

business.gov.au (<https://www.business.gov.au/>)

Home (<https://www.business.gov.au/>)

- > **Risk management** (<https://www.business.gov.au/risk-management>)
 - > **Risk assessment & planning** (<https://www.business.gov.au/risk-management/risk-assessment-and-planning>)
 - > Risk management strategies
-

Risk management strategies

Last Updated: **27 July 2018**

Making a strategy for risk management can involve more than just deciding whether to accept the risk or not.

If your business is part of a bigger supply chain that involves retailers, distributors or primary producers, you can spread the risk across a number of areas.

By spending time and resources on your risk management strategy, you'll provide a safe workplace and reduce the chances of negative impacts on your business.

Consider these steps when forming your risk management strategy:

Identify the risks

Working out the risks to your business could be as easy as thinking about what could go wrong, and how and why it could happen. You might also need to do some research into:

- past events and risks
- possible future changes to your business environment, such as changes in economic trends (find out how to conduct [market research](https://www.business.gov.au/Marketing/Marketing-research) (<https://www.business.gov.au/Marketing/Marketing-research>) and [industry research](https://www.business.gov.au/Planning/Templates-and-tools/Industry-factsheets) (<https://www.business.gov.au/Planning/Templates-and-tools/Industry-factsheets>))
- social and community issues that could affect your business.

To identify risks, you can also:

- look at hazard logs, incident reports, [customer feedback \(https://www.business.gov.au/People/Customers/Seek-customer-feedback\)](https://www.business.gov.au/People/Customers/Seek-customer-feedback) and complaints, and survey reports
- review audit reports such as financial audit reports or workplace safety reports
- do a strength, weaknesses, opportunities and threats (SWOT) check for your business (download our [marketing plan template \(https://www.business.gov.au/Planning/Templates-and-tools/Marketing-Plan-Template-and-Guide\)](https://www.business.gov.au/Planning/Templates-and-tools/Marketing-Plan-Template-and-Guide) for instructions on how to do this)
- discuss business issues with your staff, customers, suppliers and advisers.

Analyse the risks

After identifying the risks to your business, it's time to work out which ones are urgent. To analyse the risks related to an event (such as a competitor moving into the same street), you should first look at:

- the **damage** that the risk would cause (for example, the risk of fewer customers means lower sales for your business)
- the **likelihood** of the risk happening (for example, think about how similar the competitor's business is to yours, and how loyal your customers are).

Work out a rating system for damage and likelihood. For example, you could have:

- ratings of 1 to 4 for damage (1 for slight damage, and 4 for severe damage)
- ratings of 1 to 4 for likelihood (1 for not likely, and 4 for extremely likely).

Finally, to work out the level of risk for an event, use this formula: **risk level = damage x likelihood**
Based on our example above, the lowest risk level you could get is 1 (1 x 1), and the highest risk level you could get is 16 (4 x 4). You can use the risk levels to rank your risks from least urgent to urgent.

Evaluate the risk

To evaluate a risk, you should compare the level of risk for various events against your risk criteria (find out how to set your risk criteria when you design a [risk management plan \(https://www.business.gov.au/Risk-management/Risk-assessment-and-planning/Risk-management-plans\)](https://www.business.gov.au/Risk-management/Risk-assessment-and-planning/Risk-management-plans)). You should also check if your existing risk management methods are enough to accept the risk.

When to accept risk?

Sometimes businesses choose to accept risks and not spend any resources on avoiding them. You might decide to accept a level of risk for the following reasons:

- The cost of treatment is much higher than the potential results of the risk.
- The risk level works out to be very low.
- The benefits of taking the risk greatly outweighs the possible damage.

What to do...

- Incorporate risk management into your broader [business plan \(https://www.business.gov.au/Planning/Business-plans/Writing-a-Business-Plan\)](https://www.business.gov.au/Planning/Business-plans/Writing-a-Business-Plan) and [emergency management plan. \(https://www.business.gov.au/Risk-management/Emergency-management/How-do-I-write-an-Emergency-Management-Plan\)](https://www.business.gov.au/Risk-management/Emergency-management/How-do-I-write-an-Emergency-Management-Plan)
- Learn how to [protect your business from the unexpected \(https://www.business.gov.au/Risk-management/Emergency-management/Protect-your-business-in-an-emergency\)](https://www.business.gov.au/Risk-management/Emergency-management/Protect-your-business-in-an-emergency).

broadleaf.com.au

Evaluating the effectiveness of risk management – Broadleaf

14-17 minutes

This guide describes a systematic way of finding how effective is an organisation's current approach to managing risk. It considers the intentions of the organisation, how they are expressed and communicated and also what happens in practice. This leads to a realistic improvement program for the organisation's framework for managing risk and each application of the risk management process. The guide stresses how management must be involved in all stages to ensure success.

Introduction

All organizations of all kinds face internal and external factors and influences that make it uncertain whether, when and the extent to which they will achieve or exceed their objectives. These objectives are its highest expression of intent and purpose, and typically reflect an organisation's explicit and implicit goals, values, and imperatives or relevant enabling legislation.

The international risk management standard, ISO 31000:2009, defines risk as the effect of uncertainty on objectives. The effective management of risk is therefore essential if organisations are to achieve their objectives and satisfy the needs of their stakeholders.

It has been long recognised that good governance and effective management are best achieved through the development and deployment within an organisation of one coherent and consistent framework, methodology and vocabulary for management of risk, to be used for all types of activity. This ensures that:

- There is a consistent and defensible basis for decision making at all levels, particularly where effort or capital is expended
- Change activities are more likely to succeed
- The organisation can pre-empt and capitalise on external changes such as those involving demographics, customers' needs and government policy
- All employees are encouraged to focus on and give priority to actions that aid and enhance the execution of strategic and project plans and the organisation's objectives
- The organisation is prepared for and protected from major incidents and losses
- Tactical moves, to identify and seize opportunities are stimulated and enhanced
- Accountability for risks and, most importantly, for controls and the monitoring and assurance of controls is clear and not doubtful.

In time this will also lead to a significant change in culture as the organisation as its employees engage on activities directly related to ensuring the achievement of goals and objectives and the successful completion of projects.

What is a framework and how does it lead to effective risk management?

An organisation's ability to manage risk effectively depends on its intentions and its capacity to achieve those intentions. This intent and capacity is referred to as its risk management framework and is part of its system of governance and management.

The quality of the framework is important because effective risk management requires:

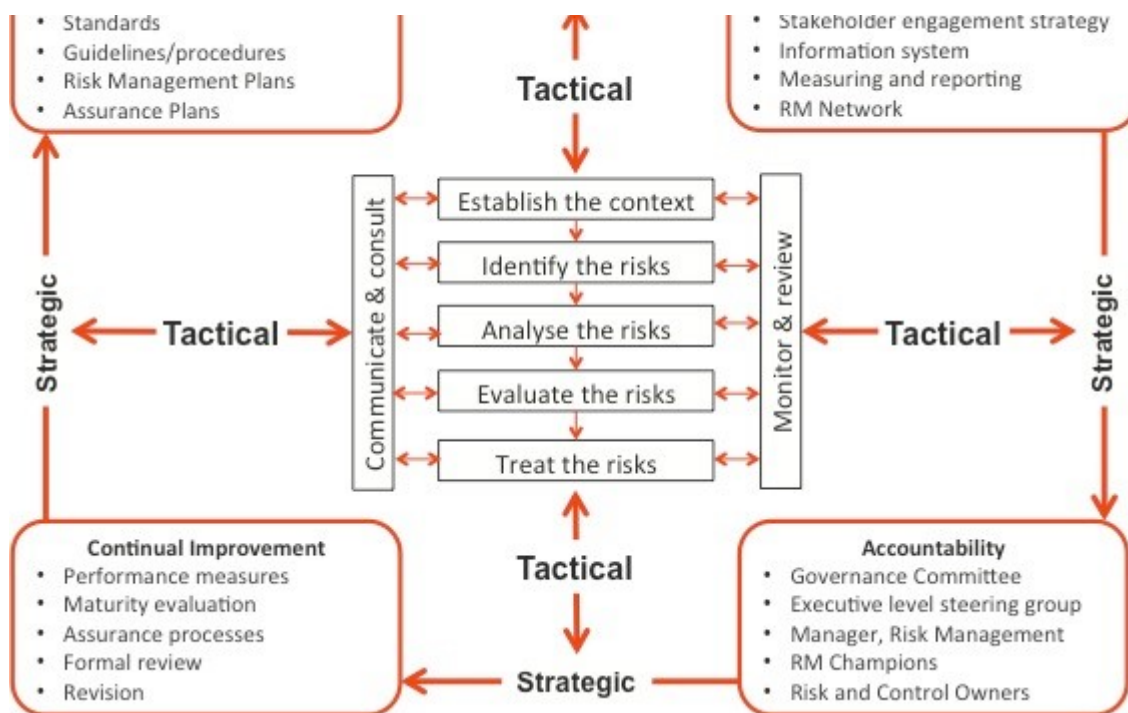
- Clear expectations from 'the top'
- Appropriate capability (skills, resources, support)
- Sound relationships with stakeholders
- Integration of necessary risk management practices into the day-to-day activities and accountabilities of the management team
- A commitment to continually learn and improve.

The risk management framework should not attempt to replace the natural capability of people to manage risk; rather it should enhance good practices so that the process is reliable, comprehensive and consistent. For this to occur and for the required capability to be achieved, the organisation requires:

1. A set of suitable 'tools'
2. A coherent approach to training and communicating to people so that they can use those tools in a competent and consistent manner
3. An approach that signals and reinforces the correct behaviour and way of thinking.

The typical elements of a framework and an illustration of how this supports the integration of the risk management process is shown in the figure below.





The framework for risk management

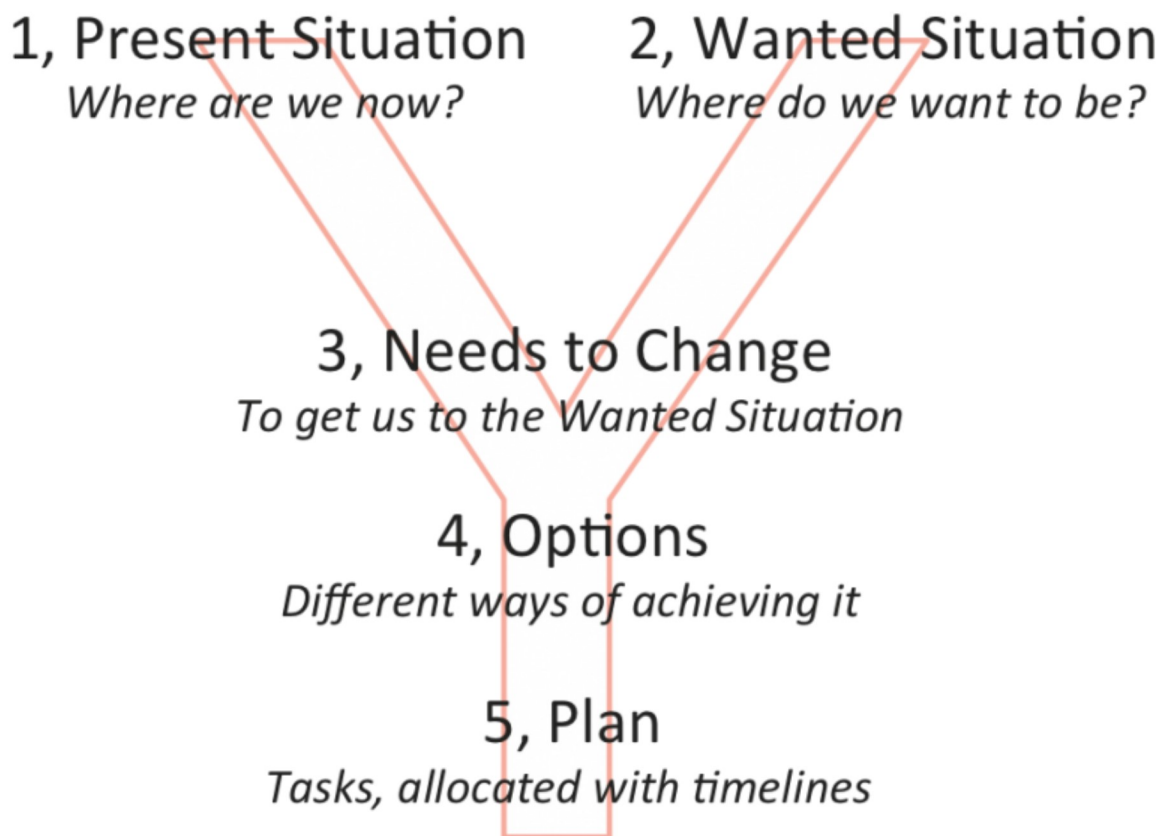
General approach to effectiveness evaluation

After many years of practical experience in evaluating and enhancing frameworks for risk management in organisations, Broadleaf believes that success depends as much in the manner in which any changes to a framework are developed and implemented as it does in the detail of the tools and written materials generated. This is why we would strongly recommend to our clients that we help it through a management of change process, where key internal stakeholders are carefully involved and engaged in evaluating the existing approach and in planning how, where and when enhancements will be made.

The core of this management of change process involves internal stakeholder representatives participating in a facilitated gap analysis and evaluation that then leads to a clear and practical enhancement and implementation plan. This is depicted in the “Y Model” shown in the figure and described below.

To enable those stakeholder representatives to participate effectively, they need to be well briefed on current risk management thinking and shown examples drawn from other organisations of elements of a risk management framework.

This approach has the added benefit that the participants of this process then become the organisation's "Champions" who are motivated to lead the implementation process in their own departments and functions. They also act to convince their superiors of the merits of the approach and motivate acceptance and use.



Y Model

To be successful and efficient, the management of change approach requires:

1. An accepted and accurate representation of the current

arrangements for managing different forms of risk – the *present situation*

2. The fundamental concepts of risk and risk management and the desired goals in terms of the risk management framework and process to be clearly understood by those sponsoring the change – the *wanted situation*
3. A clear and accepted appreciation of the elements of the existing framework that need to be enhanced or improved and the nature of those changes and any additional elements that need created – *what needs to change*
4. The exploration of options, constraints, enablers and critical paths leading to an appropriate plan of actions with timings
5. A clear commitment to the plan and its implementation through the allocation of suitable resources by senior management and by their continued oversight of progress.

These steps can be tackled separately and the results fed back to senior management. However, after many years and numerous attempts we have found that most efficient approach, and the one that gains the greatest degree of ownership and endorsement, is to involve representatives of senior internal stakeholders in all these steps over a short space of time. This approach is described in detail below.

Phase 1 - Preparation

Evaluation studies typically start with an initial meeting where the detailed arrangements, including the schedule of activities and delivery dates, the documents to review reviewed and the interview candidates are agreed.

Prior to the meeting we issue a checklist of background documentation we would like to review and will often open up a secure Internet portal to which documents can be uploaded. This list can include:

- Relevant policy statements, framework descriptions, internal standards and procedures, with a particular focus on decision support and controls assurance
- Internal standards, procedures or guidelines that deal with particular applications of risk management. For example in the area of safety, procurement, security, operations, maintenance, BCM, compliance and project management
- The current strategic plan and objectives
- Examples of risk management plans and control assurance plans
- Extracts from the risk management information system including risk registers and risk treatment plans
- Methodology for and outputs from any quantitative risk analysis studies (range analyses) for schedule, capital and value evaluation and contingency estimation
- Copies of recent reports to any risk management steering committees or review groups and the oversight committee that show risk management performance
- Copies of any existing training and briefing materials that deal with risk management.

We then normally undertake a preliminary review of the materials and, from this, develop an aide memoire of sample questions that we might ask those we interview. This document is sent to those who are to be interviewed to allow them to prepare.

Phase 2 - Elicitation and verification

In our experience it is vital to observe and review how risk management takes place in practice. This is particularly true if there might be any discontinuity of practice across the organisation or inconsistent processes and systems. It is also important to test management's perceptions of the current approach to risk management to see if it is currently viewed as effective and is likely to satisfy their future needs.

We therefore undertake this observation through a series of structured interviews with senior managers from which we will draw conclusions on:

- The suitability of the current framework and tools to manage risk associated with an organisation of a comparable size and complexity, its risk profile and the risk criteria that should reflect its attitude (appetite)
- The drivers of that attitude, based on what are recognised as the 'key success factors' and growth objectives for the organisation
- The perceived usefulness of the current risk management process and its degree of integration into key decision-making processes;
- The strengths and limitations of the other approaches to risk management specific to particular kinds of risks that co-exist in the organisation
- Whether the tools and methods currently being used are capable of providing the organisation with a current, correct and comprehensive understanding of its risks and inform it whether the risks are within its risk criteria
- The level of understanding of senior managers about aspects of the

risk management culture

- An outline of the perceived risk profile of the organisation and whether this varies from the risks reported to senior management and oversight committees.

Each interview usually takes about one hour and a member of the organisation's risk function normally accompanies us to help transfer knowledge.

While the predominant purpose of the interviews is to obtain information from the participants to support our review, they also provide an opportunity to explain the purpose of the study.

At the conclusion of the series of interviews we normally provide immediate feedback to the organisation's risk staff on:

- Our findings
- Our conclusions on the level of maturity, the strengths and weaknesses
- Our initial thoughts on where the organisation could enhance the management of risk and the steps that should be taken.

This meeting also allows any misunderstandings or misperceptions to be rectified.

Phase 3 - Gap analysis and evaluation

Using the information we have gathered we conduct a detailed gap analysis and evaluation of effectiveness using the guidelines and principles in ISO 31000 and what we understand is world's best practice as a basis for comparison. Often this is conducted as a facilitated workshop involving the management team.

The gap analysis looks at how the organisation expresses its intentions for managing risk and the elements of the capacity it claims it provides. In practice this involve us looking all the elements of the risk management framework and process shown above to determine if they are present and are suitable for the organisation and its environment.

We normally prepare a full gap analysis and evaluation report that includes our findings in terms of:

- The framework and how it facilitates the integration of risk management into decision making, including risk management plans and the strategy for their implementation
- How risk management is applied in strategy development and during the concept and development phases of projects, for decision-making and change management and as part of design review
- Control assurance and reporting
- The reliability of each element of the risk management process
- How risk management is used to deal with changes and to provide contingency arrangements that respond to disruptions, including how learning and feedback take place after events, incidents and decisions
- How the overall risk profile of the company is obtained and evaluated through aggregation and roll-up and how risks are treated at a corporate level
- The form and content of governance reporting
- How risk treatments are closed out and monitoring and review of risks, controls and risk treatments occurs

- The organisation's culture as it pertains to the management of risks in terms of both intent and practice
- The adequacy and effectiveness of the systems and resources available to support the management of risk, including human resources.

Phase 4 - Gaining ownership and detailed planning

We believe that it is important that senior managers appreciate and can comment on our findings and conclusions and that this leads to support for any enhancement plan. It is important that this takes place before our report is made available to the oversight committee so that it can indicate management's response.

We therefore normally present our findings and recommendations at a short meeting with senior managers. A typical draft agenda will be:

- Fundamentals of risk and best practice risk management
- Overall findings and assessment of the benchmarking review
- Suggested improvements and enhancement strategies
- Draft enhancement plan.

The planning component of this session follows the 'Y model' (see above) to elicit feedback and ownership of the current situation, the wanted situation and what needs to change. The management team is encouraged to discuss and compare options and then to finalise the enhancement plan actions and agree timelines. These agreements are recorded and included in our final report.

Phase 5 - Report to the oversight committee

Our clients often ask us to present our findings to their oversight committee. This provides them with the confidence that the evaluation was conducted in an independent manner and to enable the members to challenge and question any outcomes.

Normally our report is accompanied by the management-agreed enhancement plan, to indicate the organisation's commitment to improvement.

In most cases the oversight committee is provided with progress reports against this enhancement plan at subsequent meetings.

business.gov.au (<https://www.business.gov.au/>)

Home (<https://www.business.gov.au/>)

- > Risk management (<https://www.business.gov.au/risk-management>)
 - > Risk assessment & planning (<https://www.business.gov.au/risk-management/risk-assessment-and-planning>)
 - > Risk management scenarios
-

Risk management scenarios

Last Updated: **27 July 2018**

When the idea of managing risks in your business doesn't seem like an everyday occurrence you need to think about, then think again. Here are some scenarios that will make you think twice about risk management.

Identify risks

Jane runs a catering business and is thinking about buying a new delivery van. She works out the risks of buying a van, such as extra expenses if the van breaks down.

However, Jane should also focus on the other opportunities she could take with the same amount of money. Her other choices include buying new equipment or hiring more staff.

If she buys a van instead of hiring more staff, she risks missing out on the benefits of having more staff, such as faster customer service in her business. She should try to compare the future impacts of each possible choice before making her decision.

After identifying the risks, Jane can work out which ones are urgent. To analyse the risks related to an event, you should first look at:

- the **damage** that the risk would cause (for example, the risk of fewer customers means lower sales for your business)
- the **likelihood** of the risk happening (for example, think about how similar the competitor's business is to yours, and how loyal your customers are).

Work out a rating system for damage and likelihood. For example, you could have:

- ratings of 1 to 4 for damage (1 for slight damage, and 4 for severe damage)
- ratings of 1 to 4 for likelihood (1 for not likely, and 4 for extremely likely).

Finally, to work out the level of risk for an event, use this formula: **risk level = damage x likelihood.**

Based on our example above, the lowest risk level you could get is 1 (1 x 1), and the highest risk level you could get is 16 (4 x 4). You can use the risk levels to rank your risks from least urgent to urgent.

Evaluating risks

Petra runs a clothing retail store. She worries about the rise in theft during the busy end of year period. To manage this, she does a detailed assessment. She works out that she lost \$5000 to theft last December. As a result, she has security cameras installed in her store which leads to a 40% reduction in loss due to theft. She works out the expected loss at:

Expected loss (current year) = \$5000 – (\$5000*40%) = \$3000

She expects similar levels of theft this year. To reduce the risk of theft even more, the next step will be to hire a security guard during working hours. The cost of hiring a security guard for a month will be \$4000 which is more than the expected loss, so she decides to accept the risk.

Instead of hiring a security guard, Petra meets with her staff to brainstorm possible ways to reduce the theft. They decide to move the shelves so staff can see customers more clearly. She also hires more staff for peak times to check on theft.

- Read more [Risk management strategies \(https://www.business.gov.au/Risk-management/Risk-assessment-and-planning/Risk-management-strategies\)](https://www.business.gov.au/Risk-management/Risk-assessment-and-planning/Risk-management-strategies) for your business.

Risking opportunities

Mimi's story

Mimi, a business owner, has \$20,000 in the bank at an interest rate of 2.5%. She chooses to buy new equipment for her business to increase the efficiency of her workers. The risks of this choice include:

- missing out on a higher interest rate in the future

- the equipment doesn't increase efficiency as she expected.

Steve's story

Steve runs a clothing retail store in the shopping strip of a suburb in Perth. Most of his sales come from people walking past his shop. Recently, a new shopping centre opened about 1km from his shop. This new shopping centre decreases the number of people who pass by Steve's shop. He has to decide if he should move his business to the new shopping centre or stay where he is and increase marketing to attract new customers. He must think about the opportunities and the risks of changing location.

Steve notes the **opportunities** of changing location:

- increase in sales as more people will walk past his new store
- lower marketing expenses because of the busy location and co-marketing with other tenants.

And the **risks** of changing location:

- increase in competition from similar clothing stores within the shopping centre
- loss of regular customers and damage to business goodwill in local community.

Steve must decide if the opportunities are greater than the risks of moving to the new location. He also has to think about whether increasing his marketing budget will give him a better return on investment than moving.

Bob's story

Bob owns a takeaway restaurant. He understands the risks to his employees from hot cooking surfaces and sharp objects in the kitchen. He trains his staff to use appliances and knives safely to reduce the risk of injury. However, Bob didn't plan for the drop in sales when a new restaurant opened nearby selling similar food.

Bob had noted a common risk to his employees, but failed to plan for a less obvious risk to his business.

John's story

John runs a suburban bakery. He wants to introduce new menu items to increase revenue. Before deciding on the menu change, he does a thorough risk assessment and identifies two risks. He sees that some new menu items will contain ingredients with a short shelf life but the current supplier doesn't stock the ingredients throughout the year.

John is concerned about the risk of food poisoning due to short shelf life. He's also worried about creating unhappy customers due to the lack of new menu items.

After John discusses these concerns with his staff and suppliers, he decides not to add the new items to the menu yet and looks for other menu items he can add instead.

What to do...

- Learn what you need to consider when making a [Risk management plans](https://www.business.gov.au/Risk-management/Risk-assessment-and-planning/Risk-management-plans) (<https://www.business.gov.au/Risk-management/Risk-assessment-and-planning/Risk-management-plans>) for your business.

business.gov.au (<https://www.business.gov.au/>)

Home (<https://www.business.gov.au/>)

> **Risk management** (<https://www.business.gov.au/risk-management>) > Cyber Security

Cyber Security

Last Updated: **3 August 2018**

Cybercrime in Australia is a growing threat and is becoming an attractive way for criminals to steal information, money or disrupt business.

As the internet becomes easier to access, and we share and collect more information and data online, you need to ensure security measures are in place. For many businesses, this includes the data your business creates and stores, plus the information your customers share. Providing a secure setting is critical in building and maintaining confidence and trust in your business.

Find out your business's cyber risk - use our Cyber Security Risk Self-Assessment Tool to receive a tailored report.

What is cybercrime?

Cybercrime, also called computer crime, involves using computers and the internet to break the law. Common kinds of cybercrime include:

- identity theft and fraud
- online scams
- attacks on your computer systems or websites.

What is cyber security?

Cyber security is about protecting your technology and information from accidental or illicit access,

corruption, theft or damage. Cyber security is an ongoing journey in your business and needs to be part of your daily business processes.

What is at risk?

Your money, information, technology and reputation could be at risk from a cyber attack. This could include:

- customer records and personal information
- financial records
- business plans
- new business ideas
- marketing plans
- intellectual properties
- product design
- patent applications
- employee records.

Who could be a threat to your business?

Cyber criminals may be an individual or a group of people that cause a malicious cyber attack on your business. Cyber criminals that can threaten your technology or data could include:

- **criminals** - out for financial gain or information, to illegally access your hardware and data or disrupt your business
- **clients you do business with** – to compromise your information with malicious intent
- **business competitors** – looking to gain an advantage over your business
- **current or former employees** – who accidentally or intentionally compromise your information or data.

Types of cyber threats to your business

Cyber criminals look for information and data on your business, employees and customers. They develop a number of ways to exploit weaknesses in your business such as:

- theft or unauthorised access of hardware, computers and mobile devices
- infect computers with viruses and malware
- attack your technology or website
- attack third party systems
- spam you with emails containing viruses
- gain access to information through your employees.

For more information on the types of cyber threats that could harm your business, read our page [Identify cyber threats to your business \(https://www.business.gov.au/Risk-management/Cyber-Security/Identify-cyber-threats-to-your-business\)](https://www.business.gov.au/Risk-management/Cyber-Security/Identify-cyber-threats-to-your-business).

What effects could a cyber attack have on your business?

- **financial loss** – from theft of money, information, disruption to business
- **business loss** – damage to reputation, damage to other companies you rely on to do business
- **costs** – getting your affected systems up and running
- **investment loss** - time notifying the relevant authorities and institutions of the incident.

What can I do about protecting my business from cyber threats?

To [protect your business](#)  from cybercrime, try these tips:

- Develop clear [policies and procedures \(https://www.business.gov.au/Risk-management/Cyber-Security/Creating-a-cyber-security-policy-for-your-business\)](https://www.business.gov.au/Risk-management/Cyber-Security/Creating-a-cyber-security-policy-for-your-business) for your business and employees.

Outline the security measures you have put in place on how to protect your systems and information assets.

- Produce a [cyber security incident response management plan \(https://www.business.gov.au/Risk-management/Cyber-Security/Prepare-a-cyber-security-incident-response-management-plan\)](https://www.business.gov.au/Risk-management/Cyber-Security/Prepare-a-cyber-security-incident-response-management-plan) to support your policies and procedures.
- Train new and existing staff on your cyber security policies and procedures and the steps to take if a cyber threat or cyber incident occurs.
- Keep your computers, website and Point-of-Sale (POS) systems up-to-date with all software release updates or patches.
- Ensure you [back-up important data \(https://www.business.gov.au/Risk-management/Cyber-Security/Keep-your-business-safe-from-cyber-threats\)](https://www.business.gov.au/Risk-management/Cyber-Security/Keep-your-business-safe-from-cyber-threats) and information regularly to lessen the damage in case a breach occurs to your systems.

For more tips, read our page on [keeping your business safe from cyber threats \(https://www.business.gov.au/Risk-management/Cyber-Security/Keep-your-business-safe-from-cyber-threats\)](https://www.business.gov.au/Risk-management/Cyber-Security/Keep-your-business-safe-from-cyber-threats).

Cyber security webinars for business

Do you need help understanding the basics of cyber security for your business? Watch this five part webinar series on cyber security to help businesses understand:

- why small businesses are a target for cyber attackers
- simple steps to improve your cyber resilience
- the current cyber threat landscape and how to mitigate the risks posed by these threats
- the unique cyber security concerns of using cloud services and other outsourcing arrangements
- the support and resources available to help you with your cyber security issues and challenges.

The five part series includes:

- Cyber security for small to medium enterprises
- The cyber threat landscape for small to medium enterprises
- Cyber security operational basics
- Developing an effective incident response capability

- Cyber security in the cloud and outsourcing.

Watch the webinars [↗](#)

Note: You will need to register to view the webinars - registration is free.

These educational webinars are produced by the [Entrepreneurs' Programme](https://www.business.gov.au/Assistance/Entrepreneurs-Programme) (<https://www.business.gov.au/Assistance/Entrepreneurs-Programme>).

Find out more:

- Learn more about [Cyber threats to your business](https://www.business.gov.au/Risk-management/Cyber-Security/Identify-cyber-threats-to-your-business) (<https://www.business.gov.au/Risk-management/Cyber-Security/Identify-cyber-threats-to-your-business>), and how you can [Keep your business safe from cyber attacks](https://www.business.gov.au/Risk-management/Cyber-Security/Keep-your-business-safe-from-cyber-threats) (<https://www.business.gov.au/Risk-management/Cyber-Security/Keep-your-business-safe-from-cyber-threats>).
- Find out more about [creating a cyber security policy for your business](https://www.business.gov.au/Risk-management/Cyber-Security/Creating-a-cyber-security-policy-for-your-business) (<https://www.business.gov.au/Risk-management/Cyber-Security/Creating-a-cyber-security-policy-for-your-business>).
- Check out our tips on [preparing a cyber security incident response management plan](https://www.business.gov.au/Risk-management/Cyber-Security/Prepare-a-cyber-security-incident-response-management-plan) (<https://www.business.gov.au/Risk-management/Cyber-Security/Prepare-a-cyber-security-incident-response-management-plan>) to help you prepare for and respond to a cyber incident fast and effectively.
- Visit [Stay Smart Online](#) [↗](#) for more steps to protect your businesses safety online.
- You can sign up for cybersecurity alerts from Stay Smart Online [via Facebook](#) [↗](#), [email](mailto:StaySmartOnline@ag.gov.au) (<mailto:StaySmartOnline@ag.gov.au>) or [web](#) [↗](#). These alerts provide a range of important updates, including news about online threats and vulnerabilities.
- Download the [Cyber security guide](#) [↗](#) from the [Australian Small Business and Family Enterprise Ombudsman](#) [↗](#) website.

Enterprise Risk Management — An eye opener

Business is all about returns for the risks undertaken. However, every commercial enterprise has to cope with uncertainty. Uncertainty adds to risk but also provides an opportunity that, if properly exploited, could enhance the value of the firm and, if not addressed at the right time, could also result in erosion of value. A risk-centric business management approach advocates responding to risk and exploiting the opportunities as they arise. Such a strategy can help the business think tank identify and grow business that offer optimal risk-adjusted returns and hence maximize shareholder value.

Thus, CROs (Chief Risk Officers) seem to be on the rise advocating Enterprise Risk Management (ERM) as a solution to the increasing complexity witnessed in the global business environment; in other words, enterprise risk management is all about determining what level of risk an organization is prepared to accept as it seeks to build shareholder value.

In simple terms, the essence of ERM is to answer the question- "Am I taking the right risks as well as the right amount of risk?" ERM is characterized by a more integrated and



V Sreeraman

forward-looking approach that applies a common risk language in aligning strategy, processes, people, technology and knowledge to the evaluation and management of risks. An important aspect of ERM is the strong linkage between measures of risk and measures of overall organizational performance.



Changing scope

Traditionally, risk management in organization was limited in scope to evaluation of pure loss exposures, such as property risks, liability risks and personnel risks. This was addressed by way of entering into relevant contracts with insurers. In the 1990s, as many businesses began to expand, the scope of risk manage-

A risk is a risk - it affects earnings potential, whether it comes from fluctuations in commodity price, (equipment) fire, change in legislation, or adverse media coverage. Ultimately, how you parcel your risks is how you see your company's core mission and the reason investors invest in you - to that extent, knowing your risks is knowing yourself.

ment had to widen to look into speculative financial risks. This led to the birth of Financial Risk Management that began to address commodity price risk, interest rate risk and currency exchange rate risk.

Encouraged by the success of financial risk management, some organizations are taking the next logical step, to address comprehensively organization's pure risks, speculative risks, strategic and operational risks.

This approach has come to be regarded as Enterprise risk management. At the heart of this approach is the desire to increase shareholder value.

Why ERM?

Traditionally, organizations used to adopt "managing risks by silos"

The author is member of the Institute. He can be reached at sreeraman@rediffmail.com

approach. This was based on the belief that different types of risks are the responsibility of various corporate and business units. However, the last decade has witnessed financial disasters of severe levels occurring on a regular basis resulting in collapse of organizations once considered as "well managed".

The collapse of Barings Bank was an eye opener in revisiting the belief aforementioned. Also, with factors such as globalization, technology, regulation, restructurings, changing markets, and competition (both within the local markets as well as from across the borders) creating uncertainty, there seems to be a paradigm shift in the way the organizations think about management of risks. Organizations have come to accept that in an extremely competitive environment, crisis management or contingency planning would never help; it is embarrassing, time consuming and expensive. Crisis management can at the most protect oneself against the downside but could not guide towards improvement of the business performance. Contingency planning might help one to be flexible enough to follow an alternate plan to counter the unforeseen surprises in the chosen plan, primarily with a view to curtail the negative implications. To put it in layman's words, both these might help us avoid pitfalls and surprises on the way but may not enable us to reach the destination targeted. Rather, given that uncertainties have to be accepted, preparing oneself to understand them and prepare accordingly seems to be key to success.

Mark Haynes Daniell, in his book, "World of Risk - Next Generation Strategy for a volatile era", lists down "ten sets of recurring

How to define ERM

The Committee of Sponsoring Organizations of the Treadway Commission defines Enterprise risk management as -

"A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives".

This definition underlines the following -

- (a) ERM is a process, i.e. it means to an end and not an end in itself.
- (b) ERM involves people at all levels and is not just policies and forms provided by few at the top.
- (c) ERM is closely related to the organizational strategy and thus is influenced by vision and mission.
- (d) ERM is applied across all units of the business by adopting a portfolio view of the various risks influencing them.
- (e) ERM tries to identify events that potentially affect the performance and works out a plan to manage the same based upon the risk appetite.
- (f) ERM provides reasonable assurance to the Board of Directors on the efficacy and effectivity of all business operations.
- (g) ERM is oriented towards achievement of organizational objectives by addressing different components of risks in separate but overlapping categories.

patterns". He suggests that an understanding of these elements is a fundamental requisite for meeting the strategic challenges of contemporary business environments. These are:

1. **Globalisation** which redefines many of the major sources of risk and opportunity that we face today

2. **Complexity** of the dynamic global system that is increasingly rapidly every day.

3. **Turbulence** creating or reflecting greater than average discontinuity in a system.

4. **Dynamism** forcing the organizations to understand, anticipate, influence and take advantage of the inevitable movements and changes.

5. **Acceleration** in the pace of change in virtually every global system.

6. **Continuous** Obsolescence and Reinvention driving home the point that traditional models of business management are no more useful.

7. **Connectivity** leading to a new state of business dependence on technology.

8. **Convergence** by way of two non-identical systems moving towards a common end point or pattern without merging or fully consolidating into one entity.

9. **Consolidation** of subsystems and formerly independent entities into a larger unified block.

10. **Rationalization** whereby overtime, systems tend towards a more efficient relation of means to ends.

Considering the emerging phenomenon listed above, it is imperative that organizations have in place a process that continuously monitors the impact of various risk factors influencing the organizational performance. This is where ERM is considered to be a significant contributor.

ERM analyzes and measures the integrated effects of risks on

strategic objectives, including finances and cash flows. By aggregating risks, an organization can identify risk concentrations as well as offsetting risk patterns. This approach leads to superior resource allocation decisions because they are based on the risk-return characteristics of the organization's entire risk portfolio as opposed to those of its individual risk "silos."

Emergence of ERM

The collapse of mega companies, accounting scandals, market volatility, litigation and terrorism present a vast range of threats and risks. In this scenario, the top managements have come to clearly understand that earnings can no more be managed only by the accountants but more by identifying the earnings drivers and proactively managing them. Study of literature clearly reveals that ERM as a concept has emerged as a result of internal demand and external developments. Advances in risk management tools and methodologies have also aided the growth of this body of knowledge. **ERM differs from TQM in that the latter tolerates no failures.**

ERM preaches that a defined number of failures can be tolerated if the organization is convinced that the cost of guarding against them is more expensive than the risks they impose.

Internal demand

With increase in accounting irregularities coming to limelight, resulting in sudden death of large organizations, the shareholders across the world have started demanding more transparency in the way the business is managed.

The frequency of reporting has

The fall of the Barings Bank

Barings Bank had a long successful history in the U.K. economy. In February 1995, this reputed bank, with a capital of \$900 million, had to face bankruptcy. The reason was \$1 billion of unauthorized trading losses caused by Nick Leeson, who has come to be regarded as the rogue trader. Nick Leeson was able to conceal his unauthorized trading activities for over a year because he managed both the trading and back-office functions. In simple terms, this meant that he had the authority to execute, settle and account for all trading activities in his business. Leeson went for a trading strategy called "straddle" (meant for making a profit by selling put and call options on the same underlying financial instrument) with respect to Nikkei 225 index. Such a strategy is expected to produce profits when markets are stable but would result in substantial losses if the markets turn volatile. When an earthquake in Japan caused a steep drop in the Nikkei index, Lesson suffered losses. To cover up minor losses caused due to a clerical error, Lesson began trading open positions that led to mounting of huge losses. The bubble burst and the losses were uncovered. In March 1995, The Dutch Bank ING purchased Barings Bank, closing out the history of a 223 year old institution which had an excellent existence including the helping of USA by way of financing the Louisiana Purchase.



increased as well as the details provided. Post Enron, the role of people managing strategic issues have come under extensive scrutiny. "Corporate Governance" is one of the latest buzz words doing the rounds in major corporate entities.

Consequently, the people who manage the business would like to carry out a scientific analysis of all risk factors that would influence the results both in the short and in the long run before committing anything to the stakeholders.

External development

Development in e-business, Changes in regulations, say, reporting of quarterly earnings/segment reports, availability of risk transfer products like credit derivatives, catastrophe bonds allowing the option to retain

the risk as well as to hedge are all pointers to the fact that risks have come to be accepted but require careful analysis. Derivatives, insurance and hybrid products are available at the disposal of management to reduce undesirable risks, but these carry a cost. Therefore, an integrated approach to perceiving the impact of different risks at an organizational level is essential before a decision to challenge the risk is taken.

ERM addresses following queries-

- What risks am I facing, and how do they compare to those of my peers ?
- Do I understand inter-relationship of different risks?
- How are these risks changing based on changes in my business environment?

- What level of risk should I take?
- How should I manage those risks?
- Do I know who our risk owners are? Do they have systems in place for measuring and monitoring risk?

Traditional approach and Enterprise Risk Management

Traditionally, functional, divisional or departmental barriers guided the approach to managing risks. In a multi product corporation, independent business units addressed the business risks associated with their overall strategy and profitability, such as those related to products, pricing and relationship management. Collection of overdue debt and handling of bad debts was considered the responsibility of the marketing executives while abnormal increase in interest cost much more than the budgeted levels was taken to be the effect of treasurer's action. The quality department had to bother about the defectives and finance department had to look into the optimal level of insurance covers as if it just involved the principle of minimizing the costs. Such a strategy did not work, simply because, risks are highly interdependent and cannot be segmented and managed solely by independent units. For instance, by outsourcing a non-core function to mitigate performance risk, an organization assumes credit and supply-chain risks. Moreover, such an approach would not provide the strategic management team with a consolidated report that displays the "total risk" the enterprise is subject to. The objective is to move from "Risk is not my responsibility" mindset to "Risk in everyone's

"Risks are highly interdependent and cannot be segmented and managed solely by independent units. The objective should be to move from "Risk is not my responsibility" mindset to "Risk in everyone's responsibility"

responsibility".

Traditional focus was on risk mitigation (using controls to limit exposures to problems) while the trend is towards risk portfolio optimization (finding a fit between the risk appetite and opportunities with a view to capitalize on the rewards that would arise).



Types of risk

Several bases of classification of risk are reported in literature. Based on these, we could classify the types of risk as follows -

1. *Credit risks* - lending and counterparty exposures
2. *Market risks* - Interest rate, foreign exchange, equity and commodity exposures
3. *Business risks* - Volatility in volumes, margins or costs
4. *Operational risks* - Day-to-day processing errors to fraud
5. *Strategic risks* - Environmental influences that prevent the organizations from meeting the business objectives
6. *Reputation risk* - Damage to brand and corporate image

7. *Regulatory or contractual risk*

8. *Financial risk* - Unreasonable liabilities to support day-to-day operating activities

9. *Information risk* - Unreliable, irrelevant information and also untimely in addition to inadequate security systems

10. *New risks* - New competitors or emerging business models, recession risks, outsourcing risks, political risks and the like

ERM looks at all these risks in the light of interdependencies amongst them as well as the probability of occurrence against the implications on performance.

ERM Process

As a process, ERM is composed of eight interrelated components.

1) Internal environment - defined in terms of ethical values, personnel (competencies and capabilities, in addition to attitudes and beliefs), management's operating style and culture, apart from the most significant of all - risk appetite.

2) Objective setting - with reference to four major perspectives, viz., strategic, operations, reporting and compliance, after finalizing the views on risk appetite and risk tolerance.

3) Event identification - for the purposes of assessing risk through an understanding of the interrelationships between events, by aggregating them horizontally

across an entity and vertically within operating units.

4) Risk assessment - involving evaluation of both the likelihood and impact of potential events and their effects on the objectives using qualitative and quantitative methods.

5. Risk response - dealing with selection of a strategy that consider both the risk appetite and costs vs. benefits and normally falls under one of the four categories, viz., avoidance, sharing, reduction and acceptance

6. Control activities - concerned with laying down policies and procedures to ensure that risk responses are carried out efficiently and encompass IT infrastructure and management, security management and software (general controls) as well as ensuring completeness, accuracy and validity of data capture and processing (application controls)

7) Information and Communication - suggesting the significance of capturing and sharing relevant information from both internal and external sources in a form and time-frame that would enable timely, efficient and effective reaction in addition to exchange of relevant data with external parties such as customers, vendors, regulators and shareholders.

8) Monitoring - Both on an ongoing basis and via one-time evaluation to see to it that the process is applied at all levels.

ERM and Portfolio effect

The concept of active portfolio management can be applied to all the risks within an organization. If the different risks the organization is subject to can be viewed as a portfolio, then diversification effects from natural hedges could be fully exploited. For this, the strategic

management should consider themselves as fund managers, setting portfolio targets and risk limits to ensure appropriate diversification and optimal portfolio returns.

There is another issue worth considering. The bad things do not occur in concert. The different devastating effects, say, earthquake,



The strategic management should consider themselves as fund managers, setting portfolio targets and risk limits to ensure appropriate diversification and optimal portfolio returns.

serious power failure, competitive threats, supply chain disruptions, financial market volatility, management malfeasance, etc. do not tend to affect the earnings potential and hence the performance in the same fiscal period. In other words, these events are not perfectly correlated. There might be an element of negative correlation built into the relationship amongst these elements. For instance, when rupee value falls against major foreign currencies, raw material imports may prove costlier but sales revenue registers growth due to surge in export business. Therefore, there is the need to have a holistic view of the risks influencing the organization, thereby focusing one's atten-

tion on the independence and interdependence of the risks to unravel the "natural hedge" among some of their effects. This is where there is a lesson drawn from the Modern Portfolio Theory. This theory clearly advocates that what matters is not the risk of the individual investment but the risk of the entire portfolio. Therefore, by diversifying the effects of risks that are not perfectly correlated, the organization can achieve optimal results.

The first step in implementing an Enterprise Risk Management process would involve detailed discussions with various heads of the departments. This is done to get an insight into different risks as perceived at a departmental level.

After sharing information on the different strategic, financial, operations and hazard risks facing the company, the next step is to pick those risks that would benefit from a portfolio approach.

The key is to select those risks that are least correlated. All the risks are mathematically reduced to a common denominator, called a unit of risk, which permits comparison with each other. The exercise helps determine the most advantageous portfolio of risk to take to market.

ERM practices at Rolls-Royce

At Rolls Royce, it was found that the finance manual that explains their financial policies and authorization requirements for obtaining project funding needed amendment. A project could be anything from launching a new aero-engine or installing an industrial engine in a power project to relocating a business from one country to another. The finance manual explained how to compile a business case for a project, explaining the forms to be sub-

RISK MANAGEMENT

mitted for authorization and asking for extensive information about financial variables.

However, it was noticed that nowhere it asked for a qualitative or quantitative assessment of potential risks and what effect they might have on outcomes. The consequence was that resources were not allocated to areas based on marketing data and similar analyses but not based on risk data leading to sub optimal returns and substantial time and money was wasted on activities like drafting agreements that is not significant when ana-

lyzed from a risk perspective. It was therefore decided that when someone proposes a project, they must attach a "risk register" that analyzes the key risks and their potential consequences.

Conclusion

No business entity operates in a risk free environment. ERM does not attempt to create one such environment. Rather, it empowers the management to operate more effectively in environments filled with risks. It provides enhanced capability to

1. Align risk appetite and strategy

2. Link growth, risk and return
3. Enhance risk response decisions
4. Minimize operational surprises and losses
5. Identify and manage cross-enterprise risks
6. Provide integrated responses to multiple risks
7. Seize the opportunities
8. Rationalize the capital

ERM is a process that is not limited to one event or circumstance. It is a dynamic process that unfolds over time and permeates every aspect of an organization's resources and operations. ■

CAMPUS INTERVIEWS: February, 2005

The Committee for Members in Industry of the Institute organises Campus Interviews for newly qualified Chartered Accountants at various centres. The scheme has been evolved to provide an opportunity both to employing organisations as well as the young professional aspirants to meet and explore the possibility of taking up positions in Industry. In the last such interviews conducted in September-October, 2004 at various centres, 99 recruiting teams of leading companies of the country reviewed the bio-data of more than 3369 young chartered accountants and interviewed those shortlisted by them in the premises of the offices of the Institute.

INVITATION TO CANDIDATES QUALIFYING IN CA FINAL November 2004 EXAM

It has been decided to organise Campus Interviews at ten centres, viz., **Kolkata, Mumbai Chennai, New Delhi, Bangalore, Hyderabad, Coimbatore, Ahmedabad, Pune and Jaipur** in February, 2005. As earlier, a large number of leading companies are expected to participate. The schedule of interviews is as below:-

- | | |
|---|---|
| 1. Coimbatore, Pune and Jaipur | The Campus Interviews will be held concurrently at these Centres from 14th to 15th February 2005 |
| 2. Bangalore, Hyderabad and Ahmedabad | The Campus Interviews will be held concurrently at these Centres from 16th to 18th February 2005 |
| 3. Kolkata, Mumbai, Chennai, New Delhi | The Campus Interviews will be held concurrently at these Centres from 21st to 28th February 2005 (excluding Sunday) |

The Candidates who qualify in the final examination held in November 2004 and are interested to appear in these interviews may, immediately on declaration of the result, access the Institute's On-line Placement Portal at www.placements-icai.org and fill up the Application Form Online.

INVITATION TO EMPLOYERS

The Committee for Members in Industry of the Institute provides opportunity to the employers to have a look at freshly qualified Chartered Accountants and makes all arrangements at its centres. Thereby it obviates the necessity to incur high recruitment cost and provides a cost effective mode of recruiting young Chartered Accountants.

Companies intending to recruit freshly qualified Chartered Accountants through the scheme of Campus Interviews are invited to write to Shri Surinder Pal, Secretary, Committee for Members in Industry at the Institute's Head Office at Indraprastha Marg, New Delhi or they can contact him (Tel. No.23378310, 23370055-Extn. 439/450; Email:spal@icai.org) or Shri N.K. Bansal, Executive Officer on the same telephone numbers for the details of the scheme. The Companies can also register themselves on the On-line Placement Portal at 'www.placements-icai.org' A Company can participate in one or more centres, as per its requirements. Firms of Chartered Accountants are also welcome to join. Committee for Members in Industry.

Committee for Members in Industry

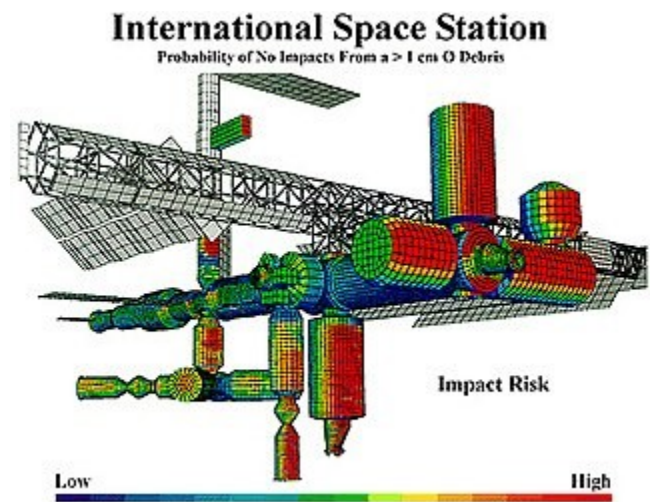
Risk management

Risk management is the identification, evaluation, and prioritization of risks (defined in ISO 31000 as *the effect of uncertainty on objectives*) followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events^[1] or to maximize the realization of opportunities.

Risks can come from various sources including uncertainty in financial markets, threats from project failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or events of uncertain or unpredictable root-cause. There are two types of events i.e. negative events can be classified as risks while positive events are classified as opportunities. Several risk management standards have been developed including the Project Management Institute, the National Institute of Standards and Technology, actuarial societies, and ISO standards.^{[2][3]} Methods, definitions and goals vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety.

Strategies to manage threats (uncertainties with negative consequences) typically include avoiding the threat, reducing the negative effect or probability of the threat, transferring all or part of the threat to another party, and even retaining some or all of the potential or actual consequences of a particular threat, and the opposites for opportunities (uncertain future states with benefits).

Certain aspects of many of the risk management standards have come under criticism for having no measurable improvement on risk; whereas the confidence in estimates and decisions seem to increase.^[1] For example, one study found that one in six IT projects were "black swans" with gigantic overruns (cost overruns averaged 200%, and schedule overruns 70%).^[4]



Example of risk assessment: A NASA model showing areas at high risk from impact for the International Space Station

Contents

Introduction

- Method
- Principles

Process

- Establishing the context
- Identification

Assessment

Risk options

- Potential risk treatments
- Risk management plan
- Implementation
- Review and evaluation of the plan

Limitations**Areas**

- Enterprise
- Enterprise Security
- Medical device
- Project management
- Megaprojects (infrastructure)
- Natural disasters
- Wilderness
- Information technology
- Petroleum and natural gas
- Pharmaceutical sector

Risk communication**See also****References****External links**

Introduction

A widely used vocabulary for risk management is defined by *ISO Guide 73:2009*, "Risk management. Vocabulary."^[2]

In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss (or impact) and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order. In practice the process of assessing overall risk can be difficult, and balancing resources used to mitigate between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

Intangible risk management identifies a new type of a risk that has a 100% probability of occurring but is ignored by the organization due to a lack of identification ability. For example, when deficient knowledge is applied to a situation, a knowledge risk materializes. Relationship risk appears when ineffective collaboration occurs. Process-engagement risk may be an issue when ineffective operational procedures are applied. These risks directly reduce the productivity of knowledge workers, decrease cost-effectiveness, profitability, service, quality, reputation, brand value, and earnings quality. Intangible risk management allows risk management to create immediate value from the identification and reduction of risks that reduce productivity.

Risk management also faces difficulties in allocating resources. This is the idea of opportunity cost. Resources spent on risk management could have been spent on more profitable activities. Again, ideal risk management minimizes spending (or manpower or other resources) and also minimizes the negative effects of risks.

According to the definition to the risk, the risk is the possibility that an event will occur and adversely affect the

achievement of an objective. Therefore, risk itself has the uncertainty. Risk management such as COSO ERM, can help managers have a good control for their risk. Each company may have different internal control components, which leads to different outcomes. For example, the framework for ERM components includes Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control Activities, Information and Communication, and Monitoring.

Method

For the most part, these methods consist of the following elements, performed, more or less, in the following order.

1. identify the threats
2. assess the vulnerability of critical assets to specific threats
3. determine the risk (i.e. the expected likelihood and consequences of specific types of attacks on specific assets)
4. identify ways to reduce those risks
5. prioritize risk reduction measures

Principles

The International Organization for Standardization (ISO) identifies the following principles of risk management:^[5]

Risk management should:

- create value – resources expended to mitigate risk should be less than the consequence of inaction
- be an integral part of organizational processes
- be part of decision making process
- explicitly address uncertainty and assumptions
- be a systematic and structured process
- be based on the best available information
- be tailorable
- take human factors into account
- be transparent and inclusive
- be dynamic, iterative and responsive to change
- be capable of continual improvement and enhancement
- be continually or periodically re-assessed

Process

According to the standard ISO 31000 "Risk management – Principles and guidelines on implementation,"^[3] the process of risk management consists of several steps as follows:

Establishing the context

This involves:

1.
 - the social scope of risk management
 - the identity and objectives of stakeholders
 - the basis upon which risks will be evaluated, constraints.
2. defining a framework for the activity and an agenda for identification

3. developing an analysis of risks involved in the process
4. mitigation or solution of risks using available technological, human and organizational resources

Identification

After establishing the context, the next step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, cause problems or benefits. Hence, risk identification can start with the source of our problems and those of our competitors (benefit), or with the problem consequences.

- Source analysis^[6] – Risk sources may be internal or external to the system that is the target of risk management (use mitigation instead of management since by its own definition risk deals with factors of decision-making that cannot be managed).

Examples of risk sources are: stakeholders of a project, employees of a company or the weather over an airport.

- Problem analysis – Risks are related to identified threats. For example: the threat of losing money, the threat of abuse of confidential information or the threat of human errors, accidents and casualties. The threats may exist with various entities, most important with shareholders, customers and legislative bodies such as the government.

When either source or problem is known, the events that a source may trigger or the events that can lead to a problem can be investigated. For example: stakeholders withdrawing during a project may endanger funding of the project; confidential information may be stolen by employees even within a closed network; lightning striking an aircraft during takeoff may make all people on board immediate casualties.

The chosen method of identifying risks may depend on culture, industry practice and compliance. The identification methods are formed by templates or the development of templates for identifying source, problem or event. Common risk identification methods are:

- Objectives-based risk identification – Organizations and project teams have objectives. Any event that may endanger achieving an objective partly or completely is identified as risk.
- Scenario-based risk identification – In [scenario analysis](#) different scenarios are created. The scenarios may be the alternative ways to achieve an objective, or an analysis of the interaction of forces in, for example, a market or battle. Any event that triggers an undesired scenario alternative is identified as risk – see [Futures Studies](#) for methodology used by [Futurists](#).
- Taxonomy-based risk identification – The taxonomy in taxonomy-based risk identification is a breakdown of possible risk sources. Based on the taxonomy and knowledge of best practices, a questionnaire is compiled. The answers to the questions reveal risks.^[7]
- Common-risk checking^[8] – In several industries, lists with known risks are available. Each risk in the list can be checked for application to a particular situation.^[9]
- Risk charting^[10] – This method combines the above approaches by listing resources at risk, threats to those resources, modifying factors which may increase or decrease the risk and consequences it is wished to avoid. Creating a matrix under these headings enables a variety of approaches. One can begin with resources and consider the threats they are exposed to and the consequences of each. Alternatively one can start with the threats and examine which resources they would affect, or one can begin with the consequences and determine which combination of threats and resources would be involved to bring them about.

Assessment

Once risks have been identified, they must then be assessed as to their potential severity of impact (generally a negative impact, such as damage or loss) and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of an unlikely event, the probability of occurrence of which is unknown. Therefore, in the assessment process it is critical to make the best educated decisions in order to properly prioritize the implementation of the [risk management plan](#).

Even a short-term positive improvement can have long-term negative impacts. Take the "turnpike" example. A highway is widened to allow more traffic. More traffic capacity leads to greater development in the areas surrounding the improved traffic capacity. Over time, traffic thereby increases to fill available capacity. Turnpikes thereby need to be expanded in a seemingly endless cycles. There are many other engineering examples where expanded capacity (to do any function) is soon filled by increased demand. Since expansion comes at a cost, the resulting growth could become unsustainable without forecasting and management.

The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents and is particularly scanty in the case of catastrophic events, simply because of their infrequency. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for intangible assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for senior executives of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized within overall company goals. Thus, there have been several theories and attempts to quantify risks. Numerous different risk formulae exist, but perhaps the most widely accepted formula for risk quantification is: "Rate (or probability) of occurrence multiplied by the impact of the event equals risk magnitude."

Risk options

Risk mitigation measures are usually formulated according to one or more of the following major risk options, which are:

1. Design a new business process with adequate built-in risk control and containment measures from the start.
2. Periodically re-assess risks that are accepted in ongoing processes as a normal feature of business operations and modify mitigation measures.
3. Transfer risks to an external agency (e.g. an insurance company)
4. Avoid risks altogether (e.g. by closing down a particular high-risk business area)

Later research^[11] has shown that the financial benefits of risk management are less dependent on the formula used but are more dependent on the frequency and how risk assessment is performed.

In business it is imperative to be able to present the findings of risk assessments in financial, market, or schedule terms. Robert Courtney Jr. (IBM, 1970) proposed a formula for presenting risks in financial terms. The Courtney formula was accepted as the official risk analysis method for the US governmental agencies. The formula proposes calculation of ALE (annualized loss expectancy) and compares the expected loss value to the security control implementation costs (cost-benefit analysis).

Potential risk treatments

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:^[12]

- Avoidance (eliminate, withdraw from or not become involved)
- Reduction (optimize – mitigate)
- Sharing (transfer – outsource or insure)
- Retention (accept and budget)

Ideal use of these risk control strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organization or person making the risk management decisions. Another source, from the US

Department of Defense (see link), [Defense Acquisition University](#), calls these categories ACAT, for Avoid, Control, Accept, or Transfer. This use of the ACAT acronym is reminiscent of another ACAT (for Acquisition Category) used in US Defense industry procurements, in which Risk Management figures prominently in decision making and planning.

Risk avoidance

This includes not performing an activity that could carry risk. An example would be not buying a [property](#) or business in order to not take on the [legal liability](#) that comes with it. Another would be not flying in order not to take the risk that the [airplane](#) were to be [hijacked](#). Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits. Increasing risk regulation in hospitals has led to avoidance of treating higher risk conditions, in favor of patients presenting with lower risk.^[13]

Risk reduction

Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. For example, [sprinklers](#) are designed to put out a [fire](#) to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable. [Halon](#) fire suppression systems may mitigate that risk, but the cost may be prohibitive as a [strategy](#).

Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied. By an offshore drilling contractor effectively applying [Health, Safety and Environment](#) (HSE) management in its organization, it can optimize risk to achieve levels of [residual risk](#) that are tolerable.^[14]

Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project. By developing in iterations, software projects can limit effort wasted to a single iteration.

[Outsourcing](#) could be an example of risk sharing strategy if the outsourcer can demonstrate higher capability at managing or reducing risks.^[15] For example, a company may outsource only its software development, the manufacturing of hard goods, or customer support needs to another company, while handling the business management itself. This way, the company can concentrate more on business development without having to worry as much about the manufacturing process, managing the development team, or finding a physical location for a center.

Risk sharing

Briefly defined as "sharing with another party the burden of loss or the benefit of gain, from a risk, and the measures to reduce a risk."

The term of 'risk transfer' is often used in place of risk sharing in the mistaken belief that you can transfer a risk to a third party through insurance or outsourcing. In practice if the insurance company or contractor go bankrupt or end up in court, the original risk is likely to still revert to the first party. As such in the terminology of practitioners and scholars alike, the purchase of an insurance contract is often described as a "transfer of risk." However, technically speaking, the buyer of the contract generally retains legal responsibility for the losses "transferred", meaning that insurance may be described more accurately as a post-event compensatory mechanism. For example, a personal

injuries insurance policy does not transfer the risk of a car accident to the insurance company. The risk still lies with the policy holder namely the person who has been in the accident. The insurance policy simply provides that if an accident (the event) occurs involving the policy holder then some compensation may be payable to the policy holder that is commensurate with the suffering/damage.

Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is different from traditional insurance, in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

Risk retention

Risk retention involves accepting the loss, or benefit of gain, from a risk when the incident occurs. True self-insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that either they cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed to war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great that it would hinder the goals of the organization too much.

Risk management plan

Select appropriate controls or countermeasures to mitigate each risk. Risk mitigation needs to be approved by the appropriate level of management. For instance, a risk concerning the image of the organization should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks.

The risk management plan should propose applicable and effective security controls for managing the risks. For example, an observed high risk of computer viruses could be mitigated by acquiring and implementing antivirus software. A good risk management plan should contain a schedule for control implementation and responsible persons for those actions.

According to ISO/IEC 27001, the stage immediately after completion of the risk assessment phase consists of preparing a Risk Treatment Plan, which should document the decisions about how each of the identified risks should be handled. Mitigation of risks often means selection of security controls, which should be documented in a Statement of Applicability, which identifies which particular control objectives and controls from the standard have been selected, and why.

Implementation

Implementation follows all of the planned methods for mitigating the effect of the risks. Purchase insurance policies for the risks that it has been decided to transferred to an insurer, avoid all risks that can be avoided without sacrificing the entity's goals, reduce others, and retain the rest.

Review and evaluation of the plan

Initial risk management plans will never be perfect. Practice, experience, and actual loss results will necessitate changes in the plan and contribute information to allow possible different decisions to be made in dealing with the risks being faced.

Risk analysis results and management plans should be updated periodically. There are two primary reasons for this:

1. to evaluate whether the previously selected security controls are still applicable and effective
2. to evaluate the possible risk level changes in the business environment. For example, information risks are a good example of rapidly changing business environment.

Limitations

Prioritizing the *risk management processes* too highly could keep an organization from ever completing a project or even getting started. This is especially true if other work is suspended until the risk management process is considered complete.

It is also important to keep in mind the distinction between risk and uncertainty. Risk can be measured by impacts × probability.

If risks are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur. Spending too much time assessing and managing unlikely risks can divert resources that could be used more profitably. Unlikely events do occur but if the risk is unlikely enough to occur it may be better to simply retain the risk and deal with the result if the loss does in fact occur. Qualitative risk assessment is subjective and lacks consistency. The primary justification for a formal risk assessment process is legal and bureaucratic.

Areas

As applied to corporate finance, *risk management* is the technique for measuring, monitoring and controlling the financial or operational risk on a firm's balance sheet, a traditional measure is the value at risk (VaR), but there also other measures like profit at risk (PaR) or margin at risk. The Basel II framework breaks risks into market risk (price risk), credit risk and operational risk and also specifies methods for calculating capital requirements for each of these components.

In Information Technology, Risk management includes "Incident Handling", an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. According to the SANS Institute,^[16] it is a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Enterprise

In enterprise risk management, a risk is defined as a possible event or circumstance that can have negative influences on the enterprise in question. Its impact can be on the very existence, the resources (human and capital), the products and services, or the customers of the enterprise, as well as external impacts on society, markets, or the environment. In a financial institution, enterprise risk management is normally thought of as the combination of credit risk, interest rate risk or asset liability management, liquidity risk, market risk, and operational risk.

In the more general case, every probable risk can have a pre-formulated plan to deal with its possible consequences (to ensure *contingency* if the risk becomes a *liability*).

From the information above and the average cost per employee over time, or cost accrual ratio, a project manager can estimate:

- the cost associated with the risk if it arises, estimated by multiplying employee costs per unit time by the estimated time lost (*cost impact*, C where $C = \text{cost accrual ratio} * S$).
- the probable increase in time associated with a risk (*schedule variance due to risk*, R_s where $R_s = P * S$):
 - Sorting on this value puts the highest risks to the schedule first. This is intended to cause the greatest risks to the project to be attempted first so that risk is minimized as quickly as possible.
 - This is slightly misleading as *schedule variances* with a large P and small S and vice versa are not equivalent. (The risk of the RMS Titanic sinking vs. the passengers' meals being served at slightly the wrong time).
- the probable increase in cost associated with a risk (*cost variance due to risk*, R_c where $R_c = P * C = P * \text{CAR} * S = P * S * \text{CAR}$)
 - sorting on this value puts the highest risks to the budget first.
 - see concerns about *schedule variance* as this is a function of it, as illustrated in the equation above.

Risk in a project or process can be due either to Special Cause Variation or Common Cause Variation and requires appropriate treatment. That is to re-iterate the concern about extremal cases not being equivalent in the list immediately above.

Enterprise Security

ESRM is a security program management approach that links security activities to an enterprise's mission and business goals through risk management methods. The security leader's role in ESRM is to manage risks of harm to enterprise assets in partnership with the business leaders whose assets are exposed to those risks. ESRM involves educating business leaders on the realistic impacts of identified risks, presenting potential strategies to mitigate those impacts, then enacting the option chosen by the business in line with accepted levels of business risk tolerance^[17]

Medical device

For medical devices, risk management is a process for identifying, evaluating and mitigating risks associated with harm to people and damage to property or the environment. Risk management is an integral part of medical device design and development, production processes and evaluation of field experience, and is applicable to all types of medical devices. The evidence of its application is required by most regulatory bodies such as the US FDA. The management of risks for medical devices is described by the International Organization for Standardization (ISO) in ISO 14971:2007, Medical Devices—The application of risk management to medical devices, a product safety standard. The standard provides a process framework and associated requirements for management responsibilities, risk analysis and evaluation, risk controls and lifecycle risk management.

The European version of the risk management standard was updated in 2009 and again in 2012 to refer to the Medical Devices Directive (MDD) and Active Implantable Medical Device Directive (AIMDD) revision in 2007, as well as the In Vitro Medical Device Directive (IVDD). The requirements of EN 14971:2012 are nearly identical to ISO 14971:2007. The differences include three "(informative)" Z Annexes that refer to the new MDD, AIMDD, and IVDD. These annexes indicate content deviations that include the requirement for risks to be reduced *as far as possible*, and the requirement that risks be mitigated by design and not by labeling on the medical device (i.e., labeling can no longer be used to mitigate risk).

Typical risk analysis and evaluation techniques adopted by the medical device industry include hazard analysis, fault

tree analysis (FTA), failure mode and effects analysis (FMEA), hazard and operability study (HAZOP), and risk traceability analysis for ensuring risk controls are implemented and effective (i.e. tracking risks identified to product requirements, design specifications, verification and validation results etc.). FTA analysis requires diagramming software. FMEA analysis can be done using a spreadsheet program. There are also integrated medical device risk management solutions.

Through a draft guidance (<http://www.fda.gov/medicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm206153.htm>), the FDA has introduced another method named "Safety Assurance Case" for medical device safety assurance analysis. The safety assurance case is structured argument reasoning about systems appropriate for scientists and engineers, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment. With the guidance, a safety assurance case is expected for safety critical devices (e.g. infusion devices) as part of the pre-market clearance submission, e.g. 510(k). In 2013, the FDA introduced another draft guidance expecting medical device manufacturers to submit cybersecurity risk analysis information.

Project management

Project risk management must be considered at the different phases of acquisition. In the beginning of a project, the advancement of technical developments, or threats presented by a competitor's projects, may cause a risk or threat assessment and subsequent evaluation of alternatives (see Analysis of Alternatives). Once a decision is made, and the project begun, more familiar project management applications can be used:^{[18][19][20]}

- Planning how risk will be managed in the particular project. Plans should include risk management tasks, responsibilities, activities and budget.
- Assigning a risk officer – a team member other than a project manager who is responsible for foreseeing potential project problems. Typical characteristic of risk officer is a healthy skepticism.
- Maintaining live project risk database. Each risk should have the following attributes: opening date, title, short description, probability and importance. Optionally a risk may have an assigned person responsible for its resolution and a date by which the risk must be resolved.
- Creating anonymous risk reporting channel. Each team member should have the possibility to report risks that he/she foresees in the project.
- Preparing mitigation plans for risks that are chosen to be mitigated. The purpose of the mitigation plan is to describe how this particular risk will be handled – what, when, by whom and how will it be done to avoid it or minimize consequences if it becomes a liability.
- Summarizing planned and faced risks, effectiveness of mitigation activities, and effort spent for the risk management.

ID	Description	Category	Status	Risk Rating
1	Identify risks	Identify	Identify	Identify
2	Analyze risks	Analyze	Analyze	Analyze
3	Plan response	Plan	Plan	Plan
4	Monitor and control	Monitor	Monitor	Monitor

An example of the Risk Register for a project that includes 4 steps: Identify, Analyze, Plan Response, Monitor and Control.^[21]

Megaprojects (infrastructure)

Megaprojects (sometimes also called "major programs") are large-scale investment projects, typically costing more than \$1 billion per project. Megaprojects include major bridges, tunnels, highways, railways, airports, seaports, power plants, dams, wastewater projects, coastal flood protection schemes, oil and natural gas extraction projects, public buildings, information technology systems, aerospace projects, and defense systems. Megaprojects have been shown to be particularly risky in terms of finance, safety, and social and environmental impacts.^[22] Risk management is therefore particularly pertinent for megaprojects and special methods and special education have been developed for

such risk management.^[23]

Natural disasters

It is important to assess risk in regard to natural disasters like floods, earthquakes, and so on. Outcomes of natural disaster risk assessment are valuable when considering future repair costs, business interruption losses and other downtime, effects on the environment, insurance costs, and the proposed costs of reducing the risk.^{[24][25]} The Sendai Framework for Disaster Risk Reduction is a 2015 international accord that has set goals and targets for disaster risk reduction in response to natural disasters.^[26] There are regular International Disaster and Risk Conferences in Davos to deal with integral risk management.

Wilderness

The management of risks to persons and property in wilderness and remote natural areas has developed with increases in outdoor recreation participation and decreased social tolerance for loss. Organizations providing commercial wilderness experiences can now align with national and international consensus standards for training and equipment such as ANSI/NASBLA 101-2017 (boating),^[27] UIAA 152 (ice climbing tools),^[28] and European Norm 13089:2015 + A1:2015 (mountaineering equipment).^{[29][30]} The Association for Experiential Education offers accreditation for wilderness adventure programs.^[31] The Wilderness Risk Management Conference provides access to best practices, and specialist organizations provide wilderness risk management consulting and training.^{[32][33][34][35]}

In his book, *Outdoor Leadership and Education*, climber, outdoor educator, and author, Ari Schneider, notes that outdoor recreation is inherently risky, and there is no way to completely eliminate risk. However, he explains how that can be a good thing for outdoor education programs. According to Schneider, optimal adventure is achieved when real risk is managed and perceived risk is maintained in order to keep actual danger low and a sense of adventure high.^[36]

One popular models for risk assessment is the Risk Assessment and Safety Management (RASM) Model developed by Rick Curtis, author of *The Backpacker's Field Manual*.^[36] The formula for the RASM Model is: Risk = Probability of Accident × Severity of Consequences. The RASM Model weighs negative risk—the potential for loss, against positive risk—the potential for growth.

Information technology

IT risk is a risk related to information technology. This is a relatively new term due to an increasing awareness that information security is simply one facet of a multitude of risks that are relevant to IT and the real world processes it supports. "Cybersecurity is tied closely to the advancement of technology. It lags only long enough for incentives like black markets to evolve and new exploits to be discovered. There is no end in sight for the advancement of technology, so we can expect the same from cybersecurity."^[37]

ISACA's Risk IT framework ties IT risk to enterprise risk management.

Duty of Care Risk Analysis (DoCRA)^[38] evaluates risks and their safeguards and considers the interests of all parties potentially affected by those risks.

CIS RAM provides a method to design and evaluate the implementation of the CIS Controls™.

Petroleum and natural gas

For the offshore oil and gas industry, operational risk management is regulated by the safety case regime in many countries. Hazard identification and risk assessment tools and techniques are described in the international standard ISO 17776:2000, and organisations such as the IADC (International Association of Drilling Contractors) publish guidelines for Health, Safety and Environment (HSE) Case development which are based on the ISO standard. Further, diagrammatic representations of hazardous events are often expected by governmental regulators as part of risk management in safety case submissions; these are known as **bow-tie diagrams** (see Network theory in risk assessment). The technique is also used by organisations and regulators in mining, aviation, health, defence, industrial and finance.

Pharmaceutical sector

The principles and tools for quality risk management are increasingly being applied to different aspects of pharmaceutical quality systems. These aspects include development, manufacturing, distribution, inspection, and submission/review processes throughout the lifecycle of drug substances, drug products, biological and biotechnological products (including the use of raw materials, solvents, excipients, packaging and labeling materials in drug products, biological and biotechnological products). Risk management is also applied to the assessment of microbiological contamination (<http://www.pharmamanufacturing.com/articles/2011/126.html>) in relation to pharmaceutical products and cleanroom manufacturing environments.^[39]

Risk communication

Risk communication is a complex cross-disciplinary academic field related to core values of the targeted audiences.^{[40][41]} Problems for risk communicators involve how to reach the intended audience, how to make the risk comprehensible and relatable to other risks, how to pay appropriate respect to the audience's values related to the risk, how to predict the audience's response to the communication, etc. A main goal of risk communication is to improve collective and individual decision making. Risk communication is somewhat related to crisis communication. Some experts coincide that risk is not only enrooted in the communication process but also it cannot be dissociated from the use of language. Though each culture develops its own fears and risks, these construes apply only by the hosting culture.

See also

- Business continuity
- Disaster risk reduction
- Environmental Risk Management Authority (NZ)
- Catastrophe modeling for risk management
- Event chain methodology
- International Institute of Risk & Safety Management
- Loss-control consultant
- National Safety Council (USA)
- Optimism bias
- Pest risk analysis
- Risk appetite
- Roy's safety-first criterion
- Precautionary principle


- Representative heuristic
- Reference class forecasting
- BNP Paribas\$152 million risk management affair

References

1. Hubbard, Douglas (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It*. John Wiley & Sons. p. 46.
2. ISO/IEC Guide 73:2009 (2009). *Risk management — Vocabulary* (http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44651). International Organization for Standardization.
3. ISO/DIS 31000 (2009). *Risk management — Principles and guidelines on implementation* (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170). International Organization for Standardization.
4. Flyvbjerg, Bent & Budzier, Alexander (2011). "Why Your IT Project May Be Riskier Than You Think" (<https://hbr.org/2011/09/why-your-it-project-may-be-riskier-than-you-think>). *Harvard Business Review*. **89** (9): 601–603.
5. "Committee Draft of ISO 31000 Risk management" (https://web.archive.org/web/20090325160441/http://www.nsa.iie/uploads/file/N047_Committee_Draft_of_ISO_31000.pdf) (PDF). International Organization for Standardization. 2007-06-15. Archived from the original (http://www.nsa.iie/uploads/file/N047_Committee_Draft_of_ISO_31000.pdf) (PDF) on 2009-03-25.
6. "Risk Identification" (http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/3IdentificaciondelosRiesgos_en.pdf) (PDF). Comunidad de Madrid. p. 3.
7. CMU/SEI-93-TR-6 Taxonomy-based risk identification in software industry (<http://www.sei.cmu.edu/library/abstracts/reports/93tr006.cfm>). Sei.cmu.edu. Retrieved on 2012-04-17.
8. "Risk Management Systems Checklist (Common Items)" (https://www.fsa.go.jp/p_fsa/news/newse/ne_023/03.pdf) (PDF). *www.fsa.go.jp*.
9. Common Vulnerability and Exposures list (<http://cve.mitre.org>). Cve.mitre.org. Retrieved on 2012-04-17.
10. Crockford, Neil (1986). *An Introduction to Risk Management* (2 ed.). Cambridge, UK: Woodhead-Faulkner. p. 18. ISBN 0-85941-332-2.
11. "CRISC Exam Questions" (<https://www.dumpsbook.com/Exam/CRISC>). Retrieved 23 Feb 2018.
12. Dorfman, Mark S. (2007). *Introduction to Risk Management and Insurance* (9 ed.). Englewood Cliffs, N.J: Prentice Hall. ISBN 0-13-224227-3.
13. McGivern, Gerry; Fischer, Michael D. (1 February 2012). "Reactivity and reactions to regulatory transparency in medicine, psychotherapy and counseling" (http://eureka.sbs.ox.ac.uk/4314/1/McGivern_G_Fischer_M_D_%282012%29_Reactivity_and_Reactions_to_Regulatory_Transparency_in_Medicine_Psychotherapy_and_Counselling_%28Authors%27_version%29.pdf) (PDF). *Social Science & Medicine*. **74** (3): 289–296. doi:10.1016/j.socscimed.2011.09.035 (<https://doi.org/10.1016%2Fj.socscimed.2011.09.035>). PMID 22104085 (<http://www.ncbi.nlm.nih.gov/pubmed/22104085>).
14. IADC HSE Case Guidelines for Mobile Offshore Drilling Units (<https://www.iadc.org/ebookstore/ebook-iadc-hse-case-guidelines-for-mobile-offshore-drilling-units/>) 3.2, section 4.7
15. Roehrig, P (2006). "Bet On Governance To Manage Outsourcing Risk" (<http://www.btquarterly.com/?mc=bet-governance&page=ss-viewresearch>). *Business Trends Quarterly*.
16. SANS Glossary of Security Terms (<https://www.sans.org/security-resources/glossary-of-terms/>) Retrieved on 2016-11-13
17. ASIS <https://www.asisonline.org/publications--resources/news/blog/esrm-an-enduring-security-risk-model/>
18. Lev Virine and Michael Trumper. *Project Decisions: The Art and Science*. (2007). Management Concepts. Vienna. VA. ISBN 978-1-56726-217-9

19. Lev Virine and Michael Trumper. *ProjectThink: Why Good Managers Make Poor Project Choices*. Gower Pub Co. ISBN 978-1409454984
20. Peter Simon and David Hillson, *Practical Risk Management: The ATOM Methodology* (2012). Management Concepts. Vienna, VA. ISBN 978-1567263664
21. Kokcharov I. What Is Risk Management? <http://www.slideshare.net/igorkokcharov/what-is-project-risk-management>
22. Flyvbjerg, Bent (2003). *Megaprojects and Risk: An Anatomy of Ambition*. Cambridge University Press. ISBN 0521804205.
23. [Oxford BT Centre for Major Programme Management](#)
24. Berman, Alan. Constructing a Successful Business Continuity Plan. *Business Insurance Magazine*, March 9, 2015. <http://www.businessinsurance.com/article/20150309/ISSUE0401/303159991/constructing-a-successful-business-continuity-plan>
25. Craig Taylor; Erik VanMarcke, eds. (2002). *Acceptable Risk Processes: Lifelines and Natural Hazards* (<https://web.archive.org/web/20131203133515/http://www.asce.org/Product.aspx?id=2147485887&productid=5260>). Reston, VA: ASCE, TCLEE. ISBN 9780784406236. Archived from the original (<http://www.asce.org/Product.aspx?id=2147485887&productid=5260>) on 2013-12-03.
26. Rowling, Megan (2015-03-18). "New global disaster plan sets targets to curb risk, losses | Reuters" (<http://in.reuters.com/article/us-disaster-risk-agreement-idINKBN0ME27720150318>). *Reuters*. Retrieved 2016-01-13.
27. "American National Standard ANSI/NASBLA 101-2017: Basic Boating Knowledge--Human Propelled" (https://cdn.ymaws.com/www.americancanoe.org/resource/resmgr/spp-documents/ANSI_NASBLA_101-2017_Human_P.pdf) (PDF). Retrieved 2018-11-01.
28. "UIAA Standard 152: Ice Tools" (https://www.theuiaa.org/documents/safety-standards/152_IceTools_UIAA2018.pdf) (PDF). Retrieved 2018-11-01.
29. "EN 13089 Mountaineering equipment - Ice-tools - Safety requirements and test methods (includes Amendment A1:2015)" (<https://www.en-standard.eu/din-en-13089-mountaineering-equipment-ice-tools-safety-requirements-and-test-methods-includes-amendment-a1-2015/>). Retrieved 2018-11-01.
30. "Irish Standard I.S.EN 13089:2011+A1:2015 Mountaineering equipment - Ice-tools - Safety requirements and test methods" (<https://infostore.saiglobal.com/preview/is/en/2011/i.s.en13089-2011%2Ba1-2015.pdf?sku=1458668>) (PDF). Retrieved 2018-11-01.
31. "Association for Experiential Education" (<https://www.aee.org/standards2>). Retrieved 2018-11-01.
32. "NOLS Risk Services" (<https://www.nols.edu/en/about/risk-services/>). Retrieved 2018-11-01.
33. "Outdoor Safety Institute" (<http://www.outdoorsafetyinstitute.com>). Retrieved 2018-11-01.
34. "Viristar" (<https://www.viristar.com>). Retrieved 2018-11-01.
35. "Adventure Risk Management" (<https://adventureriskmanagement.com>). Retrieved 2018-11-01.
36. Schneider, Ari. *Outdoor Leadership and Education*. ISBN 9781732348202.
37. Arnold, Rob (2017). *Cybersecurity: A Business Solution*. Threat Sketch. p. 4. ISBN 978-0692944158.
38. "Duty of Care Risk Analysis Standard (DoCRA)" (<https://docra.org/>). DoCRA.
39. Saghee M, Sandle T, Tidswell E (editors) (2011). *Microbiology and Sterility Assurance in Pharmaceuticals and Medical Devices* (1st ed.). Business Horizons. ISBN 978-8190646741.
40. *Risk Communication Primer—Tools and Techniques* (<http://www.med.navy.mil/sites/nmcphc/Documents/policy-and-instruction/nmcphc-risk-communications-primer.pdf>). Navy and Marine Corps Public Health Center
41. *Understanding Risk Communication Theory: A Guide for Emergency Managers and Communicators* (<http://www.start.umd.edu/sites/default/files/files/publications/UnderstandingRiskCommunicationTheory.pdf>). Report to Human Factors/Behavioral Sciences Division, Science and Technology Directorate, U.S. Department of Homeland Security (May 2012)

External links

- [DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs \(https://www.acq.osd.mil/se/docs/2017-rio.pdf\)](https://www.acq.osd.mil/se/docs/2017-rio.pdf) (2017)
 - [DoD Risk Management Guide for Defense Acquisition Programs \(http://acqnotes.com/wp-content/uploads/2014/09/DoD-Risk-Mgt-Guide-v7-interim-Dec2014.pdf\)](http://acqnotes.com/wp-content/uploads/2014/09/DoD-Risk-Mgt-Guide-v7-interim-Dec2014.pdf) (2014)
 -  Media related to [Risk management](#) at Wikimedia Commons
-

Retrieved from "https://en.wikipedia.org/w/index.php?title=Risk_management&oldid=909801948"

This page was last edited on 7 August 2019, at 18:05 (UTC).

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.

[simplilearn.com](https://www.simplilearn.com)

Risk Management Strategies

View More

5-6 minutes

A risk can be a **Threat** i.e. a risk with negative impact on project objectives or it may be an **Opportunity** i.e. a risk which brings positive impact on project objectives, and accordingly there are different strategies to deal with negative and positive risks, when it comes to [Project management](#).

The strategies to deal with **Negative Risk or Threats** are:

1) Avoid – Avoidance eliminates the risk by eliminating the cause. It may lead to not doing the activity or doing the activity in different way. The project manager may also change or isolate the objective that is in trouble. Some risks can be avoided by early collection of information, by improving communication between stakeholders or by use of expertise.

Example of this approach includes extending the schedule or changing the [scope of the project activity](#). Another example could be a risk which is too hazardous that it may lead to loss of life and is avoided by shutting down the project completely.

2) Transfer – In Risk Transfer approach, risk is shifted to a third party. The third party, like insurance company or vendor, is paid to accept or handle the risk on your behalf and hence the ownership as well as impact of the risk is borne by that third party. This payment is called risk premium. Contracts are signed to transfer the liability of risks to third party.

Risk Transfer does not eliminate the risk but it eliminates the direct impact of the risk on the project. Few Transference tools are insurance policy, performance bonds, warranties, guaranties etc. This approach is most effective in covering financial risk exposure.

3) Mitigate – Mitigation reduces the probability of occurrence of a risk or reduces the impact of the risk within acceptable limits. This approach is based on the fundamental principle that earlier the action taken to reduce the probability or impact of a risk is more effective than doing fixes to repair the damages after the risk occurs.

Example of mitigating a risk includes use of advance technology or [best practices to produce more defect free products](#). Mitigation may require a prototype development to measure the risk level. In case where it is not possible to reduce the probability of the risk, the risk impact reduction is targeted by identifying the linkages that determine the risk severity.

4) Accept – Acceptance means accepting the risk, especially when no other suitable strategy is available to eliminate the risk. Acceptance can be passive acceptance or active acceptance.

Passive acceptance requires no other action except to document the risk and leaving the team to deal with the risks as they occur. In an active acceptance approach, a contingency reserve is designed to recover the losses of time, money or resources.

The strategies to deal with **Positive Risk or Opportunity** are:

1) **Exploit** – Exploitation increases the chances of making a positive risk happen, leading to an opportunity. As a project manager you assigned sufficient and efficient resources to take advantage of this opportunity. This approach reduces the uncertainty associated with a positive risk by ensuring that it definitely happens.

2) Share – When the project team themselves are not fully capable of taking advantage of the opportunity they might call in another company to partner with. The expertise of another company is leverage to maximize the return out of the opportunity. Examples of sharing opportunity include forming risk-sharing partnerships, teams, special purpose companies, or joint ventures. In this all parties gains as per their investment and action.

3) Enhance – Enhancing involves increasing the probability of occurrence of the risk and expanding its impact. This is done by identifying and influencing the various risk triggers. Example of enhancing an opportunity includes adding more resources to project activities to finish it earlier.

4) Accept – This involves taking the advantage of the positive risk as it happens but not actively pursuing it. It is just like opportunity coming and being accepted without much pre-planning.

Contingent Risk Response Strategies

These strategies are implied only when certain events occur. The execution of these strategies happens only under certain predefined conditions. The team waits for sufficient warning signals before implementing these strategies. These signals could be missing the milestones work items or deadlines etc.

These strategies includes using **Financial reserves, Staffing reallocations and implementing Workarounds** to minimize the loss, repair the damage to the extent possible and prevent recurrence.

References:-

Achieve PMP Exam Success, Margaret Chu, Diane Altwies,
Edward Walker, JRoss Publishing, 3rd Edition Head First PMP,
Jennifer Greene and Andrew Stellman, O'Reilly, 2nd Edition

business.tutsplus.com

Effective Risk Management Strategies

by Andrew Blackman 5 Jan 2015

13-16 minutes

So far in this series on risk management, we've looked at the [main types of risk a business can face](#), and how to [measure risk in your business](#).

The next logical step, of course, is to put together a plan for dealing with each risk you've identified, so that you can manage your risks on an ongoing basis. You'll learn exactly how to do that in this tutorial.

We'll start by seeing what a risk management plan might look like, and how you can put one together for your business. Then we'll look at the options you have in dealing with each individual risk, and how you can decide which strategy to employ. And finally we'll see how you can monitor risk in your business on a regular basis, and update your plan as necessary.

Putting together a solid risk management plan is one of the most important things you can do for your business. Companies fail all the time, sometimes blaming bad luck, "the economy", or other unforeseen circumstances. Risk management is about being prepared for as many of these adverse events as possible, so that you can ride out storms that make your competitors go under.

Disaster can still wreck the best-laid plans, of course, but taking risk management seriously will certainly increase your chances of long-term success. So let's get started.

1. Make a Plan

Every business should have a solid risk management plan. Here's a guide to putting one together.

The format can vary widely, depending on your company's needs. A risk management plan for a large, complex business could easily run to hundreds of pages, while a small business might just have a small spreadsheet focusing on the main items.

There are a few essential items to include in a risk management plan, however. Here they are:

- a list of individual risks
- a rating of each risk based on likelihood and impact
- an assessment of current controls
- a plan of action

Let's look at each of those in turn. If you've been following the series so far, you'll notice that we already covered the first two items in the [last tutorial](#). So we've got a good head-start on our plan already. Here's the sample table we put together last time:

Risk	Likelihood	Impact	Risk Score
Key client XYZ Corp is late paying its invoice.	5	2	10
Loss of power for more than 24 hours.	1	3	3
Our COO Janet leaves the company.	4	4	16
A new competitor undercuts the price of our main product.	2	5	10

Scathing product review from an influential magazine/website.	3	2	6
---	---	---	---

Your full plan will of course have a lot more items, but this example at least illustrates the format. You can refer to the other tutorial for more details about what each score means.

So to complete our risk management plan, we just need to add two more columns to our table.

The first new column is an assessment of current controls. For each of the risks you've identified, what are you currently doing to control that risk, and how effective is it?

For example, let's look at the first item on our table: "Key client XYZ Corp is late paying its invoice." Maybe you are already controlling for that risk by having automated reminders sent out when the invoice is close to its due date, and having one of your staff members responsible for following up personally with phone calls and emails. You'd list those as existing controls on your risk management plan.

So the next step is to consider the effectiveness of those actions. How well are things working right now? If your client almost always pays on time, for example, then your controls are effective. But if XYZ Corp has been late with its payments two or three times already this year, the controls are inadequate. Again, you could use a simple five-point scale here:

1. very inadequate, or non-existent
2. inadequate
3. satisfactory
4. strong
5. very strong

Then the final element of your plan details the action you plan to take in order to manage the risk more effectively. What could you do, either to reduce the likelihood of that event happening, or to minimize its impact when it does happen?

This last item is a little more complex, so we'll look at it in some more detail in the next section of this tutorial.

2. Decide How to Handle Each Risk

So at this point in the series, we've identified all the main risks in our business, prioritized them based on likelihood and impact, and assessed the effectiveness of our current controls.

The next step is to decide what to do about each risk, so that we can manage them best. In the world of risk management, there are [four main strategies](#):

1. Avoid it.
2. Reduce it.
3. Transfer it.
4. Accept it.

Each strategy has its own advantages and disadvantages, and you'll probably end up using all four. Sometimes it may be necessary to avoid a risk, and other times you'll want to reduce it, transfer it, or simply accept it. Let's look at what those terms mean, and how to decide on the right classification to use for each of your own business risks.

Avoid the Risk

Sometimes, a risk will be so serious that you simply want to eliminate it, for example by avoiding the activity altogether, or using a completely different approach. If a particular type of trading is very risky, you may decide it's not worth the potential reward, and

abandon it.

The advantage of this strategy is that it's the most effective way of dealing with a risk. By stopping the activity that's causing the potential problems, you eliminate the chance of incurring losses. But the disadvantage is that you also lose out on any benefits too. Risky activities can be very profitable, or perhaps have other benefits for your company. So this strategy is best used as a last resort, when you've tried the other strategies and found that the risk level is still too high.

Reduce the Risk

If you don't want to abandon the activity altogether, a common approach is to reduce the risk associated with it. Take steps to make the negative outcome less likely to occur, or to minimize its impact when it does occur.

With our earlier case, "Key client XYZ Corp is late paying its invoice", for example, we could reduce the likelihood by offering an incentive to the client to pay its bills on time. Maybe a 10% discount for early payment, and a penalty for late payment. Dealing with late-paying customers can be tricky, and we covered it more in our tutorial on [managing cash flow more efficiently](#), but these are a couple of options.

In the same example, we could reduce the *impact* by arranging access to a short-term credit facility. That way, even if the client does pay late, we don't run out of money. For more on short-term borrowing options like factoring and lines of credit, see our tutorial on [borrowing money to fund a business](#).

This is probably the most common strategy, and is appropriate for a wide range of different risks. It lets you continue with the activity, but with measures in place to make it less dangerous. If done well, you have the best of both worlds. But the danger is that your

controls are ineffective, and you end up still suffering the loss that you feared.

Transfer the Risk

We're all familiar with the concept of insurance from our everyday lives, and the same applies in business. An insurance contract is basically a transfer of risk from one party to another, with a payment in return.

When you own a home, for example, there's a big risk of losses from fire, theft, and other damage. So you can buy a home insurance policy, and transfer that risk to the insurance company. If anything goes wrong, it's the insurance company that bears the loss, and in return for that peace of mind, you pay a premium.

When you own a business, you have the option to transfer many of your risks to an insurance company as well. You can insure your properties and vehicles, and also take out various types of liability insurance to protect yourself from lawsuits. We'll look at insurance in more detail in the next tutorial in the series, but it's a good option for dealing with risks that have a large potential impact, as long as you can find an affordable policy.

Accept the Risk

As we've seen, risk management comes at a price. Avoiding a risk means constricting your company's activities and missing out on potential benefits. Reducing a risk can involve costly new systems or cumbersome processes and controls. And transferring a risk also has a cost, for example an insurance premium.

So in the case of minor risks, it may be best simply to accept them. There's no sense investing in a whole new suite of expensive software just to mitigate a risk that wouldn't have had a very big impact anyway. For the risks that received a low score for impact

and likelihood, look for a simple, low-cost solution, and if you can't find one, it may be worth simply accepting the risk and continuing with business as usual.

The advantage of accepting a risk is pretty clear: there's no cost, and it frees up resources to focus on more serious risks. The downside is also pretty clear: you have no controls in place. If the impact and likelihood are minor, that may be fine. But make sure you've assessed those things correctly, so that you don't get a nasty surprise.

3. Monitor

Putting measures in place isn't enough; you also need to check whether they're working, and monitor your business on a regular basis to identify and deal with new risks.

The starting point is the plan you've been putting together. You should now have a list of all the risks in your business, an assessment of their likelihood and impact, an evaluation of your current controls, and an action plan for dealing with them. [Here's an example](#) of how it could look when you put it all together (click the **Risk management plan and register** button at the bottom of the page).

The danger with a document like this is that you spend lots of time preparing it initially, but then never go back and update it later. A good risk management plan must be a living document, constantly referred to and updated to reflect new situations, new risks, and the effectiveness of your actions.

First of all, each action you define should have a target date for completion, and a person who's primarily responsible for it. For example, with our late-paying client, we could decide that our salesperson, Tina, will be responsible for renegotiating payment terms with XYZ Corp. to create incentives for timely payment, and

that this will be completed by March 1st.

When Tina's finished doing this, you'd move that from the "actions" column to the "current controls" column. Then over the following months, you'd assess how effective the new payment terms are at reducing the risk. If they're still not effective, you could look at the short-term financing option to reduce the impact of the late payments.

If neither of those options work, then you could look for other alternatives. If you've tried everything and the client still pays late, then you may decide to accept the risk if the client's business is really important to you, or you could go for the nuclear option of eliminating the risk altogether by avoiding doing business with that client.

The situation will evolve constantly over time, as the risks change and your responses to them have their own effect. Some of the controls you put in place may reduce the likelihood of the client paying late, making it less important to deal with. Or you may take on so many other clients that XYZ Corp. accounts for a smaller share of your revenue, so the impact of late payment is smaller. All of this needs to be accounted for.

There's no hard and fast rule about how often to update your risk management plan. Large companies have whole departments dedicated to full-time risk management, whereas in a small company the resources you can devote to it will probably be more limited. The key is to make a commitment to update your plan regularly, whether that's on a monthly basis, quarterly, or even annually.

One of the best approaches is to make small changes to individual items on an ongoing basis, as the changes occur, and then to carry out a more comprehensive review of the document on a less frequent, but still regular schedule. The comprehensive review

would include going back to the steps we covered in the earlier parts of this series, brainstorming about all the risks your business is subject to, adding new items to the list, and ranking them by importance. Then do the same with your existing risks, noting any changes.

Next Steps

If you take all of the steps outlined in this tutorial and the earlier parts of the series, you'll be in a good position to protect your business from many of the pitfalls that will come your way.

You now have a comprehensive risk management plan that outlines all the risks your business faces, and ranks them according to how likely they are to occur and how serious their impact would be.

You've evaluated the effectiveness of the controls you currently have in place, and come up with an action plan for either avoiding, reducing, transferring or accepting the risk.

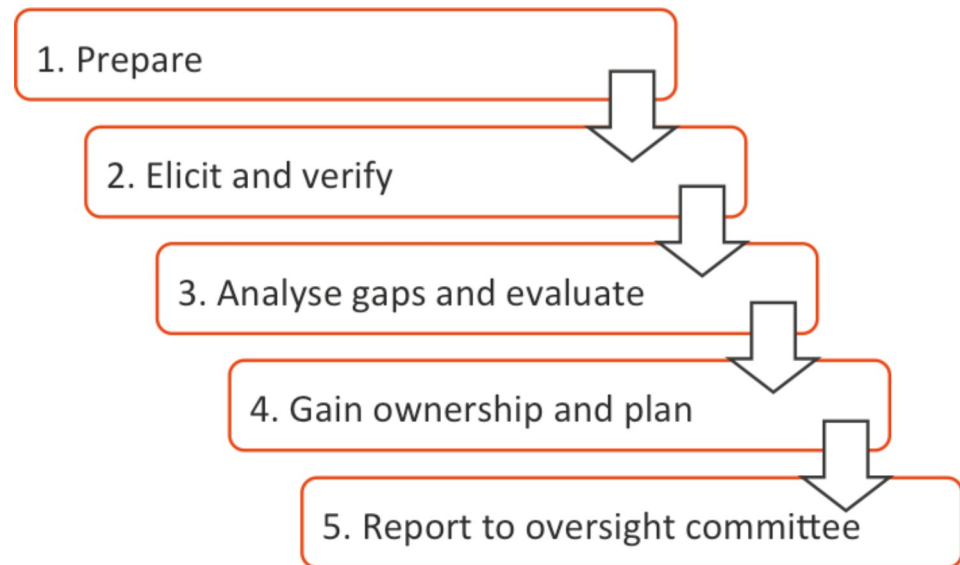
Your action plan has a clear timeline and a person responsible for implementing it, and you've made a commitment to monitoring the success of your actions and updating the plan as necessary.

Congratulations! You're in a better position than many other business owners. Truly unforeseeable events can still crop up and pose challenges, but you've done your best to plan for likely risks and to protect yourself as far as possible.

The final tutorial in this series will look in more detail at the option of transferring risk. There are quite a few different types of business insurance, and the categories are different from those you might be used to from your personal life. So stay tuned for a look at the main types of insurance that your business needs.

[Resource material](#) /

Evaluating the effectiveness of risk management



Our phased approach to evaluating risk management effectiveness

June 2014, published under [Governance assurance and oversight](#), [Managing risk in organisations](#)

This guide describes a systematic way of finding how effective is an organisation's current approach to managing risk. It considers the intentions of the organisation, how they are expressed and communicated and also what happens in practice. This leads to a realistic improvement program for the organisation's framework for managing risk and each application of the risk management process. The guide stresses how management must be involved in all stages to ensure success.

Introduction

All organizations of all kinds face internal and external factors and influences that make

it uncertain whether, when and the extent to which they will achieve or exceed their objectives. These objectives are its highest expression of intent and purpose, and typically reflect an organisation's explicit and implicit goals, values, and imperatives or relevant enabling legislation.

The international risk management standard, ISO 31000:2009, defines risk as the effect of uncertainty on objectives. The effective management of risk is therefore essential if organisations are to achieve their objectives and satisfy the needs of their stakeholders.

It has been long recognised that good governance and effective management are best achieved through the development and deployment within an organisation of one coherent and consistent framework, methodology and vocabulary for management of risk, to be used for all types of activity. This ensures that:

- There is a consistent and defensible basis for decision making at all levels, particularly where effort or capital is expended
- Change activities are more likely to succeed
- The organisation can pre-empt and capitalise on external changes such as those involving demographics, customers' needs and government policy
- All employees are encouraged to focus on and give priority to actions that aid and enhance the execution of strategic and project plans and the organisation's objectives
- The organisation is prepared for and protected from major incidents and losses
- Tactical moves, to identify and seize opportunities are stimulated and enhanced
- Accountability for risks and, most importantly, for controls and the monitoring and assurance of controls is clear and not doubtful.

In time this will also lead to a significant change in culture as the organisation as its employees engage on activities directly related to ensuring the achievement of goals and objectives and the successful completion of projects.

What is a framework and how does it lead to effective risk management?

An organisation's ability to manage risk effectively depends on its intentions and its

capacity to achieve those intentions. This intent and capacity is referred to as its risk management framework and is part of its system of governance and management.

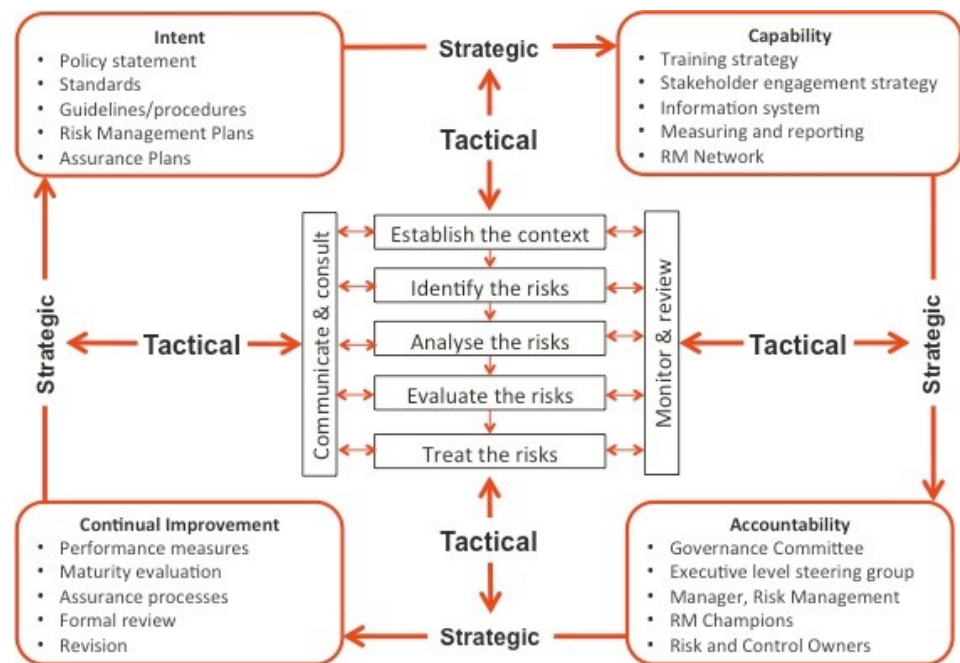
The quality of the framework is important because effective risk management requires:

- Clear expectations from 'the top'
- Appropriate capability (skills, resources, support)
- Sound relationships with stakeholders
- Integration of necessary risk management practices into the day-to-day activities and accountabilities of the management team
- A commitment to continually learn and improve.

The risk management framework should not attempt to replace the natural capability of people to manage risk; rather it should enhance good practices so that the process is reliable, comprehensive and consistent. For this to occur and for the required capability to be achieved, the organisation requires:

1. A set of suitable 'tools'
2. A coherent approach to training and communicating to people so that they can use those tools in a competent and consistent manner
3. An approach that signals and reinforces the correct behaviour and way of thinking.

The typical elements of a framework and an illustration of how this supports the integration of the risk management process is shown in the figure below.



The framework for risk management

General approach to effectiveness evaluation

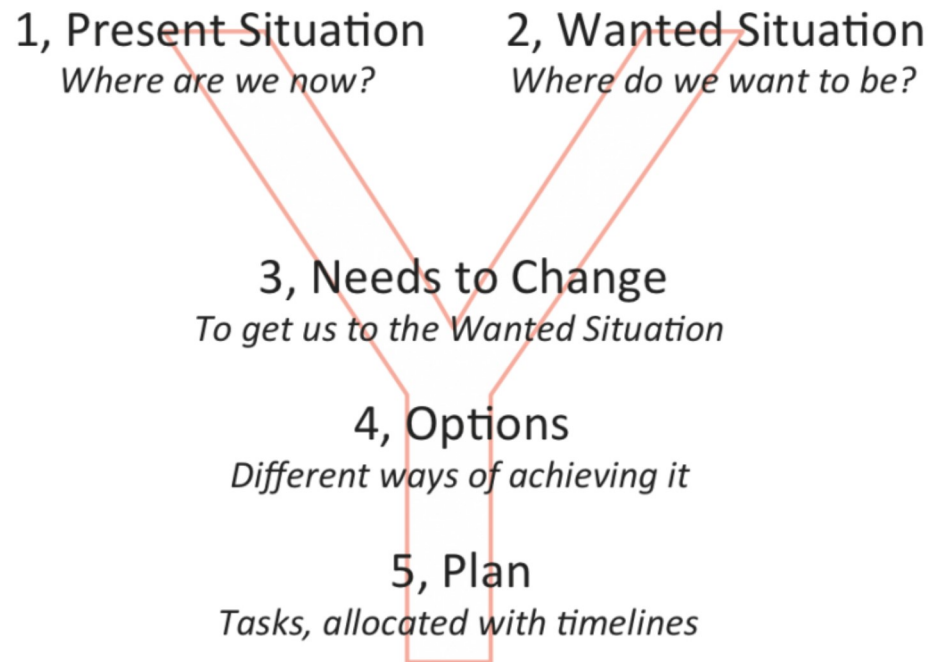
After many years of practical experience in evaluating and enhancing frameworks for risk management in organisations, Broadleaf believes that success depends as much in the manner in which any changes to a framework are developed and implemented as it does in the detail of the tools and written materials generated. This is why we would strongly recommend to our clients that we help it through a management of change process, where key internal stakeholders are carefully involved and engaged in evaluating the existing approach and in planning how, where and when enhancements will be made.

The core of this management of change process involves internal stakeholder representatives participating in a facilitated gap analysis and evaluation that then leads to a clear and practical enhancement and implementation plan. This is depicted in the “Y Model” shown in the figure and described below.

To enable those stakeholder representatives to participate effectively, they need to be well briefed on current risk management thinking and shown examples drawn from other organisations of elements of a risk management framework.

This approach has the added benefit that the participants of this process then become the organisation’s “Champions” who are motivated to lead the implementation process

in their own departments and functions. They also act to convince their superiors of the merits of the approach and motivate acceptance and use.



Y Model

To be successful and efficient, the management of change approach requires:

1. An accepted and accurate representation of the current arrangements for managing different forms of risk – the *present situation*
2. The fundamental concepts of risk and risk management and the desired goals in terms of the risk management framework and process to be clearly understood by those sponsoring the change – the *wanted situation*
3. A clear and accepted appreciation of the elements of the existing framework that need to be enhanced or improved and the nature of those changes and any additional elements that need created – *what needs to change*
4. The exploration of options, constraints, enablers and critical paths leading to an appropriate plan of actions with timings
5. A clear commitment to the plan and its implementation through the allocation of suitable resources by senior management and by their continued oversight of progress.

These steps can be tackled separately and the results fed back to senior management. However, after many years and numerous attempts we have found that most efficient approach, and the one that gains the greatest degree of ownership and endorsement, is to involve representatives of senior internal stakeholders in all these steps over a short space of time. This approach is described in detail below.

Phase 1 - Preparation

Evaluation studies typically start with an initial meeting where the detailed arrangements, including the schedule of activities and delivery dates, the documents to review reviewed and the interview candidates are agreed.

Prior to the meeting we issue a checklist of background documentation we would like to review and will often open up a secure Internet portal to which documents can be uploaded. This list can include:

- Relevant policy statements, framework descriptions, internal standards and procedures, with a particular focus on decision support and controls assurance
- Internal standards, procedures or guidelines that deal with particular applications of risk management. For example in the area of safety, procurement, security, operations, maintenance, BCM, compliance and project management
- The current strategic plan and objectives
- Examples of risk management plans and control assurance plans
- Extracts from the risk management information system including risk registers and risk treatment plans
- Methodology for and outputs from any quantitative risk analysis studies (range analyses) for schedule, capital and value evaluation and contingency estimation
- Copies of recent reports to any risk management steering committees or review groups and the oversight committee that show risk management performance
- Copies of any existing training and briefing materials that deal with risk management.

We then normally undertake a preliminary review of the materials and, from this, develop an aide memoire of sample questions that we might ask those we interview. This document is sent to those who are to be interviewed to allow them to prepare.

Phase 2 - Elicitation and verification

In our experience it is vital to observe and review how risk management takes place in practice. This is particularly true if there might be any discontinuity of practice across the organisation or inconsistent processes and systems. It is also important to test management's perceptions of the current approach to risk management to see if it is currently viewed as effective and is likely to satisfy their future needs.

We therefore undertake this observation through a series of structured interviews with senior managers from which we will draw conclusions on:

- The suitability of the current framework and tools to manage risk associated with an organisation of a comparable size and complexity, its risk profile and the risk criteria that should reflect its attitude (appetite)
- The drivers of that attitude, based on what are recognised as the 'key success factors' and growth objectives for the organisation
- The perceived usefulness of the current risk management process and its degree of integration into key decision-making processes;
- The strengths and limitations of the other approaches to risk management specific to particular kinds of risks that co-exist in the organisation
- Whether the tools and methods currently being used are capable of providing the organisation with a current, correct and comprehensive understanding of its risks and inform it whether the risks are within its risk criteria
- The level of understanding of senior managers about aspects of the risk management culture
- An outline of the perceived risk profile of the organisation and whether this varies from the risks reported to senior management and oversight committees.

Each interview usually takes about one hour and a member of the organisation's risk function normally accompanies us to help transfer knowledge.

While the predominant purpose of the interviews is to obtain information from the participants to support our review, they also provide an opportunity to explain the purpose of the study.

At the conclusion of the series of interviews we normally provide immediate feedback to the organisation's risk staff on:

- Our findings

- Our conclusions on the level of maturity, the strengths and weaknesses
- Our initial thoughts on where the organisation could enhance the management of risk and the steps that should be taken.

This meeting also allows any misunderstandings or misperceptions to be rectified.

Phase 3 - Gap analysis and evaluation

Using the information we have gathered we conduct a detailed gap analysis and evaluation of effectiveness using the guidelines and principles in ISO 31000 and what we understand is world's best practice as a basis for comparison. Often this is conducted as a facilitated workshop involving the management team.

The gap analysis looks at how the organisation expresses its intentions for managing risk and the elements of the capacity it claims it provides. In practice this involve us looking all the elements of the risk management framework and process shown above to determine if they are present and are suitable for the organisation and its environment.

We normally prepare a full gap analysis and evaluation report that includes our findings in terms of:

- The framework and how it facilitates the integration of risk management into decision making, including risk management plans and the strategy for their implementation
- How risk management is applied in strategy development and during the concept and development phases of projects, for decision-making and change management and as part of design review
- Control assurance and reporting
- The reliability of each element of the risk management process
- How risk management is used to deal with changes and to provide contingency arrangements that respond to disruptions, including how learning and feedback take place after events, incidents and decisions
- How the overall risk profile of the company is obtained and evaluated through aggregation and roll-up and how risks are treated at a corporate level
- The form and content of governance reporting

- How risk treatments are closed out and monitoring and review of risks, controls and risk treatments occurs
- The organisation's culture as it pertains to the management of risks in terms of both intent and practice
- The adequacy and effectiveness of the systems and resources available to support the management of risk, including human resources.

Phase 4 - Gaining ownership and detailed planning

We believe that it is important that senior managers appreciate and can comment on our findings and conclusions and that this leads to support for any enhancement plan. It is important that this takes place before our report is made available to the oversight committee so that it can indicate management's response.

We therefore normally present our findings and recommendations at a short meeting with senior managers. A typical draft agenda will be:

- Fundamentals of risk and best practice risk management
- Overall findings and assessment of the benchmarking review
- Suggested improvements and enhancement strategies
- Draft enhancement plan.

The planning component of this session follows the 'Y model' (see above) to elicit feedback and ownership of the current situation, the wanted situation and what needs to change. The management team is encouraged to discuss and compare options and then to finalise the enhancement plan actions and agree timelines. These agreements are recorded and included in our final report.

Phase 5 - Report to the oversight committee

Our clients often ask us to present our findings to their oversight committee. This provides them with the confidence that the evaluation was conducted in an independent manner and to enable the members to challenge and question any outcomes.

Normally our report is accompanied by the management-agreed enhancement plan, to indicate the organisation's commitment to improvement.

In most cases the oversight committee is provided with progress reports against this enhancement plan at subsequent meetings.

[Resource material](#) /

[Evaluating the effectiveness of risk management \(http://broadleaf.com.au/resource-material/evaluating-the-effectiveness-of-risk-management/\)](http://broadleaf.com.au/resource-material/evaluating-the-effectiveness-of-risk-management/)

Broadleaf Capital International

ABN 24 054 021 117

PO Box 607

Cammeray NSW 2062 Australia

Contact@Broadleaf.com.au

[+61 2 9488 8477](tel:+61294888477)

[+61 419 433 184](tel:+61419433184)

Creating value from uncertainty

Specialists in managing strategic, enterprise and project risk

Visit our website at www.Broadleaf.com.au

© Broadleaf Capital International Pty Ltd 2019