. It also provides strategic direction for the development of risk management and may be tasked with managing the implementation of risk management activities into business operations.
- **Standards.** This involves the alignment of risk management activities for compliance with and adoption of appropriate standards for respective business areas, together with enterprise-wide standards (e.g., ISO 31000).
- **Consistency and persistency.** Similar to other programs of work and ongoing business activities, consistency and persistency in performance is required,

and regular reviews, inclusions of lessons learned, and other standard management activities apply to risk management.

- **Persuasion, motivation, and mentoring.** This centers on the ability to influence people and to change the way things operate.

Successful implementation of risk management is likely to be in a phased approach, empowering managers to progressively deliver and reduce risks. Any implementation should be simple and pragmatic, should deliver business benefits to those doing the risk management, and should not try to address everything in one step. Focus on developing a base capability to a common level across the business and then mature the capability over time and in response to specific risks.

Successful implementation requires an alignment of risk management to other business activities and processes; for example, risk management with OH&S and security as part of business as usual. The alignment of risk management to the planning and budgeting processes can include:

- **CAPEX.** The capital expenditure process should include the ability to escalate risks and seek funding for risk mitigation.
- **Planning.** Business plans include risk identification and proposed risk mitigation. Any costs related to the risks are included within the respective budget. Revision of risk is part of the business plan review process.
- **Cost centers.** Cost of risk and provision for loss associated with the risk should be included within cost centers and activity-based accounting; that is, a provision for risk like the provision for bad debt.
- **Costing.** As part of the costing process, this includes recognition of both the cost of being proactive in mitigating risk and the cost of not acting to mitigate risk. Likely subsequent remediation costs need to be identified and provisioned.
- **Suppliers.** Risk management requirements should be included in supplier contracts, with appropriate clauses, incentives, and penalties.
- **Outsourcing vendor(s).** Provision for risk management is included within outsourcing contracts. The risk management activities of outsourcing vendor(s) are aligned to the risk management of a business, including appropriate clauses, incentives, and penalties for impacts on a business.

Any implementation is only as good as the people who implement the risk management regime and is only as effective as the people that manage and use a risk-based approach.

RISK AND BUSINESS BENEFIT

An understanding of risks within a business and the existence of the necessary capacities and capabilities provides a platform for realizing benefits from a risk-based approach. Some of these benefits are presented in this section.

Risk-Based Opportunities

Examples of risk-based opportunities are presented in Table 3.

Risk Benefits to Business Decision Making

Business decisions are made in response to risks, and business decisions affect the risk profile of a business. Consider the role of risk in any business decisions that may have been made by Qantas during a strike by engineers in 2008. A good understanding of risks would be required before any decision may have been made to sacrifice revenue from the busy Melbourne-Sydney-Brisbane triangle routes to stem a greater loss of revenue that may have occurred from shaken confidence by not being able to service all Australian capital cities.

Opportunities for improved decision making based on risk include:

- **Strategy revision.** Changes in risk are part of strategy review; for example, the emergence of the Apple iPad and resulting change in risk profile as well as strategies of media companies and computer hardware manufacturers. Therefore, businesses that are effectively managing their risk profile are better placed to manage strategy and business decision making.
- **Priority setting.** A risk-based approach affects business priorities. A rapid increase in the consequences of a risk and an increase in the likelihood of occurrence may see the business priorities change; for instance, a product recall may need to be invoked now that more information has come to light and could save costs in litigation.
- **Business plan revision.** Changes in risk profile may affect business plans, providing an opportunity to review business plans and realign resources and expenditures.

- **Resource allocation.** Changing priorities require reallocation of resources. Risk assessment helps determine the effectiveness of a solution, the resources required, and the overall business case for an activity; that is, better decision making.
- **Cost management.** Changes in risk profile can be used to influence cost management decisions. The merger of Reuters with Thomson changed the risk profile of many of its respective product offerings, leading to a consolidation of products and to lower costs.
- **Equipment replacement.** Increases in risk profile associated with the operation of old equipment can change the justification for replacement of equipment. An opportunity to standardize equipment could also see lower ongoing costs.
- **Program management.** The change in risk profile of the program, and more significantly the business impacts, can see an underperforming program changed or other programs initiated to realize business benefits.

Table 3 — Examples of Risk-Based Business Opportunities

Risk Details	Example Impact	Example Opportunity
Financial — risk from excessive debt levels in a business	One example of a debt-laden business was the Centro Properties Group that accepted the risk of too much debt and was caught by the global financial crisis, being forced to sell shopping malls and other assets.	Assets from Centro Properties Group were disposed of at heavily reduced rates to the benefit of competitors.
Market — risk from changes in consumer trends as a result of ICT consumption	Changes in ICT provide many risks to businesses, with the most current being changes in media consumption and the risks to print news of losing its business and to free-to-air commercial television of losing ratings (revenue).	Opportunity for new businesses to be established and take market share (e.g., *Huffington Post*, Google, or Facebook).
Market — risk of non-alignment with industry standard or emerging industry standards	IBM used QBE (Query By Example) for databases and did not respond to the risk of SQL (Structured Query Language) becoming an industry standard.	Oracle used SQL to become an industry standard, realized the opportunity provided by the standardization risk, and is now a de facto standard for relational databases.
Market — risk to telecommunication carriers around the emergence of broadband Internet	Telstra knew of the risk and opportunities associated with the emergence of broadband and implementing fiber networks but resisted while its customers were abandoning the older technology (copper network).	Telstra has the opportunity to reinvent itself and continue market leadership by providing a range of new and innovative products and services. Competitors have the opportunity to take market share from Telstra.
Operational — risk of loss of market opportunities due to quality of products and services	While many factors led to the rise of the Japanese auto manufacturers, one key element was a focus on quality by the Japanese (to gain market share) and the continuation of poor quality production within British manufacturers (leading to their decline).	Ability to gain market share from rivals through offering better-quality products and services (e.g., the use of exclusive brands in clothing).
Program — risk from poor risk management in a program (e.g., the now aborted Australian loft insulation program)	Program to insulate lofts in Australian homes was poorly managed and has since been suspended. Risks around the program were not well managed and became issues, with loss of life, householders living in unsafe homes, and significant damage to the image of the government.	The program offered opportunities to new businesses for loft insulation services and for existing installers to grow their business. Other risk-based opportunities have included compliance work, remediation work, and opportunities for legal services.
Regulatory — risk from certification (e.g., accountants or ISO 9000 to business)	When regulation is proposed for certification, the risk to businesses is that by not responding they will lose market share or not be allowed to operate.	Opportunities developed for those businesses providing certification. Those businesses that embraced certification can use it as a marketing tool to gain market share.
Strategic — risk to business from the availability of cheaper labor in other countries	China is now the world leader in manufacturing of all sorts of products and is still growing (e.g., car manufacturing), and many businesses that did not respond to the risk have suffered.	Businesses responded by offshoring operations to realize lower costs and gained market share. Alternatively, businesses have specialized in high-value products.

- **Change management.** A change in risk profile can provide extra stimulus for the implementation of a change initiative or the cancellation of a change activity that is underperforming.

Business Benefits from Risk

A risk-based approach provides opportunities for using risk to achieve a range of business benefits. Figure 5 shows the main business areas and likely business benefits to be seen.

Examples of business benefits from a risk-based approach include:

- **Brand preservation.** While the risk profile of a brand is dynamic, the use of a risk-based approach enables the risk profile of the brand to be managed. The implementation of meals deemed "Healthy Choices" by McDonald's is an example of how mitigation of the risk of brand damage due to the association of fast food with obesity has also increased sales and profits.
- **Business continuity.** Part of a risk-based approach is to turn the need for business continuity management from an ongoing cost to a tool for achieving business outcomes. Having the capability to route calls between call centers with cross-trained staff is good business practice, reduces risks, minimizes impacts, and forms a business continuity solution. This approach of developing durability and resiliency within a business both improves a business and makes better use of resources.[13]
- **Cash flow.** A decision to defer expenditure because a customer is likely to delay payment on an invoice is an example of a risk-based approach to cash-flow management. Through risk management, a business can make better use of its cash reserves and lower its cash-flow management expenses.
- **Change management.** The ongoing operation and maturity of a risk-based approach acts as an ongoing agent for change. Furthermore, strong risk management serves to minimize adverse impacts and increases the likelihood of successful change implementation.
- **Cost savings.** High-cost and high-risk operations tend to be synonymous; for example, the manual rekeying of data between systems requires expenditure on wages, is error-prone (risk and cost), and requires expenditure on remediation of errors. Reducing the risk of rekeying errors through systems integration also achieves cost savings.

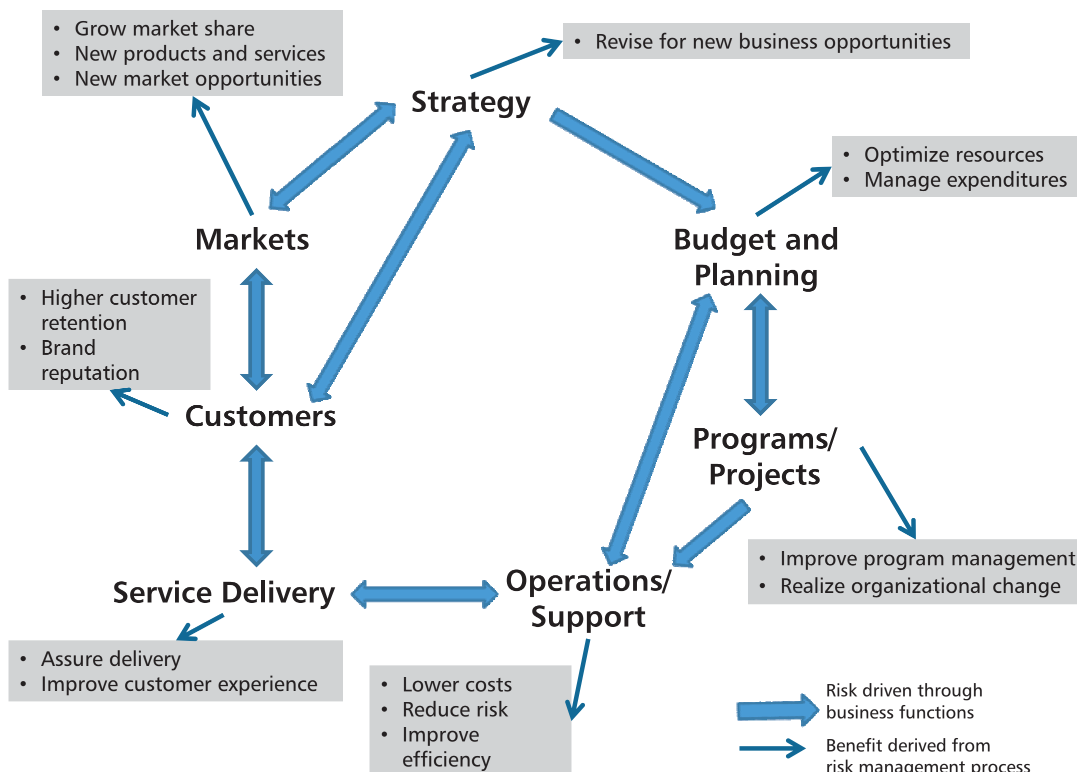


Figure 5 — Use of risk to realize business benefits.

- **Crisis management.** Certain industry sectors have a higher risk profile and are more vulnerable to crises (crises being the realization of a major risk); for example, aviation or toxic substance transportation. The management of a crisis requires the development and implementation of the necessary capacities and capabilities beforehand and then invoking them to manage a crisis. A risk-based approach sees the identification of potential crises (risks), taking actions to mitigate risk, and preparing for a crisis. By developing required crisis management solutions (see sidebar "Business Planning with a Risk-Based Approach"), a business can benefit from a skilled, cross-trained, and adaptive workforce.
- **Customer service.** A risk-based approach is seen in many areas of customer service; for instance, an assessment of the likelihood of winning a tender and whether it is worth the investment by a business. Prioritizing a customer of higher value over another in a resource-constrained environment occurs in a risk-based approach to business.
- **Market opportunities.** To realize an opportunity, risks need to be taken, and risks exist while that opportunity is realized. A risk-based approach is part of business operations to realize new and existing market opportunities.
- **OH&S.** Risk management is routine to OH&S practices. Where the risk-based approach brings other benefits is in establishing the overall risk profile for business areas and identifying a prioritization and utilization of resources; that is, most effective returns for cost incurred.
- **Operational performance.** The adoption of a risk-based approach and relating risk to performance metrics makes it harder for areas of underperformance to be "hidden away." A risk-based approach can also be used to minimize disruptions to operations with subsequent benefits of improved customer service.
- **Program management.** A risk-based approach to program management drives performance by holding underperforming programs accountable. The mitigation of strategic and resilience risks can also be used to establish and/or improve program management within a business.
- **Resource allocation.** A risk-based approach facilitates a prioritization of business activities and an allocation of resources; the issues register is the task list, and a risk register is the lower-priority items on a task list.
- **Revenue preservation.** Similar to cash-flow management is the role of risk management in preservation of revenues; for example, a decision to terminate profit-loss and end-of-life products to realize revenue from new higher-value products.
- **Compliance.** A risk-based approach can be used to ease compliance because an effective risk governance process would meet risk compliance and feed into the different compliance requirements of a business.

STRATEGIC RISKS AND BUSINESS CHANGE

Globalization and rapid changes in ICT are redefining markets and changing the way business processes are implemented. As a result, the roles of knowledge workers are being redefined and new management methods are being explored. Based on some future business trends recognized by the authors,[14] various likely aspects of strategic risks, possible impacts, and expected business benefits are identified in Tables 4a and 4b.

Some common risks across business as a result of changes in the business environment are likely to include:

- **People.** Business will require highly skilled resources who are active and empowered to problem solve. The ability of staff to work across channels in diverse environments will be the norm. The strategic risk of securing these resources and the necessary skilling and training is expected to be seen by many businesses.
- **Processes.** Strategic risk is seen in the new business processes that will evolve to meet the changing business environment. Aligning the management and governance frameworks to support an empowered workforce is expected be a significant risk in many businesses.
- **Information.** Meeting future information needs of the business, particularly information sharing across organizations, poses several risks to businesses. An increase in risk profile for security and privacy risks is already being seen.
- **Communication.** Risks in the adoption of mobile communications to support a mobile workforce are already being seen; for example, security risks from use of the iPhone. The communication risks are expected to increase significantly.
- **Infrastructure.** The strategic risk with infrastructure is the increasing rate of obsolesce as technology

Table 4a — Likely Future Trends in Business Risk Implications

Trend	Description	Likely Strategic Risk to Business	Risk-Based Approach Implications	Business Benefits and Opportunities
Decentralized command and control	Centralized decision making is too slow. Decentralization of command and control sees management within business and empowerment of problem resolution at source.	Manage risk associated with the skilling and training of managers as well as revision of management framework and performance management.	Risk-based decisions occur closer to source. Requires revision to risk management framework and governance to support decentralized command and control.	Opportunity to revise business governance and business operations.
Profiting from free	Adoption of profiting from free (e.g., Google provides free search to customers and profits from advertising paid for by others).	Key risk for media, entertainment, and publishing industries but affects all service- and content provision-based industries. Risk around development of correct revenue models.	Risk profile of product and services more dynamic, with products more easily copied and innovated by competitors.	Opportunity to leverage profiting from free to gain market share in both existing and new markets.
Value of how-to	Give away the "how to do it" but charge for the details, services, and support. From sales presentations to education and training to marketing and advertising, video on-demand and Webinars will be the default.	How to be competitive and derive revenue from "value of how to" services.	Risk profile of product and services more dynamic, with products more easily copied and innovated by competitors.	Strengthen customer loyalty by providing value-added service at minimal cost to business.
Mobile knowledge workers	Knowledge workers using multiple devices and operating in diverse environments to meet customer needs.	Revision and implementation of the ICT infrastructure necessary, together with changes in process and management frameworks.	Greater coordination of efforts required and risk of underperformance accommodated within risk frameworks.	Realize the benefits from an empowered and highly productive workforce.
Transaction processing	More transaction processing done by ICT. Need problem solvers to intervene when it goes wrong. Staff focus on exceptions management and high-value transactions that cannot be done by ICT.	Alignment of ICT and the skilling up of the workforce with active problem-solving skills.	Risk of major system failure(s) and/or risk of significant processing errors when things go wrong to be provisioned for within risk-based approach.	Opportunity to further automate routine transaction processing and to make better use of staff in high-value transaction processing and specialized customer service.
Virtual teams	Work changes from transaction processing to more project-based, with participants from many areas of business working collaboratively in virtual teams to deliver outcomes.	As more programs and projects are implemented, better program management and governance needed together with business-as-usual integration.	Risk profile of business increases as a lot of concurrent projects underway. Greater management of business implications around projects.	Derive value from an empowered and skilled workforce.

Table 4b — Likely Future Trends in Business Risk Implications

Trend	Description	Likely Strategic Risk to Business	Risk-Based Approach Implications	Business Benefits and Opportunities
Business planning	As ICT changes drive increased flexibility, there becomes a greater need to plan. The planning is about a framework that empowers delivery and providing infrastructure that allows people to adapt to meet customer needs.	Effective planning and management capability enhanced so that people are empowered to deliver.	Greater emphasis of risk within planning process and accommodated within risk management framework.	Use of planning to drive business operations and better communication within a mobile workforce.
Management framework	Changes will pose new challenges for managers driving the emergence of new methods of management, new operational frameworks, and new levels of accountability.	Development of new management frame-works and skilling of management to manage required workforce.	Risk-based approach to operations will be a fundamental plank of management framework.	Opportunity to revise management structures to achieve more efficient operations.
Product offering	Products and services come to market faster, have a shorter life expectancy in the market, and need to be targeted to ever more specific market segments.	Risk of developing the innovation and creativity culture and implementing organizational structures to support innovation and creativity.	Greater budget allocated to innovation with increased risk of fewer ideas yielding returns.	Gain new markets and revenue from revised products and services.
Consumer choice	Customers increasingly look to the trusted advisor to lead them through the ocean of choice and complexity and to bring them safely to the wise outcome.	Risk of revision to sales model, together with reskilling of the sales team across channels.	Management of customer volatility.	Market recognition through differentiation and value-added service.
Getting the message across	Need to get a message across different channels in an environment of information overload where people tune out to cope and have shorter retention spans.	Inability to communicate a sticky message across channels will under-mine the brand with subsequent business impacts.	Additional dimensions to risk management of brand required.	Opportunity to differen-tiate position in the market and attract customers.

improves. The obsolescence risk would be managed through a business-as-usual process for product management risk.

- **Suppliers.** The strategic impacts of changes in suppliers are likely to occur as part of the routine change in business processes to market dynamics. Risk management would include regular supplier review, ability to multisource from suppliers, and sourcing new suppliers for evolving services and offerings.
- **Third parties.** The strategic risk with third parties in the changing business environment is expected to be split around trends in outsourcing and changes in regulation that occur over time.
  - *Regulation.* The regulatory framework usually responds to events and often causes major changes; for example, changes to border security after 9/11. The time required to shape regulation usually gives business time to manage the regulatory risk as part of ongoing business processes.

- *Outsourcing.* The changes in outsourcing are likely to be driven by how the outsourcing vendors themselves respond to the changes in markets over the period.[15] In terms of strategic risk to a business, trends in the use of specialist outsourcing vendors for specific business functions and greater integration of outsourcing vendors into business functionality are expected to continue.

CONCLUSION

A risk-based approach to business formalizes and aligns many current activities to include the use of risk for achieving better business outcomes. Any implementation of a risk-based approach is a change management program to progressively develop capacities and capabilities, including board ownership and accountability for risk, effective governance, the alignment of risk management to other business processes, and active risk mitigation and impact minimization at the source as part of business as usual. Successful operation of a risk-based approach embeds durability and resiliency into a business to ensure management of known risks and effective response to unknown risks. Risk mitigation and impact minimization can be used to achieve benefits from a risk-based approach, including brand preservation, cash-flow management, protection of revenue, cost savings, improved customer service, and realization of market opportunities. Any risk-based approach to business is only as good as its implementation and as effective as the managers who use it.

ACKNOWLEDGMENTS

Thanks to Kathy Dube and Dr. Patrick McConnell for their informative discussions on aspects of risk and for reviewing this report. This report is based on the experiences of the authors in a range of corporations, which have helped shape their approach to ERM.

ENDNOTES

[1]Norris, Floyd. "Market Drop Fueled by a Crisis, Anxiety and an Error." *New York Times*, 6 May 2010.

[2]A risk is something that has the potential to affect the achieving of an outcome. An issue is a realization of a risk and is something that is now having an impact on achieving an outcome.

[3]Sherringham, Keith. "Pragmatic Business Takeaways from the Icelandic Volcanic Ash Events." Contingency Planning & Management, 5 May 2010 (http://contingencyplanning.com/articles/2010/05/05/pragmatic-business-takeaways-from-the-icelandic-volcanic-ash-events.aspx).

[4]The less ethical practices of a minority of insurance companies that refuse payment and wait to be sued for nonpayment is another example of a risk-based approach to business operations.

[5]Charette, Robert N. "Showing Value in Risk Management Is Tough, Worth the Effort." Cutter Consortium Enterprise Risk Management & Governance *E-Mail Advisor*, 8 April 2010.

[6]Sherringham, Keith. *Cookbook for Market Dominance and Shareholder Value: Standardising the Roles of Knowledge Workers*. Athena Press, 2005.

[7]The share price of Apple has fluctuated significantly in response to the presence of Steve Jobs as CEO.

[8]"Overview of Enterprise Risk Management." Casualty Actuarial Society, May 2003 (www.casact.org/research/erm/overview.pdf).

[9]Charette, Robert N. "The Rise of Enterprise Risk Management and Governance." Cutter Consortium Enterprise Risk Management & Governance *Executive Report*, Vol. 1, No. 1, 2004; Sobel, Paul J., and Kurt F. Reding. "Aligning Corporate Governance with Enterprise Risk Management." *Management Accounting Quarterly*, 2004.

[10]Doughty, Ken. "Enterprise Risk Management Framework: A Practical View." Cutter Consortium Enterprise Risk Management & Governance *Executive Report*, Vol. 7, No. 1, 2010.

[11]Hiatt, Jeffrey M. *ADKAR: A Model for Change in Business, Government and our Community*. Prosci Research, 2006.

[12]DeMarco Tom. "Can't Anybody Do Risk Management?" Cutter Consortium Business Technology Trends & Impacts *Council Opinion*, Vol. 10, No. 4, 2009.

[13]Sherringham, Keith. "The Volcanic Dust Cloud: Some Business Continuity Lessons." Continuity Central, 23 April 2010 (www.continuitycentral.com/feature0770.html).

[14]Sherringham, Keith, and Bhuvan Unhelkar. "Strategic Elements for the Mobile Enablement of Business." In *Handbook of Research in Mobile Business: Technical, Methodological and Social Perspectives*. 2nd edition. Edited by Bhuvan Unhelkar, IGI Global, 2009; Sherringham, Keith, and Bhuvan Unhelkar. "Strategic Business Trends in the Context of Green ICT." In *Handbook of Research on Green ICT*. Edited by Bhuvan Unhelkar. IGI Global, forthcoming 2010.

[15]Sherringham, Keith. "Outsourcing? Hollywood Knows How." *Information Age*, February/March 2007.

ABOUT THE AUTHORS

Keith Sherringham has more than 15 years' experience in business consulting in corporations and in government at executive and senior leadership levels on business strategy and planning; business improvement through risk management and resiliency; and the business application of ICT. Mr. Sherringham is also an author and speaker with recognized thought leadership in areas that include real-time decision making, standardizing the roles of knowledge workers, and green ICT. He is former Director of the Australian Computer Society with responsibility for strategy and planning and has guest lectured at various universities in Australia on the business impacts of changes in ICT. As a company director and mentor to CEOs and boards within nonprofits, Mr. Sherringham also brings his practical pragmatic business experience to address organizational performance and board and executive relationships in nonprofits. He can be reached at shocs@bigpond.com.

Bhuvan Unhelkar is a Senior Consultant with Cutter Consortium's Business-IT Strategies and Enterprise Architecture practices. He has more than two decades of strategic as well as hands-on professional experience in the information and communication technologies (ICT) industry. As a Founder of MethodScience.com, Dr. Unhelkar has notable practical consulting and training expertise in software engineering (object modeling, processes, and quality), enterprise architecture (including SOA), project management, collaborative Web services, environmental responsibilities, and mobile business. His domain experience includes financial, insurance, government, as well as telecommunication organizations wherein he has created industry-specific SOAs, process maps, quality strategies, and business-transformation approaches.

Recently, Dr. Unhelkar has updated three large organizations (two banks and an insurance organization) in the use of composite agile and demonstrated the concept through training and workshops. His other courses over the past few years in the aforementioned areas have now been delivered to business executives and IT professionals globally, from Australia, the US, Canada, and the UK to China, India, Sri Lanka, New Zealand, and Singapore. Training courses delivered through MethodScience are consistently ranked highly by the participants. Dr. Unhelkar earned his PhD in the area of object orientation from the University of Technology, Sydney, in 1997. Subsequently, he designed and delivered courses on such topics as global information systems, object-oriented analysis and design, business process reengineering, and IT project management in the industry as well as across universities in Australia, China, and India.

Dr. Unhelkar leads the Mobile Internet Research and Applications Group (MIRAG) at the University of Western Sydney, where he is also an adjunct Associate Professor. He has written/edited 15 books in the areas of collaborative business, globalization, mobile business, software quality, business analysis, business processes, and UML and has extensively presented and published papers and case studies. Dr. Unhelkar's current research interests include the application of emerging technologies to enterprise architectures, business analysis in the context of agile, smart sourcing, and environmentally responsible business strategies. He is writing two books: *The Art of Practicing Agile: Applying Composite Agile Method and Strategy to Real Projects* and *Green IT: Strategies and Applications*. Dr. Unhelkar is a sought-after speaker, a Fellow of the Australian Computer Society (elected to this prestigious membership grade in 2002 for distinguished contribution to the field of ICT), life member of the Computer Society of India, Rotarian at St. Ives (Paul Harris Fellow), discovery volunteer at NSW parks and wildlife, and a previous TiE Mentor. He can be reached at bunhelkar@cutter.com.

APPENDIX: GLOSSARY

A risk-based approach to business — formalizes the management of risk across all areas of a business and includes risk management within all aspects of business to achieve better business outcomes.

Business risk — generic term for a range of risks occurring within a business; for example, credit risk or occupational health and safety (OH&S) risk.

Enterprise risk management (ERM) — a risk-based approach to business, integrating risk management into business operations to achieve better outcomes.

Financial risk — risks related to financial management of a business.

Impact minimization — measure taken to reduce the impact of risk when it is realized.

Issue — realized risk. Something that is affecting the achievement of an outcome.

Market risk — risks related to the actions of markets on a business.

Objective risk — risks influencing the setting of objectives and outcomes and risk resulting from the setting of objectives.

Operational risk — risk related to the operation of a business. Also has a specific meaning in financial market regulation.

Program risk — risks in a project or program of work. Also used for the overall risk profile of a program upon a business; for example, risk of cost overruns on business operations.

Regulatory risk — risks related to legislation on a business.

Residual risk — amount of risk remaining after agreed level of mitigation implemented.

Resilience risk — having high impact but low likelihood of occurrence; for example, loss of building.

Risk — something that has the potential to affect the achievement of an outcome.

Risk appetite — how accepting of risk a business is and its willingness to accept more or less risk to achieve an outcome.

Risk mitigation — measure taken to reduce the likelihood of risk occurring.

Risk profile — a consolidated view of risks within an entity; for example, the overall risk profile of a business.

Risk rating — an assessment of the likelihood of a risk occurring and the likely impacts of a risk.

Risk owner — the owner of a risk who is responsible and accountable for all aspects of a risk.

Slow burn — a risk with a high likelihood of becoming an issue, but the impacts are expected to take a while to be seen.

Strategic risk — risks influencing the setting of strategy and risk resulting from the setting of strategy.

©2010 Cutter Consortium

Cutter Consortium

SUMMIT 2010 North America

Interact with the Experts in IT

Strategies for the Road Forward

Summit 2010

25–27 October 2010 | Cambridge, MA, USA

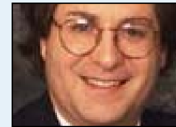
Why Attend Summit 2010?

An economy that's only just beginning to inch back to "normal" and the relentless forward march of technology have not stopped every IT organization from providing the differentiators their enterprises need to succeed. Our mission is to ensure Cutter's clients are among them. We have designed *Summit 2010* to further that goal. Join us to explore the issues you should be pondering and the strategies you should be implementing to ensure you're providing the most value to your organization.

Summit 2010: Unlike Any Other IT Conference

You'll get advice that is insightful and forthcoming. You'll have a chance to voice your opinion and hear the opinions of international experts and various IT professionals. You'll debate with — and listen to the debate among — some of today's most experienced and clear-thinking business technologists. And you'll return home with ideas to implement right away. Our only agenda is to support you by providing a forum for thinking about your business world — outside of the box. Don't miss this opportunity.

Visit www.cutter.com/summit.html to register.



Security, Privacy, and Risk: Shaping Cloud Computing
Keynote by Lou Mazzucchelli

Agile Leadership: What It Takes
Keynote by Jim Highsmith

The Cost and Value of IT
Case Study by Rogelio Oliva

Shared Services: Transitioning from Efficiency to Effectiveness
Keynote by Robert Scott

What Does It All Mean?
Keynote by Rob Austin

IT Governance
Seminar with Bob Benson

How Architecture Has Resulted in Competitive Leadership: A Case Study
Seminar with Mike Rosen

CIO and IT Managers Forum
Seminar with Rob Austin

Cloud Computing: Fear, Hype, Reality, and Pragmatics
Seminar with Claude Baudoin

The Changing Face of Government IT
Seminar with Mitchell Ummel

Technical Debt Assessment: The Science of Software Development Governance
Lesson by Israel Gat and Jim Highsmith

Jump ahead of the competition. Reserve your seat for *Summit 2010* today!

"The *Summit* stretched my thinking in some new directions."

— Martin Malley, AVP, Information Systems, Union Pacific Railroad

"Engaging in a way that other conferences don't accomplish."

— David Smalley, IT Group Manager, Progressive

"Learned some new ways of looking at or managing things."

— David Sum, Director, Product Platforms, Custom House

Cutter Consortium
Access to the Experts

Register Today

To ensure a lively and interactive event, attendance for *Summit 2010* will be limited. Register early and guarantee a space for yourself at this exclusive conference.

Return this form by fax to +1 781 648 8707, or mail it to Summit 2010, Cutter Consortium, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA. Checks should be made payable to Cutter Consortium. To register by phone, call +1 781 648 8700. Or visit www.cutter.com/summit.html to register online.

	# Registrants	Total
Summit 2010 Conference (25–27 October 2010) ☐ US $1,995 each	____________	$____________

If you would like to register your team for *Summit 2010*, please contact your account representative for multiple-attendee discounts.

Name	Title
Organization	Department
Address	Mail Stop/Suite #
City	State/Province
ZIP/Postal Code	Country
Telephone	E-Mail

☐ Check enclosed (payable to Cutter Consortium).
☐ Please invoice my company.
☐ Charge MasterCard, Visa, AmEx, or Diners Club. (Charge will appear as Cutter Consortium.)

Account Number	Expiration Date
Name on Credit Card	Signature

Registrant #1 Name	Title
Registrant #2 Name	Title
Registrant #3 Name	Title
Registrant #4 Name	Title

Registrations for *Summit 2010* are transferable. If you find that you cannot attend, you may transfer the registration to another member of your organization at any time prior to the first day of the event. Cancellations after 30 September 2010 are nonrefundable. In the unlikely event that Cutter Consortium cancels the conference, Cutter Consortium is not responsible for any airfare, hotel, or other costs incurred by registrants. Speakers subject to change without notice.

60R*AO5FLY

About the Practice

Enterprise Risk Management & Governance Practice

The Enterprise Risk Management & Governance (ERM&G) practice area focuses on helping organizations assess their total risk spectrum and manage it as a whole. Through the subscription-based advisory service, the ERM&G team of Senior Consultants helps organizations implement sound risk management and governance strategies that allow for innovation and profitability, even under the increasing pressures of compliance. You'll get the tools and strategies you need to make better decisions, gain the trust of your corporate leaders, and create a risk-taking culture that minimizes risk and maximizes valuable opportunities for your organization.

Consulting and training services within this practice area are customized to meet your organization's needs. Our team of practitioners can provide their expertise to help your organization create enterprise risk management frameworks, develop business continuity plans, identify and manage operational and enterprise risk, achieve compliance with corporate governance directives, identify IT security risk, understand the impact of outsourcing on IT auditing, and more.

The ERM&G practice provides your organization with the guidance it needs to comprehend and manage its enterprise risks in a manner that yields the most value from its IT investments.

Products and Services Available from the Enterprise Risk Management & Governance Practice

- The ERM&G Advisory Service
- Consulting
- Inhouse Workshops
- Mentoring
- Research Reports

Other Cutter Consortium Practices

Cutter Consortium aligns its products and services into the nine practice areas below. Each of these practices includes a subscription-based periodical service, plus consulting and training services.

- Agile Product & Project Management
- Business Intelligence
- Business-IT Strategies
- Business Technology Trends & Impacts
- Enterprise Architecture
- Enterprise Risk Management & Governance
- Innovation & Enterprise Agility
- IT Management
- Measurement & Benchmarking Strategies
- Social Networking
- Sourcing & Vendor Relationships

Senior Consultant Team

The Cutter Consortium ERM&G team includes seasoned practitioners in the enterprise risk management and governance arena. Dr. Robert Charette, Director of the ERM&G practice, is recognized as an international authority and pioneer regarding information systems, technology, and risk management. He also serves as a senior risk advisor to Global 100 CEOs, CFOs, program and project managers, as well as to senior government officials worldwide. Collectively, the Senior Consultants on the ERM&G team have decades of experience working for government and private industry in performing enterprise and program risk assessments and management, audits, corporate compliance, legal risk management, and risk consulting as it applies to strategic, operational, technical, and financial risk.

- Robert N. Charette, Director
- Steve Andriole
- Robert D. Austin
- Edmund H. Conrow
- Steven I. Cooper
- Sara Cullen
- Tom DeMarco
- Lynne Ellyn
- Andrew Fried
- Scott Hastings
- Rebecca Herold
- Sebastian Konkol
- Steven R. Kursh
- Tim Lister
- Gerald H. Peterson
- Carl Pritchard
- Mark Seiden
- Mike Sisco
- Scott Stribrny
- Catherine L. Szpindor
- William Zucker