RISK MANAGEMENT WORKSHOP

Risk Management Handbook

Contents

Appendices

Understanding risk

Shon Harris

In this instalment of the Risk Management Guide, contributor Shon Harris explains what risk is and clarifies the differences between risk and vulnerability management.

Companies have always had to deal with different types of risk, be it financial, legal, the success of a new product launch or a merger, or the threat of natural disasters. These risks are traditionally treated as silos. The CFO is responsible for understanding and making decisions pertaining to financial risk. The IT department is responsible for the risk of losing data processing capabilities. Legal council is responsible for understanding and managing the company's legal issues. And so on. But this fragmented approach to risk is becoming more dangerous as companies face risks that threaten the company's overall existence. These risks come in the form of non-compliance with government regulations, increasing information security threats, terrorist activities and natural disasters. It is important now more than ever, for companies to develop and maintain a holistic risk management program that coordinates these silos because they all have the same overall goal – to protect the company and its assets.

Although many people in the information security industry use the word "risk," few have a true understanding of its definition and how it relates to the business world. Technically speaking, risk is the probability of a threat agent exploiting a vulnerability and the resulting business impact. For example, an open port could be a vulnerability and the corresponding threat agent could be a hacker who gets through that port and causes damage or loss, such as accessing customer credit card information in a backend database. Calculating the risk of this scenario requires understanding the possibility and probability of this taking place, but even more important, the to cost the company. Cost does not always have a straight forward quantitative value, which is what makes risk management a difficult task. Cost can come in the form of lost data, discredited reputation, loss of potential and unrealized customer revenue, loss of market share and more. These are qualitative and intangible components that make the calculation of risk much more difficult.

The misunderstanding of the term "risk" can be clearly seen in some of today's security product lines. There are many vendors that refer to their products as "risk management tools," when in fact they are vulnerability management tools. Identifying a vulnerability is usually simple. A vulnerability can be untrained workers, a misconfigured firewall, a facility in a flood zone, lack of security guards, an uninformed management staff, an open port or an unpatched system. The list of vulnerabilities that a company faces is practically infinite. Most vulnerability management tools today are high powered scanners that look for open ports, unpatched systems, default user accounts, etc. As "risk management tools," these products stop short.

For risk management to be carried out properly, a company must understand all of its vulnerabilities and match them to specific threats. (Some vulnerabilities do not have corresponding threat agents that can exploit them, so we don't need to worry about them as much.) The steps are:

- Identify the vulnerabilities
- Map the vulnerabilities to their corresponding threat agents
- Calculate the probability of each vulnerability being exploited
- Calculate the actual business impact that would result from such a compromise

The crux of risk management is that a company has an infinite amount of vulnerabilities, but finite amount of money available to deal with them. So the vulnerabilities that can cause the company the most harm must be dealt with first. Risk management is a science and an art that ensures that a company takes on only as much risk as it can handle and no more. This balance is much more difficult to achieve than most people are aware of.

In the following article I discuss risk management at the 10,000 foot level. In each remaining article I will dig deeper into each component and explain different risk management approaches, models and methodologies. The skill to the art of risk management is to know which approach is best for specific situations. From here I plan to then dig deep into how organizational security programs should be set up, implemented and maintained. Before a solid security program can be successfully erected, one must understand the underlining risk the company faces – because the main reason for a security program to even exist is to maintain the company's risk level.

An overview of the risk management process

Shon Harris

In this instalment of the Risk Management Guide, Shon Harris provides a 10,000-foot view of the risk management process.

A big question that companies have to deal with is, "What is enough security?" This can be restated as, "What is our acceptable risk level?" These two questions have an inverse relationship. You can't know what constitutes enough security unless you know your necessary baseline risk level.

To set an enterprise wide acceptable risk level for a company, a few things need to be investigated and understood. A company must understand its federal and state legal requirements, its regulatory requirements, its business drivers and objectives, and it must carry out a risk and threat analysis. (I will dig deeper into formalized risk and threat analysis processes in a later article, but for now we will take a broad approach.) The result of these findings is then used to define the company's acceptable risk level, which is then outlined in security policies, standards, guidelines and procedures.

Although there are different methodologies for risk management, the core components of any risk analysis is made up of the following:

1. Identify company assets
2. Assign a value to each asset
3. Identify each asset's vulnerabilities and associated threats
4. Calculate the risk for the identified assets

Once these steps are finished, then the risk analysis team can identify the necessary countermeasures to mitigate the calculated risks, carry out cost/benefit analysis for these countermeasures and report to senior management their findings.

Senior management can then choose one of the following activities pertaining to each of the identified risks:

- Mitigate the risk by implementing the recommended countermeasure
- Accept the risk
- Avoid the risk
- Transfer the risk by purchasing insurance

Many times senior management will follow the advice of the risk analysis team and allocate the necessary funds to implement the suggested countermeasures. Countermeasures can come in many different forms: firewalls, IDS, training, written policies and procedures, and so on. What is important to understand is

that no countermeasure can completely eliminate risk – there is always some risk. This is called residual risk. The question is if this residual risk is still too high or if it is below the organization's acceptable risk level.

The acceptable risk level revolves around the business impact that would be experienced if certain risks became realized. For example, employees in Company ABC are allowed to use instant messaging to communicate to each other and to customers. This is a vulnerability because it opens the door to viruses and other types of malware. The company has to weigh the necessity of this type of communication and how it relates to business needs, and determine if its benefits outweigh the corresponding risks. The company can carry out qualitative or quantitative processes to determine the business value of this type of communication and the cost of a virus infection.

If Company ABC is a stock brokerage firm, it may determine that time sensitive communication must be available between the customers and employees to allow the timely selling and purchasing of stocks. So the business impact of not being able to purchase and sell stocks in a restricted timeframe outweighs the business impact of a virus infection. As a software developer, Company EFG does not have a need for dynamic communication. This business risk is unacceptable and the company could choose to disallow any instant messaging traffic through its border devices. So in this example, Company ABC may choose to accept this specific risk and Company EFG may choose to avoid this risk. Risk avoidance means to not permit the actual activity that allows this risk to exist.

Company LMN may choose to implement a countermeasure for this type of situation. The company could choose to implement an internal instant messaging server, which allows their internal employees to use instant messaging. The border firewalls block instant messaging traffic from entering or leaving the network, which reduces the potential of obtaining virus infections through this medium.

I will go into all of the possible insurance policy types pertaining to information security that are available, but for now note that this is a way of transferring the burden of carrying so much risk. Currently this is the least most used way of dealing with information security risk because of its "newness" and cost, but this trend may change over time as companies are currently faced with risks that cannot be tamed with their available countermeasures.

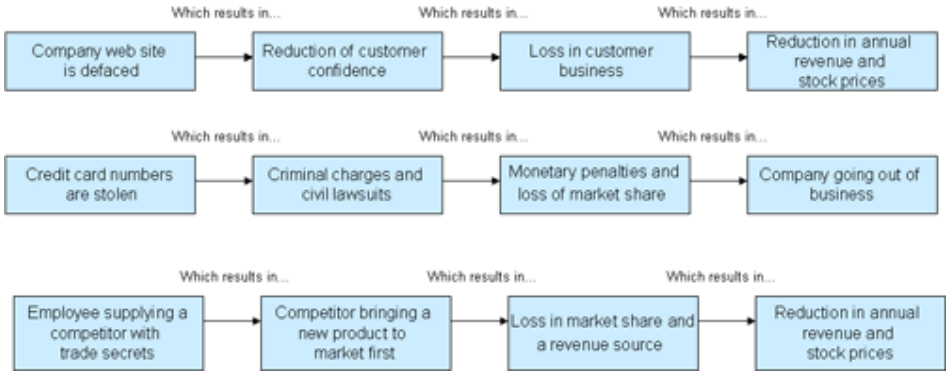
How to define an acceptable level of risk

Shon Harris

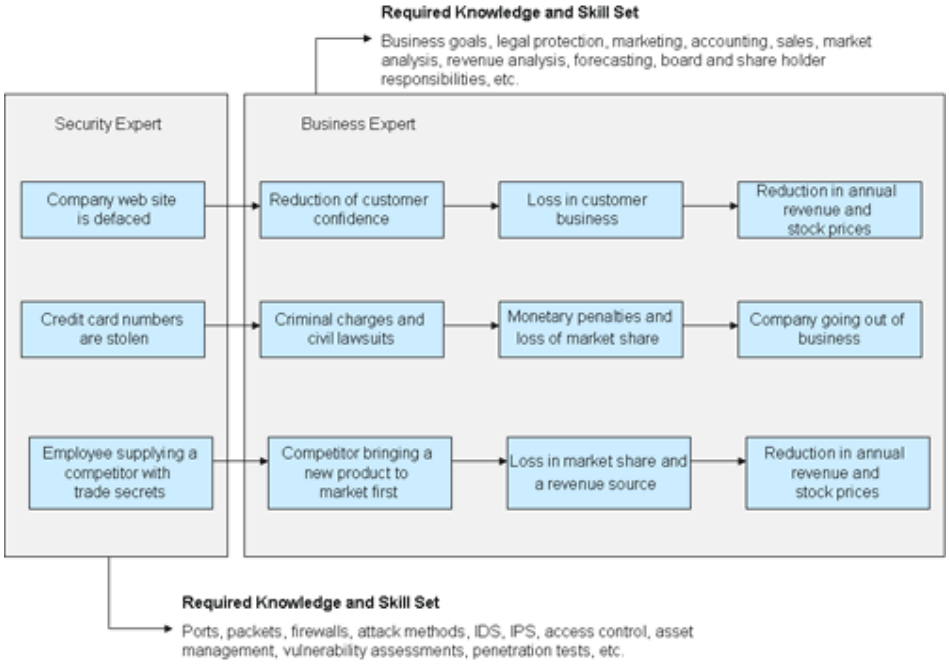
In this instalment of the Risk Management Guide, Shon Harris explains how to use threat modelling to define an organization's acceptable level of risk.

It is management's responsibility to set their company's level of risk. As a security professional, it is your responsibility to work with management and help them understand what it means to define an acceptable level of risk. Each company has its own acceptable risk level, which is derived from its legal and regulatory compliance responsibilities, its threat profile, and its business drivers and impacts. This article explains how to go about defining an acceptable level of risk based on a threat profile and business drivers. (Later in this series I will cover legal and regulatory compliance specifications.)

Defining the company's acceptable risk level falls to management because they intimately understand the company's business drivers and the corresponding impact if these business objectives are not met. Also, it is management's ultimate responsibility to ensure that the company meets these business objectives and goals. As a security professional, it is your job to illustrate to management how underlining security threats can negatively affect business objectives as shown in the following graphic.



It is important to understand the symbiotic relationship between business drivers and the security issues that can affect them. A company is not in business to be secure; it is in business to be profitable. A security professional may be an expert in firewalls, vulnerability management and IDS technologies, but if this knowledge is applied in a vacuum devoid of business goals, a company will end up wasting money and time in its security efforts. As illustrated in the following figure, each entity (security professional and business professional) must apply their expertise and work together to understand security and business in a holistic manner. Failure to identify and document business drivers and processes are the main reasons that mapping security and business drivers are difficult to accomplish and usually not properly carried out.



A company needs to recognize its top 5-8 business threats that can cause the most impact. For profit-driven companies, threats usually correspond to revenue sources. The following are common threats that companies are faced with:

1. Negative affects to reputation in the market
2. Loss of market share to competitors
3. Loss of customer confidence
4. Loss of revenue streams
5. Criminal and civil legal issues
6. Loss of trade secrets and sensitive information

For non-revenue driven organizations, such as the NSA and DoD, threats are not business-driven. These organizations' top threats could be:

1. Loss of the ability to protect the nation from nuclear and/or terrorist attacks
2. Loss of top secret information to the nation's enemies
3. Loss of communication with distributed military bases and troop units
4. Loss of the ability to tap into the enemy's communication channels
5. Loss of the ability to dispatch emergency crews

The security team should have an understanding of what is most critical to the organization to ensure that the most critical items are appropriately prioritized and protected. This information is also used to understand what attackers and enemies are most likely to attack and compromise. This information is captured in the organization's threat profile.

The threat modelling process

The term "threat modelling" is mainly used in application security. It is a process to identify threats that can impact a software program so that the application architects and developers can implement the necessary controls to thwart the identified threats. The same exercise is carried out for an organization. The resulting threat profile is used to define the company's acceptable risk level. This level is then used as the baseline to define "enough security" for all future security efforts within the company.

Threat modelling entails looking at an organization from an adversary's point of view. You must understand your adversaries' goals and motives if you want to implement the correct countermeasures to stop them. Threat modelling uses a methodical thought process to identify the most critical threats a company needs to be concerned with. The results of a threat modelling exercise are used to justify and integrate security at an architectural and implementation level. Threat modelling allows you to construct a structured and disciplined approach to address the top threats that have the greatest potential impact to the company as a whole.

The key in threat modelling is to understand the company's threat agents. For example, the NSA has a large range of dedicated and funded enemies that are set out to derail the agency's security measures. Foreign enemies attempt to break the encryption used to protect communication channels, NSA employees are targeted for social engineering attacks and perimeter devices are under

constant attack. If any of the identified threats become realized, the affects and impacts can be devastating to national security.

For most organizations, this is where threat modelling stops and a vulnerability assessment begins. You understand your enemy types and goals and corresponding threats at a high level, and then identify the vulnerabilities that these enemies can use against the company. In most cases the threat profile is not actually documented but understood at an intuitive level. This knowledge is then used throughout all risk management processes.

The objective is to determine the overall level of risk that the organization can tolerate for the given situation. The risk acceptance level is the maximum overall exposure to risk that should be accepted, based on the benefits and costs involved. If the responses to risk cannot bring the risk exposure to below this level, the activity will probably need to be stopped. So, once the acceptable risk level is set for a company, a risk management team is identified and delegated the task of ensuring that no risks exceed this established level.

To return to our example, the NSA's threat profile is at a heightened level because of its sheer number of threat agents and extremely low level of risk acceptance. The answer to, "How much is enough security?" for the NSA is extensive, expensive and robust security.

How to write a risk management policy

Shon Harris

In this instalment of the Risk Management Guide, Shon Harris describes the contents of a risk management policy and provides a sample policy template.

Proper risk management requires a strong commitment from senior management, a documented process that supports the organization's mission, an information risk management (IRM) policy and a delegated IRM team. Once you've identified your company's acceptable level of risk, you need to develop an information risk management policy.

The IRM policy should be a subset of the organization's overall risk management policy (risks to a company include more than just information security issues) and should be mapped to the organizational security policies, which lay out the acceptable risk and the role of security as a whole in the organization. The IRM policy is focused on risk management while the security policy is very high-level and addresses all aspects of security. The IRM policy should address the following items:

- Objectives of IRM team
- Level of risk the company will accept and what is considered an acceptable risk (as defined in the previous article)
- Formal processes of risk identification
- Connection between the IRM policy and the organization's strategic planning processes
- Responsibilities that fall under IRM and the roles that are to fulfil them
- Mapping of risk to internal controls
- Approach for changing staff behaviours and resource allocation in response to risk analysis
- Mapping of risks to performance targets and budgets
- Key indicators to monitor the effectiveness of controls

The IRM policy provides the infrastructure for the organization's risk management processes and procedures, and should address all issues of information security, from personnel screening and the insider threat to physical security and firewalls. It should provide direction on how the IRM team relates information on company risks to senior management and how to properly execute management's decisions on risk mitigation tasks.

The IRM policy can be written by outside security consultants, the CISO or the internal security team. The following is an example of a university IRM policy that can be used as a guideline to help in constructing a policy for your organization.

Intent

_____ Council has approved the introduction and embedding of risk management into the key controls and approval processes of all major business processes and functions of the University.

Risk is inherent in all academic, administrative and business activities, and every member of the University community continuously manages risk. _____ recognizes that the aim of risk management is not to eliminate risk totally, but rather to provide the structural means to identify, prioritize and manage the risks involved in all University activities. It requires a balance between the cost of managing and treating risks, and the anticipated benefits that will be derived.

_____ acknowledges that risk management is an essential element in the framework of good corporate governance and is an integral part of good management practice. The intent is to embed risk management in a very practical way into business processes and functions via key approval processes, review processes and controls -- not to impose risk management as an extra requirement.

Policy objectives

The Risk Management Policy has been created to:

- Protect the University from those risks of significant likelihood and consequence in the pursuit of the University's stated strategic goals and objectives;
- Provide a consistent risk management framework in which the risks concerning business processes and functions of the University will be identified, considered and addressed in key approval, review and control processes;
- Encourage pro-active rather than re-active management;
- Provide assistance to and improve the quality of decision making throughout the University;
- Meet legal or statutory requirements; and
- Assist in safeguarding the University's assets --¬ people, finance, property and reputation.

Policy statement

_____ adopts the Risk Management approach and general methodology specified in the AS/NZS4360:1999 Risk Management Standard.

All _____ business processes and functions will adopt a risk management approach consistent with the AS/NZS4360:1999 Risk Management Standard in their approval, review and control processes. The generic _____ risk management approach and methodology for this purpose is as set out in the _____ Risk Management Guidelines, as approved by the Vice-Chancellor from time-to-time.

The responsible manager for each _____ business process and function shall develop a form of risk management approach and associated documentation appropriate to their domain, which will be approved by the Vice-Chancellor upon recommendation from the Vice-President (Organizational Support).

Policy scope

This policy is applicable to all areas of the University, including:

- Faculties and academic units;
- _____ centres and institutes;
- Administrative units;
- Controlled entities, and entities that are derived from the University's legal status.

Responsibilities

Overall

Everyone in the University has a role in the effective management of risk. All staff should actively participate in identifying potential risks in their area and contribute to the implementation of appropriate treatment actions.

Governance

The Vice-Chancellor will be responsible on behalf of _____ Council for ensuring that a risk management system is established, implemented and maintained in accordance with this policy.

The Audit and Review Committee of _____ Council will be responsible for oversight and assurance of the processes for the identification and assessment of the strategic-level risk environment.

Operational

The Vice-Chancellor has delegated responsibility for oversight and implementation of this policy to the Vice-President (Organizational Support). The Senior Executive of the University will ensure risk management is embedded into the key controls and approval processes of all major business processes and functions. The Executive will be responsible to the Vice-President (Organizational Support) for the implementation of this policy within their respective areas of responsibility.

Heads of _____ subsidiaries and controlled entities ¬and associated entities operating under the name or legal status of the University ¬will be responsible to their respective Boards for the implementation and maintenance of appropriate risk management processes; and will provide reports to the Vice-Chancellor as directed on the implementation of these risk management processes.

The Planning & Quality Unit will provide reports to the Vice-Chancellor, Vice-President (Organizational Support), and Audit and Review Committee on the status of risk management implementation and effectiveness across the University; and will periodically report on the identification and assessment of major, strategic risk levels.

Communication

This policy is to be made available to all _____ staff, observed by all members of staff, both academic and administrative.

There will be an ongoing professional development and educational strategy to accompany the implementation of this policy.

Definitions

Definitions are taken from the Australian and New Zealand Risk Management Standard, with some modifications as appropriate to the particular _____ context.
A complete listing of methodology definitions related to risk management at _____ are included in the _____ Risk Management Guidelines.

Key definitions are:

- **Risk**
  The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood.
- **Consequence**
  The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
- **Likelihood**
  A qualitative description or synonym for probability or frequency.
- **Risk Assessment**
  The overall process of risk analysis and risk evaluation.
- **Risk Management**
  The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
- **Risk Treatment**
  Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:
  - Avoid the risk
  - Reduce the likelihood of occurrence
  - Reduce the consequences of occurrence
  - Transfer the risk
  - Retain/accept the risk
- **Risk Management Process**
  The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating risk.

Exclusions

There are no exclusions. This policy applies to all areas of the University.

Related information

Further administrative information about this policy
Related policies/guidelines
Responsibilities and contacts
Implementation of the policy: Vice-President (Organizational Support)
Monitoring & evaluation of the policy: Planning & Quality
Development/revision of the policy Planning & Quality
Review date: 2008
The following person may be approached on a routine basis in relation to this policy:
Name:
Area:
Position:
Extension:
E-mail:

How to conduct a risk analysis

Shon Harris

In this instalment of the Risk Management Guide, Shon Harris provides step-by-step instructions on conducting a risk analysis.

A risk analysis helps integrate security program objectives with the company's business objectives and requirements. The more the business and security objectives are in alignment, the more successful the two will be. The analysis also helps the company draft a proper budget for a security program and its constituent security components. Once a company knows how much its assets are worth and the possible threats they are exposed to, it can make intelligent decisions on how much money to spend on protecting those assets.

Risk analysis, which is a tool for risk management, is a method of identifying vulnerabilities and threats, and assessing the possible damage to determine where to implement security safeguards. Risk analysis is used to ensure that security is cost effective, relevant, timely and responsive to threats. Security can be quite complex, even for well-versed security professionals, and it is easy to apply too much security, not enough security or the wrong security components, and spend too much money in the process without attaining the necessary objectives. Risk analysis helps companies prioritize their risks and shows management the amount of money that should be applied to protecting against those risks in a sensible manner.

A risk analysis has four main goals:

- Identify assets and their values
- Identify vulnerabilities and threats
- Quantify the probability and business impact of these potential threats
- Provide an economic balance between the impact of the threat and the cost of the countermeasure

The process of conducting a risk analysis is very similar to identifying an acceptable risk level. Essentially, you do a risk analysis on the organization as a whole to determine the acceptable risk level. This is then your baseline to compare all other identified risks to determine whether the risk is too high or if it is under the established acceptable risk level.

Step one: Identify assets and their values

Risk analysis provides a cost/benefit comparison, which compares the annualized cost of safeguards to protect against threats with the potential cost of loss. A safeguard, in most cases, should not be implemented unless the annualized cost of loss exceeds the annualized cost of the safeguard itself. This means that if a

facility is worth $100,000, it does not make sense to spend $150,000 trying to protect it.

The value placed on assets (including information) is relative to the parties involved, what work was required to develop it, how much it costs to maintain, what damage would result if it were lost or destroyed, and what benefit another party would gain if it were to obtain it. If a company does not know the value of the information and the other assets it is trying to protect, it does not know how much money and time it should spend on protecting them.

The value of an asset should reflect all identifiable costs that would arise if there were an actual impairment of the asset. If a server costs $4,000 to purchase, this value should not be input as the value of the asset in a risk assessment. Rather, the cost of replacing or repairing it, the loss of productivity and the value of any data that may be corrupted or lost, need to be accounted for to properly capture the amount the company would lose if the server were to fail for one reason or another.

The following issues should be considered when assigning values to assets:

- Cost to acquire or develop the asset
- Cost to maintain and protect the asset
- Value of the asset to owners and users
- Value of the asset to adversaries
- Value of intellectual property that went into developing the information
- Price others are willing to pay for the asset
- Cost to replace the asset if lost
- Operational and production activities that are affected if the asset is unavailable
- Liability issues if the asset is compromised
- Usefulness and role of the asset in the organization

Understanding the value of an asset is the first step to understanding what security mechanisms should be put in place and what funds should go toward protecting it. A very important question is how much it could cost the company to not protect the asset.

Step two: Identify vulnerabilities and threats

Once the assets have been identified and assigned values, all of the vulnerabilities and associated threats need to be identified for each asset or group of assets. The IRM team needs to identify the vulnerabilities that could affect each asset's integrity, availability or confidentiality requirements. All of the relevant vulnerabilities need to be identified and documented so that the necessary countermeasures can be implemented.

Since there is a large amount of vulnerabilities and threats that can affect the different assets, it is important to be able to properly categorize them. The goal is to determine which threats and vulnerabilities could cause the most damage so that the most critical items can be taken care of first.

Step three: Quantify the probability and business impact of these potential threats

The team carrying out the risk assessment needs to figure out the business impact for the identified threats.

To estimate potential losses posed by threats, answer the following questions:

- What physical damage could the threat cause, and how much would that cost?
- How much productivity loss could the threat cause, and how much would that cost?
- What is the value lost if confidential information is disclosed?
- What is the cost of recovering from a virus attack?
- What is the cost of recovering from a hacker attack?
- What is the value lost if critical devices were to fail?
- What is the single loss expectancy (SLE) for each asset and each threat?

This is just a small list of questions that should be answered. The specific questions will depend upon the types of threats the team uncovers.

The team then needs to calculate the probability and frequency of the identified vulnerabilities being exploited. The team will need to gather information about the likelihood of each threat taking place from people in each department, past records and official security resources. If the team is using a quantitative approach, then they will calculate the annualized rate of occurrence (ARO), which is how many times the threat can take place in a 12-month period.

Step four: Identify countermeasures and determine cost/benefit

The team then needs to identify countermeasures and solutions to reduce the potential damages from the identified threats.

A security countermeasure must make good business sense, meaning that it is cost-effective and that its benefit outweighs its cost. This requires another type of analysis: ***a cost/benefit analysis***.

A commonly used cost/benefit calculation for a given safeguard is:
(ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the company

For example, if the ALE of the threat of a hacker bringing down a Web server is $12,000 prior to implementing the suggested safeguard, $3,000 after implementing the safeguard, and the annual cost of maintenance and operation of the safeguard is $650, then the value of this safeguard to the company is $8,350 each year.

The cost of a countermeasure is more than just the amount that is filled out on the purchase order. The following items need to be considered and evaluated when deriving the full cost of a countermeasure:

- Product costs

- Design/planning costs
- Implementation costs
- Environment modifications
- Compatibility with other countermeasures
- Maintenance requirements
- Testing requirements
- Repair, replacement or update costs
- Operating and support costs
- Effects on productivity

So, for example, the cost of this countermeasure could be:

$5,500 for the product
$2,500 for training
$3,400 for the lab and testing time
$2,600 for the loss in user productivity once the product was introduced into production
$4,000 in labour for router reconfiguration, product installation, troubleshooting, and installation of the two service patches.

The real cost of this countermeasure is $18,000. If our total potential loss was calculated at $9,000, we went over budget by 100% when applying this countermeasure for the identified risk. Some of these costs may be hard or impossible to identify before they are acquired, but an experienced risk analyst would account for many of these possibilities.

It is important that the team knows how to calculate the actual cost of a countermeasure to properly weigh it against the benefit and savings the countermeasure is supposed to provide.

Goals of a risk analysis

The risk analysis team should have clearly defined goals that it is seeking. The following is a short list of what generally is expected from the results of a risk analysis:

- Monetary values assigned to assets
- Comprehensive list of all possible and significant threats
- Probability of the occurrence rate of each threat
- Loss potential the company can endure per threat in a 12-month time span
- Recommended safeguards, countermeasures and actions

Although this list looks short, there is usually an incredible amount of detail under each bullet item. This report is presented to senior management, which will be concerned with possible monetary losses and the necessary costs to mitigate these risks. Although the reports should be as detailed as possible, there should be executive abstracts so that senior management may quickly understand the overall findings of the analysis.

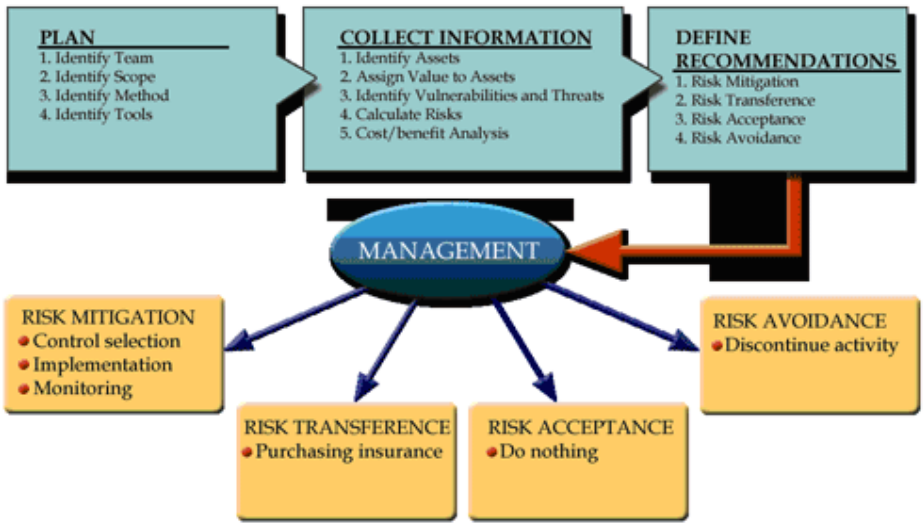
How to deal with risk

Shon Harris

In this instalment of the Risk Management Guide, Shon Harris explains the four ways to deal with identified risk: transfer it, avoid it, reduce it or accept it.

Once a company knows the amount of risk it is faced with, it must decide how to handle it. There are four basic ways of dealing with risk: transfer it, avoid it, reduce it or accept it.

Many types of insurance are available to companies to protect their assets. If a company decides that the total or residual risk is too high to gamble with, it can purchase insurance, which transfers the risk to the insurance company.



If the company implements countermeasures, this reduces the risk. If management decides that the action that is incurring the risk does not have a strong business case for its existence, then they can decide to stop that activity altogether. This is referred to as avoiding the risk. The last approach is to accept the risk, which means the company understands the level of risk and the potential cost of damage, and decides to just live with it without implementing any countermeasures. Many companies will accept risk when the cost/benefit ratio indicates that the cost of the countermeasure outweighs the potential loss value.

The reason that a company implements countermeasures is to reduce its overall risk to an acceptable level. But no system or environment is 100% secure, which

means there is always some risk left over to deal with. This is called residual risk.

Residual risk is different from total risk, which is the risk a company faces if it chooses not to implement any type of safeguard or to transfer some of the risk. A company may choose to take on total risk if the cost/benefit analysis results indicate that this is the best course of action. For example, if there is a small likelihood that a company's Web servers can be compromised and the necessary safeguards to provide a higher level of protection cost more than the potential loss in the first place, the company will choose not to implement the safeguard, leaving it with the total risk.

There is an important difference between total risk and residual risk, and which type of risk a company is willing to accept. The following are conceptual formulas:

threats x vulnerability x asset value = total risk
(threats x vulnerability x asset value) x controls gap = residual risk

During a risk assessment, the threats and vulnerabilities are identified. The possibility of a vulnerability being exploited is multiplied by the value of the assets that are being assessed, which results in the total risk. Once the controls gap (protection the control cannot provide) is factored in, the result is the residual risk. Implementing countermeasures is a way of mitigating risks. Because no company can remove all threats, there will always be some residual risk. The question is what level of risk the company is willing to accept.

The information risk management team is responsible for ensuring that any countermeasure that is implemented or when some risk is transferred that the remaining residual risk meets the acceptable risk level set by management. This is not a scientific process that can be carried out through the use of mathematical formulas – it is more subjective in nature.

The Channel Tunnel (20 June 1993)

The Channel Tunnel linking England with France is a superb technical and engineering achievement. However, as a business project it has undoubtedly been a failure. Shareholders in the company operating the concession for the tunnel have witnessed significant loss of value in their equity stake in the company.
The paragraphs below are taken from The Management of Projects by Peter W G Morris published by Thomas Telford, London, in 1994:

"Proposals for tunnelling under the English Channel became a serious possibility in 1955, when the British ceased to regard a tunnel as a threat to national security. In 1967 proposals were invited for private financing and construction of the tunnel, with 70 - 90 % of the loans guaranteed by the British and French governments; once operational the facility was to be government owned. British Rail was a member of the project, but was not anxious to divert its scarce funds to it and never took it particularly seriously, at least not until the UK Government issued a White Paper in 1973 that endorsed the project but added, unnecessarily, 'that a high quality railway between the Tunnel and London and the provision for through services to the provincial centres is essential for success.' During 1974 the UK Government faced a rapidly deteriorating economic situation, caused largely by the first OPEC price rise (Maplin and the London Ringway motorway scheme being cancelled at this time). In the summer of 1974 British Rail revised its forecast for the high-speed rail link upwards by £130m to £330m, a far greater increase than the Government could then countenance. Unfortunately, it was not able to postpone a decision on funding, as it wished to do, since the Anglo-French Treaty had to be ratified by January 1975. The project was therefore abandoned.

"Following this failure, however, studies were continued by British Rail and SNCF, the French national rail company, who published proposals in February 1979 for a rail-only single-track tunnel, British Rail suggesting that an adequate connection might now be built at the relatively low cost of £25m. The interest of several construction firms was stimulated by this new proposal. To be financially viable, the contractors felt, the cross-Channel link had to be capable of taking vehicles: the rail scheme did not allow this. One group, later to be called the Channel Tunnel Group (CTG), concluded that the scheme cancelled in January 1975 was still the most viable. Another, Euroroute, decided that the link should be a drive-through scheme consisting of bridges and an immersed tube.

"The governments' response to the various proposals now being generated was supportive, provided that -crucially, in terms of the subsequent development of BOO(T)- the scheme would be financed from the private sector. It was agreed that a joint official study should be commissioned. This appeared in 1982, recommending 'bored twin rail tunnels with a vehicle shuttle constructed, if necessary, in phases.

"In June 1982 the governments accepted an offer by an Anglo-French financing group to study the feasibility of privately financing the fixed link. This reported in May 1984, concluding that the bored tunnel option was best. Since there was no natural owner for the project, the banks felt that the chance of getting a significant portion of equity into the scheme was slim. Some level of EEC or government support would be necessary, they believed, given the size and novelty of the project, but some form of risk sharing between the private and public sectors might also be possible.

"The UK Government rejected this call for 'marginal guarantees' and made it clear that the project would have to be financed 'entirely without the assistance of public funds and without commercial guarantees by the Government'. Observing the success of recent UK privatization schemes, CTG and the banks now concluded that perhaps the financial markets could after all fund the project. Euroroute soon announced that it too would be able to raise the necessary private funds provided certain political guarantees of non-interference could be given.

" On 30 November 1984, Mrs Thatcher met with President Mitterand. To the surprise of many,, the two leaders announced their enthusiasm for a fixed link between their two countries, provided it was financed, built and operated by the private sector.

"The timetable set by the two governments was tight. French parliamentary elections were scheduled for March 1986 and the French presidential election for 1988, which was also the latest year for a general election in the UK. Agreement between the governments before March 1986, and the passing of all necessary legislation before the presidential and general elections, were seen as essential to avoid the 1974 problem of political change disrupting the project. The governments decided, therefore, to issue their guidelines by the spring of 1985, which they did.

"Schemes were submitted on 31 October 1985. On 20 January 1986 it was announced that the CTG's scheme had been selected. One month later the Concession Agreement, granting the CTG the right to build and operate the tunnel, was concluded. In April a hybrid bill was introduced to Parliament with the aim of obtaining Royal Assent in the early summer of 1987.

"Under-staffing posed an immediate and serious problem. Huge effort had gone into getting the concession. Now, suddenly, the winning group had to staff and organize to carry out the project. Since the project was contractor-originated, the question immediately arose (as it always does on BOO(T) projects) of how to set up a strong owner organization independent of the sponsoring contractors that could give direction, manage the contractors and ensure value for money.

"CTG was split into an owner organization, Eurotunnel, and the contractors, Transmanche-Link. Staff were temporarily seconded from the promoting companies with the intention that they be replaced rapidly at CTG. The secondees, however, had to negotiate with their own companies and report to a board drawn totally from contractors and banks. At the highest level, therefore, there were conflicts of interest. And work started at a furious pace. Construction was to start in march 1986, and a construction contract therefore had to be in

place very soon; a firm underwriting of funds from lending banks had to be obtained before going to the equity markets; the Termsheet for the bank lending and the underwriting, meanwhile, was not achievable until agreement had been reached with the railways.

"The financing scheme proposed was one of the most complex for many years. The CTG partners contributed to the initial £50m of the project's working capital (Equity1). Further share placings were planned for June 1986 (Equity 2) and mid-1987 (Equity 3). The programme was almost certainly over-optimistic, bring driven by the original promoters' desire to minimize the money they had to put in (Equity 1) and to go to the market for equity 2 before complaints began to be aired during the planning hearings in Parliament. The date for Equity 3 was based on the project's requirement for funds rather than the ability of Eurotunnel to prepare for such a major share issue. Equity 3 also, of course, had to be after the Treaty had been ratified, so that the political risk element would not disturb the placing.

"The financing schedule was soon delayed. Suspicious that the contract terms were too easy on the contractors, the financiers insisted on their revision: as new banks and other financiers were introduced to the project, several further revisions were requested. In addition, Eurotunnel's advisers were strongly of the opinion that the contracts had to be sharper if the share prospectus was to be successful. The contracts were eventually signed, after numerous lengthy and often acrimonious drafting sessions, only in mid-August 1986, some three months later than planned. This delay caused Equity 3 to be postponed to October.

"The Equity 2 share placing represented the first major testing of the financial viability of the project - and the project would be nothing if it was not supported by the markets. In the event, the placing was almost a disastrous failure. The £206m sought was to be raised from institutions in Britain (£70m), France (£70m), Japan, the USA and other international markets. The French placing proved relatively straightforward. In Britain, the result was nailbiting. Subscriptions had to be paid by 2 p.m. on 29 October. By Friday lunchtime, 24 October, there was clear indication that the placing might fail. The Government later denied lobbying, but in the event £75m was raised in the UK (£75m was also raised in France) amid much talk of last minute arm-twisting by the Bank of England.

"In February 1987, Eurotunnel got a new Chairman, Alastair Morton; he was faced with several immediate challenges. Most important was the re-establishment of confidence in the project among financiers to the level where the £750m of Equity 3, on which the £5bn of bank lending depended, could successfully be raised. Politically, the project still had to steer its way through Parliament, where its planning application was being reviewed. There was also the threat of the general election turning out badly for the project. In fact all these difficulties were successfully overcome within a few months. Mrs Thatcher was re-elected. Royal Assent was given in July, and the Equity 3 shares were successfully placed by November. With the money thus raised, construction of the Tunnel began in earnest.

"However, there was a final, unplanned stage in the saga of raising finance and managing the Channel Tunnel project. By late 1988 - early 1989 it was apparent that additional finance might be required to complete the project. By October 1989 the estimate had risen to £7bn. November 1990 saw Eurotunnel launching a rights issue to fund the £7.6bn now estimated to be required. By December 1993 the total cost looked like exceeding £10bn with a further rights issue necessary. Equally depressing, completion slipped to March - may 1994. Once again, the awful predictions of major project pundits were being proved true: a cost overrun of 100% and the project about a year late. How had this happened? Why had we still not learnt to get the management of projects right? After all, the contractors - those who 'really know' about construction - had assured the markets that the project could be built for the £4.87bn forecast in November 1987.

"Essentially, the answer is to be found in that old problem of concurrency - of starting construction before the design is properly worked out. With the Tunnel, the problem was that the mechanical and electrical systems, the rolling stock and various safety requirements were not fully defined before the markets were approached for full funding. As the complexity of these systems grew, their costs rose. Inflation was significantly higher than forecast. Claims of £800m arose between Eurotunnel and the contractors. Conflict grew; teamwork, never particularly good, declined to the point in mid 1993 that Eurotunnel was even barred from access to the works by the contractors. Concurrency, contractual disputes, overruns: a familiar story!"

Taken from the Management of Projects by Peter W G Morris published by Thomas Telford, London, in 1994

The Concorde aircraft (01 May 1976)

The Concorde aircraft can also be regarded as a technical and engineering triumph but a commercial disaster as a project. The following extract is also taken from Peter Morris's book:
" Concorde was the first of an important new breed of aerospace projects: those built through international collaboration. It was a huge technology-push 'spearhead' project, whose basic requirement was simply to carry passengers safely and supersonically. Its development represented a continual struggle to reconcile two entirely different requirements: sustained supersonic flight and subsonic approach. Its management practices were largely those of TSR-2: its cost-escalation and schedule delays were huge. This occasioned much public criticism and governmental chagrin. The British governmental psyche was so traumatized that its response to suggestions for high-risk major projects for many decades subsequently was invariably one of nervous disinclination. However, Concorde was an economic disaster not so much because of its huge developmental difficulties and costs as because of the unexpectedly high cost of fuel and the inability to obtain authorization to fly it supersonically over land.

"Concorde was first proposed by UK government ministers in 1956. The feasibility of a supersonic transport was confirmed in principle in 1959. In 1960 - 1062 the British and French governments discussed, at the initiative of the British, the prospect of the project being accomplished jointly. In 1962 a treaty was signed between the two governments for the joint design, development and production of a supersonic airliner. There was no break clause to the treaty, no performance requirements and no financial limits. Management structures and programmes (schedules) were proposed in the treaty, but generally in imprecise terms. The management structure, for example, comprised a series of hierarchical committees: the project was set up with little regard to the most basic rules of project management, such as a clearly identified owner organization; there was no owner and no one person 'in charge'. The first prototype flight was scheduled for the second half of 1966, with the Certificate of Airworthiness to be awarded at the end of 1969; in fact these were accomplished in October 1969 and December 1975 respectively. The project's financial estimate in November 1962 was £135.2 m; by 1979 the cost of the programme had grown more than eightfold to around £1129 m."

" Between 1964 and 1970, Concorde's commercial prospects became increasingly doubtful. The pattern of air traffic began to change with the advent of wide-bodied aircraft; economy and price became the critical parameters rather than speed. The new Labour government of 1964 attempted to cancel the plane, along with TSR-2, the P-1154 and HS-681, but was rebuffed by the French who threatened to sue the British government in the International Court of Justice if the Treaty was abrogated. The decision to go into production was taken in 1968, Environmentalist opposition grew dramatically, particularly in the USA, where it effectively killed the US Supersonic Transport…..With the rise in the price of fuel oil following the Yom Kippur war in 1973, the economics of operating Concorde became even more unfavourable, especially as its economic speed was designed to be Mach 2 rather than subsonic. In 1973, most of the options taken by airlines to buy Concorde were revoked. Obtaining permission to enter the USA proved extremely difficult, and it was not until May 1976, 20

years after the project's inception, that the first flight landed in Washington DC. Concorde did not land in New York until November 1977.

"In the end, Concorde proved to be a commercial disaster for its developers (the two governments), although not for its builders or operators: a technological triumph yet a plane designed on the massive misconception that speed was the principal criterion for airliner success' an aircraft project that was set up with no regard to the most basic rules of project management, such as a clearly identified owner organization, and one which experienced severe problems of design and technology management; a project whose chances of success were severely compromised by the two external factors of changes in fuel prices and environmentalist opposition."

Taken from The Management of Projects: Peter W G Morris (Thomas Telford, London, 1994) pp 171 – 176

The sinking of the RMS Titanic (15 April 1915)

The tragic sinking of the Titanic after colliding with an iceberg on her maiden voyage across the Atlantic in April 1912 is a good example of the catastrophic failure of a business 'project' - the project in question being the safe operation of a large passenger liner. The loss of the Titanic was a disaster, with incalculable losses, including very heavy loss of life -1523 passengers perished in one of the worst maritime disasters of the last century; the destruction of an asset worth hundreds of millions of pounds in todays prices and the reputation of the White Star Line permanently tarnished. What compounds the nature of this catastrophe is that the huge loss of life associated with the sinking of the Titanic was largely avoidable had sufficient precautions been taken. Truly the designers of the Titanic, by failing to provide sufficient lifeboat capacity, were dicing with death.
The RMS Titanic sunk on April 15 1912 with very heavy loss of life which occurred because of a number of reasons. First, there was undeniably a certain amount of complacency and which affected the management of the ship. It is possible that this complacency may have been linked with the reputation, which proved tragically quite unjustified in the subsequent light of the tragic sinking, of the unsinkability of this vessel. Secondly, there does appear to have been evidence of insufficient preparation for the evacuation of the ship once the iceberg had been struck. Thirdly, there were design faults in the structure of the ship itself which greatly increased the probability of the ship sinking in case of the eventuality of significant damage to the hull. The particular design faults concern the transverse bulkheads which were not high enough to prevent water spilling over from allegedly watertight compartments, eventually causing the ship to sink. Fourthly, the Board of Trade regulations which stipulated the numbers of lifeboats that a passenger steamer was obliged to carry had not been updated to deal with oceangoing steamers as large as the Titanic. Under the regulations, all British registered vessels more than 10,000 tons displacement had to have 16 lifeboats with a capacity of 5,500 cubic feet together with enough rafts and floats for 75 percent capacity of the lifeboats. Therefore, the Titanic, a ship of 46,000 tons, was not legally required to carry more lifeboats than a vessel of 10,000 tons. The regulations therefore meant that the Titanic had to carry boats only for 962 passengers although she could carry a maximum of 3,547 persons.

The owners of RMS Titanic -the White Star Line- had provided additional capacity to take seating capacity up to 1,176, well in excess of official needs, but this was still only 53 percent of the 2,207 people on board at the time of the disaster. In these circumstances it was inevitable that the death toll would be in four figures.

Manage risk

B10

UNIT SUMMARY

What is the unit about?

This unit is about taking the lead in establishing and operating an effective risk management process across your organisation. This involves systematically identifying, evaluating and prioritising potential risks and communicating information to enable appropriate decisions and actions to be taken. It also involves developing an organisational culture in which individuals are risk aware but are not afraid of taking decision and undertaking activities which involve acceptable levels of risk.

For the purposes of this unit, 'organisation' can mean a self-contained entity such as a private sector company, a charity or a local authority **or** a significant operating unit, with a relative degree of autonomy, within a larger organisation.

Who is the unit for?

The unit is recommended for senior managers.

Links with other units

This unit is linked to a number of units in the overall suite of National Occupational Standards for management and leadership where risk is a factor that needs to be considered in planning and undertaking activities.

Skills

Listed below are the main generic skills which need to be applied in managing risk. These skills are explicit/implicit in the detailed content of the unit and are listed here as additional information.

- Evaluating
- Reviewing
- Consulting
- Presenting information
- Decision-making
- Monitoring
- Communicating
- Influencing and persuading
- Leadership
- Contingency planning
- Prioritising
- Planning
- Scenario building
- Information management
- Involving others
- Thinking systematically

Providing direction

Manage risk

B10

OUTCOMES OF EFFECTIVE PERFORMANCE

You must be able to do the following:

1 Ensure that your organisation has a written risk management policy, including setting out responsibilities for risk management, which is clearly communicated across the organisation and to other relevant parties.

2 Establish, and periodically review, risk criteria for your organisation, seeking and taking account of the views of relevant people across the organisation and stakeholders.

3 Evaluate significant current and planned organisational activities and identify potential risks, the nature of the risks, the probability of occurrence and consequences.

4 Produce a risk profile for your organisation and, taking account of the organisation's risk criteria and other relevant information, prioritise the identified risks.

5 Communicate information on identified risks to relevant people across the organisation and, where appropriate, to stakeholders, to enable decisions and actions to be taken in terms of accepting or treating the risks.

6 Collect and evaluate information from across the organisation on how identified risks have been or are being dealt with, including contingency plans which have been put in place.

7 Develop an organisational culture in which people are risk aware but are prepared to take acceptable risks and to make and learn from mistakes.

8 Ensure that there is senior management commitment to the risk management process.

9 Ensure that sufficient resources are allocated across the organisation to support and enable effective risk management.

10 Monitor and review the effectiveness of the risk management process in your organisation, identifying potential improvements and making changes where necessary.

BEHAVIOURS WHICH UNDERPIN EFFECTIVE PERFORMANCE

1 You constantly seek to improve performance.

2 You show sensitivity to stakeholders' needs and interests and manage them effectively.

3 You identify people's information needs.

4 You identify the implications or consequences of a situation.

5 You use communication styles that are appropriate to different people and situations.

6 You balance risks against the benefits that may arise from taking risks.

7 You comply with, and ensure others comply with, legal requirements, industry regulations, organisational policies and professional codes.

8 You are vigilant for potential risks and hazards.

9 You take personal responsibility for making things happen.

10 You balance agendas and build consensus.

11 You create a sense of common purpose.

Providing direction

Manage risk

B10

KNOWLEDGE AND UNDERSTANDING

You need to know and understand the following:

General knowledge and understanding

1 Types of risk and the factors which drive different types of risk.
2 Key stages in the risk management process.
3 The importance of protecting the interests of stakeholders and how to identify their views in relation to risk.
4 The importance of showing senior management commitment to risk management.
5 How to develop a written risk management policy and what it should cover.
6 How to communicate the written risk management policy to people who work for the organisation and other relevant parties.
7 How and when to revise the written risk management policy including taking views from across the organisation and other relevant parties.
8 What risk criteria might cover and the importance of seeking and taking account of the views of relevant people across the organisation and stakeholders.
9 How and where to identify current and planned organisational activities.
10 Ways of identifying and clearly describing potential risks in relation to current and planned activities, the nature of the risks, the probability of occurrence and consequences.
11 Why it is important and how to communicate information on identified risks to relevant people across the organisation and, where appropriate, to stakeholders.
12 The type of decisions and actions that might be taken in relation to identified risks.
13 Why it is important and how to collect and evaluate information on how identified risks have been or are being dealt with, including contingency plans.
14 Ways of developing an organisational culture in which people are risk aware but are prepared to take acceptable risks in undertaking activities.
15 The type of resources required to raise risk awareness across the organisation and with stakeholders and implement the risk management policy effectively.
16 How to establish effective systems for monitoring the risk management process of an organisation.

Industry/sector specific knowledge and understanding

1 The sector(s) in which your organisation operates
2 Sector-specific legislation, regulations, guidelines and codes of practice.
3 Current and emerging political, economic, social, technological, legal and environmental) developments in the sectors(s) in which your organisation operates.
4 Typical risks encountered in the sector(s) in which your organisation operates.

Context specific knowledge and understanding

1 The vision, values, objectives and plans of your organisation.
2 Your organisation's products and services.
3 Other relevant parties with an interest in risk management in your organisation.
4 Mechanisms for consulting with and the views of relevant people across the organisation and stakeholders in relation to risk.
5 The written risk management policy of the organisation, including allocated responsibilities for risk management, and how it is communicated to people who work for the organisation and to other relevant parties.
6 Risk criteria of your organisation.
7 Significant current and planned organisational activities and the related potential risks, including probability of occurrence and consequences.
8 The risk profile of your organisation and prioritised risks.
9 Relevant people across the organisation and, where appropriate, stakeholders, to whom information on identified potential risks should be communicated.
10 Decisions and actions taken across the organisation in relation to identified potential risks, including any contingency plans which have been put in place.
11 Your organisation's culture in relation to risk.
12 How senior management's commitment to risk management has been demonstrated.
13 Resources made available across the organisation to support risk management.
14 Systems in place for monitoring and reviewing the effectiveness of the risk management process in your organisation.
15 Identified improvements and changes made to the risk management process in your organisation.

A Risk Management Standard

IRM

airmic

ALARM
MANAGING RISK

Published by AIRMIC, ALARM, IRM: 2002

Introduction

This Risk Management Standard is the result of work by a team drawn from the major risk management organisations in the UK - The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and ALARM The National Forum for Risk Management in the Public Sector.

In addition, the team sought the views and opinions of a wide range of other professional bodies with interests in risk management, during an extensive period of consultation.

Risk management is a rapidly developing discipline and there are many and varied views and descriptions of what risk management involves, how it should be conducted and what it is for. Some form of standard is needed to ensure that there is an agreed:

- *terminology related to the words used*
- *process by which risk management can be carried out*
- *organisation structure for risk management*
- *objective for risk management*

Importantly, the standard recognises that risk has both an upside and a downside.

Risk management is not just something for corporations or public organisations, but for any activity whether short or long term. The benefits and opportunities should be viewed not just in the context of the activity itself but in relation to the many and varied stakeholders who can be affected.

There are many ways of achieving the objectives of risk management and it would be impossible to try to set them all out in a single document. Therefore it was never intended to produce a prescriptive standard which would have led to a box ticking approach nor to establish a certifiable process. By meeting the various component parts of this standard, albeit in different ways, organisations will be in a position to report that they are in compliance. The standard represents best practice against which organisations can measure themselves.

The standard has wherever possible used the terminology for risk set out by the International Organization for Standardization (ISO) in its recent document ISO/IEC Guide 73 Risk Management - Vocabulary - Guidelines for use in standards.

In view of the rapid developments in this area the authors would appreciate feedback from organisations as they put the standard into use (addresses to be found on the back cover of this Guide). It is intended that regular modifications will be made to the standard in the light of best practice.

1. Risk

Risk can be defined as the combination of the probability of an event and its consequences (ISO/IEC Guide 73).

In all types of undertaking, there is the potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside).

Risk Management is increasingly recognised as being concerned with both positive and negative aspects of risk. Therefore this standard considers risk from both perspectives.

In the safety field, it is generally recognised that consequences are only negative and therefore the management of safety risk is focused on prevention and mitigation of harm.

2. Risk Management

Risk management is a central part of any organisation's strategic management. It is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.

The focus of good risk management is the identification and treatment of these risks. Its objective is to add maximum sustainable value to all the activities of the organisation. It marshals the understanding of the potential upside and downside of all those factors which can affect the organisation. It increases the probability of success, and reduces both the probability of failure and the uncertainty of achieving the organisation's overall objectives.

Risk management should be a continuous and developing process which runs throughout the organisation's strategy and the implementation of that strategy. It should address methodically all the risks surrounding the organisation's activities past, present and in particular, future.

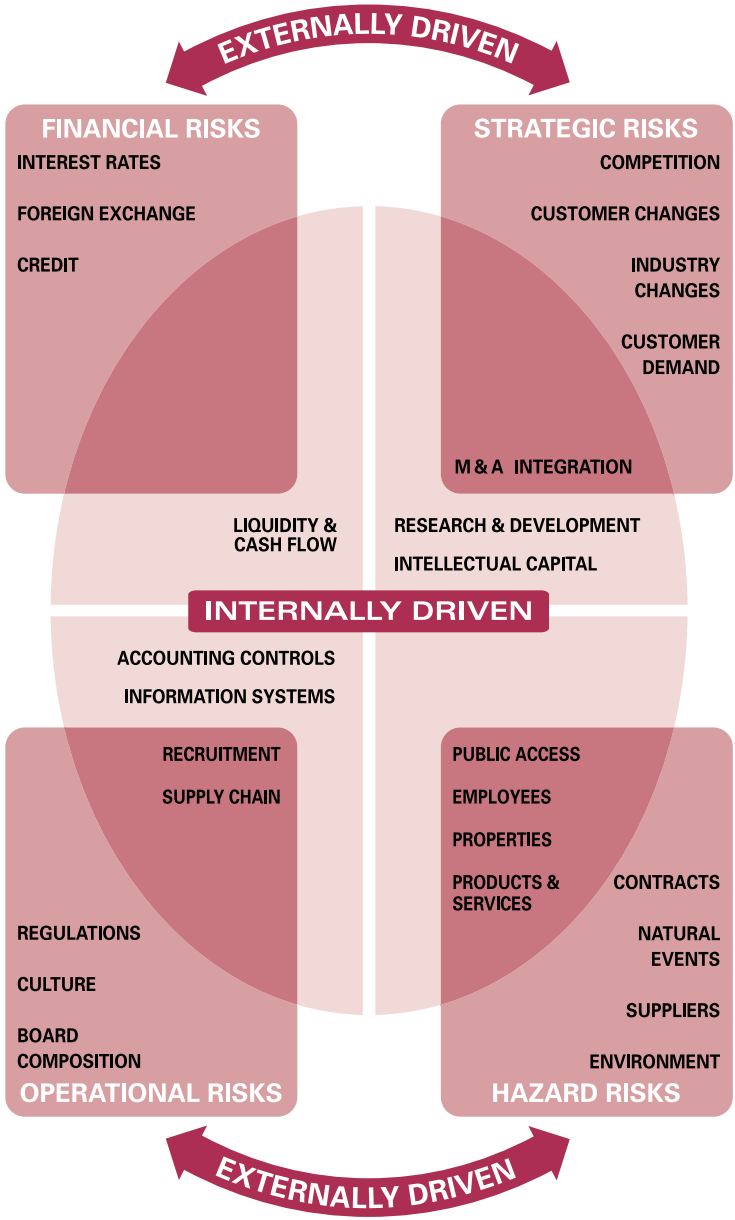
It must be integrated into the culture of the organisation with an effective policy and a programme led by the most senior management. It must translate the strategy into tactical and operational objectives, assigning responsibility throughout the organisation with each manager and employee responsible for the management of risk as part of their job description. It supports accountability, performance measurement and reward, thus promoting operational efficiency at all levels.

2.1 External and Internal Factors

The risks facing an organisation and its operations can result from factors both external and internal to the organisation.

The diagram overleaf summarises examples of key risks in these areas and shows that some specific risks can have both external and internal drivers and therefore overlap the two areas. They can be categorised further into types of risk such as strategic, financial, operational, hazard, etc.

2.1 Examples of the Drivers of Key Risks



2.2 The Risk Management Process

Risk management protects and adds value to the organisation and its stakeholders through supporting the organisation's objectives by:

- *providing a framework for an organisation that enables future activity to take place in a consistent and controlled manner*
- *improving decision making, planning and prioritisation by comprehensive and structured understanding of business activity, volatility and project opportunity/threat*
- *contributing to more efficient use/allocation of capital and resources within the organisation*
- *reducing volatility in the non essential areas of the business*
- *protecting and enhancing assets and company image*
- *developing and supporting people and the organisation's knowledge base*
- *optimising operational efficiency*

3. Risk Assessment

Risk Assessment is defined by the ISO / IEC Guide 73 as the overall process of **risk analysis** and **risk evaluation**. *(See appendix)*

4. Risk Analysis

4.1 Risk Identification

Risk identification sets out to identify an organisation's exposure to uncertainty. This requires an intimate knowledge of the organisation, the market in which it operates, the legal, social, political and cultural environment in which it exists, as well as the development of a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

Risk identification should be approached in a methodical way to ensure that all significant activities within the organisation have been identified and all the risks flowing from these activities defined. All associated volatility related to these activities should be identified and categorised.

Business activities and decisions can be classified in a range of ways, examples of which include:

- *Strategic - These concern the long-term strategic objectives of the organisation. They can be affected by such areas as capital availability, sovereign and political risks, legal and regulatory changes, reputation and changes in the physical environment.*
- *Operational - These concern the day-to-day issues that the organisation is confronted with as it strives to deliver its strategic objectives.*
- *Financial - These concern the effective management and control of the finances of the organisation and the effects of external factors such as availability of credit, foreign exchange rates, interest rate movement and other market exposures.*
- *Knowledge management - These concern the effective management and control of the knowledge resources, the production, protection and communication thereof. External factors might include the unauthorised use or abuse of intellectual property, area power failures, and competitive technology. Internal factors might be system malfunction or loss of key staff.*
- *Compliance - These concern such issues as health & safety, environmental, trade descriptions, consumer protection, data protection, employment practices and regulatory issues.*

Whilst risk identification can be carried out by outside consultants, an in-house approach with well communicated, consistent and co-ordinated processes and tools (see Appendix, page 14) is likely to be more effective. In-house 'ownership' of the risk management process is essential.

4.2 Risk Description

The objective of risk description is to display the identified risks in a structured format, for example, by using a table. The risk description table overleaf can be used to facilitate the description and assessment

of risks. The use of a well designed structure is necessary to ensure a comprehensive risk identification, description and assessment process. By considering the consequence and probability of each of the risks set out in the table, it should be possible to prioritise the key risks that need to be analysed in more detail. Identification of the risks associated with business activities and decision making may be categorised as strategic, project/tactical, operational. It is important to incorporate risk management at the conceptual stage of projects as well as throughout the life of a specific project.

4.2.1 Table - Risk Description

1. Name of Risk	
2. Scope of Risk	Qualitative description of the events, their size, type, number and dependencies
3. Nature of Risk	Eg. strategic, operational, financial, knowledge or compliance
4. Stakeholders	Stakeholders and their expectations
5. Quantification of Risk	Significance and Probability
6. Risk Tolerance/ Appetite	Loss potential and financial impact of risk Value at risk Probability and size of potential losses/gains Objective(s) for control of the risk and desired level of performance
7. Risk Treatment & Control Mechanisms	Primary means by which the risk is currently managed Levels of confidence in existing control Identification of protocols for monitoring and review
8. Potential Action for Improvement	Recommendations to reduce risk
9. Strategy and Policy Developments	Identification of function responsible for developing strategy and policy

4.3 Risk Estimation

Risk estimation can be quantitative, semi-quantitative or qualitative in terms of the probability of occurrence and the possible consequence.

For example, consequences both in terms of threats (downside risks) and opportunities (upside risks) may be high, medium or low (see table 4.3.1). Probability may be high, medium or low but requires different definitions in respect of threats and opportunities (see tables 4.3.2 and 4.3.3).

Examples are given in the tables overleaf. Different organisations will find that different measures of consequence and probability will suit their needs best.

For example many organisations find that assessing consequence and probability as high, medium or low is quite adequate for their needs and can be presented as a 3 x 3 matrix.

Other organisations find that assessing consequence and probability using a 5 x 5 matrix gives them a better evaluation.

Table 4.3.1 Consequences - Both Threats and Opportunities

High	Financial impact on the organisation is likely to exceed £x Significant impact on the organisation's strategy or operational activities Significant stakeholder concern
Medium	Financial impact on the organisation likely to be between £x and £y Moderate impact on the organisation's strategy or operational activities Moderate stakeholder concern
Low	Financial impact on the organisation likely to be less that £y Low impact on the organisation's strategy or operational activities Low stakeholder concern

Table 4.3.2 Probability of Occurrence - Threats

Estimation	Description	Indicators
High (Probable)	Likely to occur each year or more than 25% chance of occurrence.	Potential of it occurring several times within the time period (for example - ten years). Has occurred recently.
Medium (Possible)	Likely to occur in a ten year time period or less than 25% chance of occurrence.	Could occur more than once within the time period (for example - ten years). Could be difficult to control due to some external influences. Is there a history of occurrence?
Low (Remote)	Not likely to occur in a ten year period or less than 2% chance of occurrence.	Has not occurred. Unlikely to occur.

Table 4.3.3 Probability of Occurrence - Opportunities

Estimation	Description	Indicators
High (Probable)	Favourable outcome is likely to be achieved in one year or better than 75% chance of occurrence.	Clear opportunity which can be relied on with reasonable certainty, to be achieved in the short term based on current management processes.
Medium (Possible)	Reasonable prospects of favourable results in one year of 25% to 75% chance of occurrence.	Opportunities which may be achievable but which require careful management. Opportunities which may arise over and above the plan.
Low (Remote)	Some chance of favourable outcome in the medium term or less than 25% chance of occurrence.	Possible opportunity which has yet to be fully investigated by management. Opportunity for which the likelihood of success is low on the basis of management resources currently being applied.

4.4 Risk Analysis methods and techniques

A range of techniques can be used to analyse risks. These can be specific to upside or downside risk or be capable of dealing with both. (See Appendix, page 14, for examples).

4.5 Risk Profile

The result of the risk analysis process can be used to produce a risk profile which gives a significance rating to each risk and provides a tool for prioritising risk treatment efforts. This ranks each identified risk so as to give a view of the relative importance.

This process allows the risk to be mapped to the business area affected, describes the primary control procedures in place and indicates areas where the level of risk control investment might be increased, decreased or reapportioned.

Accountability helps to ensure that 'ownership' of the risk is recognised and the appropriate management resource allocated.

5. Risk Evaluation

When the risk analysis process has been completed, it is necessary to compare the estimated risks against risk criteria which the organisation has established. The risk criteria may include associated costs and benefits, legal requirements, socio-economic and environmental factors, concerns of stakeholders, etc. Risk evaluation therefore, is used to make decisions about the significance of risks to the organisation and whether each specific risk should be accepted or treated.

6. Risk Reporting and Communication

6.1 Internal Reporting

Different levels within an organisation need different information from the risk management process.

The Board of Directors should:

- *know about the most significant risks facing the organisation*
- *know the possible effects on shareholder value of deviations to expected performance ranges*
- *ensure appropriate levels of awareness throughout the organisation*
- *know how the organisation will manage a crisis*
- *know the importance of stakeholder confidence in the organisation*
- *know how to manage communications with the investment community where applicable*
- *be assured that the risk management process is working effectively*
- *publish a clear risk management policy covering risk management philosophy and responsibilities*

Business Units should:

- *be aware of risks which fall into their area of responsibility, the possible impacts these may have on other areas and the consequences other areas may have on them*
- *have performance indicators which allow them to monitor the key business and financial activities, progress towards objectives and identify developments which require intervention (e.g. forecasts and budgets)*
- *have systems which communicate variances in budgets and forecasts at appropriate frequency to allow action to be taken*
- *report systematically and promptly to senior management any perceived new risks or failures of existing control measures*

Individuals should:

- *understand their accountability for individual risks*
- *understand how they can enable continuous improvement of risk management response*
- *understand that risk management and risk awareness are a key part of the organisation's culture*
- *report systematically and promptly to senior management any perceived new risks or failures of existing control measures*

6.2 External Reporting

A company needs to report to its stakeholders on a regular basis setting out its risk management policies and the effectiveness in achieving its objectives.

Increasingly stakeholders look to organisations to provide evidence of effective management of the organisation's non-financial performance in such areas as community affairs, human rights, employment practices, health and safety and the environment.

Good corporate governance requires that companies adopt a methodical approach to risk management which:

- *protects the interests of their stakeholders*
- *ensures that the Board of Directors discharges its duties to direct strategy, build value and monitor performance of the organisation*
- *ensures that management controls are in place and are performing adequately*

The arrangements for the formal reporting of risk management should be clearly stated and be available to the stakeholders.

The formal reporting should address:

- *the control methods - particularly management responsibilities for risk management*
- *the processes used to identify risks and how they are addressed by the risk management systems*
- *the primary control systems in place to manage significant risks*
- *the monitoring and review system in place*

Any significant deficiencies uncovered by the system, or in the system itself, should be reported together with the steps taken to deal with them.

7. Risk Treatment

Risk treatment is the process of selecting and implementing measures to modify the risk. Risk treatment includes as its major element, risk control/mitigation, but extends further to, for example, risk avoidance, risk transfer, risk financing, etc.

NOTE: In this standard, risk financing refers to the mechanisms (eg insurance programmes) for funding the financial consequences of risk. Risk financing is not generally considered to be the provision of funds to meet the cost of implementing risk treatment (as defined by ISO/IEC Guide 73; see page 17).

Any system of risk treatment should provide as a minimum:

- *effective and efficient operation of the organisation*
- *effective internal controls*
- *compliance with laws and regulations.*

The risk analysis process assists the effective and efficient operation of the organisation by identifying those risks which require attention by management. They will need to prioritise risk control actions in terms of their potential to benefit the organisation.

Effectiveness of internal control is the degree to which the risk will either be eliminated or reduced by the proposed control measures.

Cost effectiveness of internal control relates to the cost of implementing the control compared to the risk reduction benefits expected.

The proposed controls need to be measured in terms of potential economic effect if no action is taken versus the cost of the proposed action(s) and invariably require more detailed information and assumptions than are immediately available.

Firstly, the cost of implementation has to be established. This has to be calculated with some accuracy since it quickly becomes the baseline against which cost effectiveness is measured. The loss to be expected if no action is taken must also be estimated and by comparing the results, management can decide whether or not to implement the risk control measures.

Compliance with laws and regulations is not an option. An organisation must understand the applicable laws and must implement a system of controls to achieve compliance. There is only occasionally some flexibility where the cost of reducing a risk may be totally disproportionate to that risk.

One method of obtaining financial protection against the impact of risks is through risk financing which includes insurance. However, it should be recognised that some losses or elements of a loss will be uninsurable eg the uninsured costs associated with work-related health, safety or environmental incidents, which may include damage to employee morale and the organisation's reputation.

8. Monitoring and Review of the Risk Management Process

Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place. Regular audits of policy and standards compliance should be carried out and standards performance reviewed to identify opportunities for improvement. It should be remembered that organisations are dynamic and operate in dynamic environments. Changes in the organisation and the environment in which it operates must be identified and appropriate modifications made to systems.

The monitoring process should provide assurance that there are appropriate controls in place for the organisation's activities and that the procedures are understood and followed.

Changes in the organisation and the environment in which it operates must be identified and appropriate changes made to systems.

Any monitoring and review process should also determine whether:

- *the measures adopted resulted in what was intended*
- *the procedures adopted and information gathered for undertaking the assessment were appropriate*
- *improved knowledge would have helped to reach better decisions and identify what lessons could be learned for future assessments and management of risks*

9. The Structure and Administration of Risk Management

9.1 Risk Management Policy

An organisation's risk management policy should set out its approach to and appetite for risk and its approach to risk management. The policy should also set out responsibilities for risk management throughout the organisation.

Furthermore, it should refer to any legal requirements for policy statements eg. for Health and Safety.

Attaching to the risk management process is an integrated set of tools and techniques for use in the various stages of the business process. To work effectively, the risk management process requires:

- *commitment from the chief executive and executive management of the organisation*
- *assignment of responsibilities within the organisation*
- *allocation of appropriate resources for training and the development of an enhanced risk awareness by all stakeholders.*

9.2 Role of the Board

The Board has responsibility for determining the strategic direction of the organisation and for creating the environment and the structures for risk management to operate effectively.

This may be through an executive group, a non-executive committee, an audit committee or such other function that suits the organisation's way of operating and is capable of acting as a 'sponsor' for risk management.

The Board should, as a minimum, consider, in evaluating its system of internal control:

- *the nature and extent of downside risks acceptable for the company to bear within its particular business*
- *the likelihood of such risks becoming a reality*
- *how unacceptable risks should be managed*
- *the company's ability to minimise the probability and impact on the business*
- *the costs and benefits of the risk and control activity undertaken*
- *the effectiveness of the risk management process*
- *the risk implications of board decisions*

9.3 Role of the Business Units

This includes the following:

- *the business units have primary responsibility for managing risk on a day-to-day basis*
- *business unit management is responsible for promoting risk awareness within their operations; they should introduce risk management objectives into their business*
- *risk management should be a regular management-meeting item to allow consideration of exposures and to reprioritise work in the light of effective risk analysis*
- *business unit management should ensure that risk management is incorporated at the conceptual stage of projects as well as throughout a project*

9.4 Role of the Risk Management Function

Depending on the size of the organisation the risk management function may range from a single risk champion, a part time risk manager, to a full scale risk management department. The role of the Risk Management function should include the following:

- *setting policy and strategy for risk management*
- *primary champion of risk management at strategic and operational level*
- *building a risk aware culture within the organisation including appropriate education*
- *establishing internal risk policy and structures for business units*
- *designing and reviewing processes for risk management*
- *co-ordinating the various functional activities which advise on risk management issues within the organisation*
- *developing risk response processes, including contingency and business continuity programmes*
- *preparing reports on risk for the board and the stakeholders*

9.5 Role of Internal Audit

The role of Internal Audit is likely to differ from one organisation to another. In practice, Internal Audit's role may include some or all of the following:

- *focusing the internal audit work on the significant risks, as identified by management, and auditing the risk management processes across an organisation*
- *providing assurance on the management of risk*
- *providing active support and involvement in the risk management process*
- *facilitating risk identification/assessment and educating line staff in risk management and internal control*
- *co-ordinating risk reporting to the board, audit committee, etc*

In determining the most appropriate role for a particular organisation, Internal Audit should ensure that the professional requirements for independence and objectivity are not breached.

9.6 Resources and Implementation

The resources required to implement the organisation's risk management policy should be clearly established at each level of management and within each business unit.

In addition to other operational functions they may have, those involved in risk management should have their roles in co-ordinating risk management policy/strategy clearly defined. The same clear definition is also required for those involved in the audit and review of internal controls and facilitating the risk management process.

Risk management should be embedded within the organisation through the strategy and budget processes. It should be highlighted in induction and all other training and development as well as within operational processes e.g. product/service development projects.

10. Appendix

Risk Identification Techniques - examples

- *Brainstorming*
- *Questionnaires*
- *Business studies which look at each business process and describe both the internal processes and external factors which can influence those processes*
- *Industry benchmarking*
- *Scenario analysis*
- *Risk assessment workshops*
- *Incident investigation*
- *Auditing and inspection*
- *HAZOP (Hazard & Operability Studies)*

Risk Analysis Methods and Techniques - examples

Upside risk

- *Market survey*
- *Prospecting*
- *Test marketing*
- *Research and Development*
- *Business impact analysis*

Both

- *Dependency modelling*
- *SWOT analysis (Strengths, Weaknesses, Opportunities, Threats)*
- *Event tree analysis*
- *Business continuity planning*
- *BPEST (Business, Political, Economic, Social, Technological) analysis*
- *Real Option Modelling*
- *Decision taking under conditions of risk and uncertainty*
- *Statistical inference*
- *Measures of central tendency and dispersion*
- *PESTLE (Political Economic Social Technical Legal Environmental)*

Downside risk

- *Threat analysis*
- *Fault tree analysis*
- *FMEA (Failure Mode & Effect Analysis)*

The Institute of Risk Management
Telephone 020 7709 9808

6 Lloyd's Avenue,
London EC3N 3AX
Facsimile 020 7709 0716
Email enquiries@theIRM.org
www.theirm.org

ALARM The National Forum for Risk Management in the Public Sector
Telephone 01395 223399

Queens Drive, Exmouth
Devon, EX8 2AY
Facsimile 01395 223304
Email admin@alarm.uk.com
www.alarm-uk.com

The Association of Insurance and Risk Managers
Telephone 020 7480 7610

6 Lloyd's Avenue,
London EC3N 3AX
Facsimile 020 7702 3752
Email enquiries@airmic.co.uk
www.airmic.com

THAMES VALLEY UNIVERSITY
RISK MANAGEMENT POLICY

Definitions:

Thames Valley University - "The Institution"

Thames Valley University's Risk Management Policy - "The Policy"

Purpose of this document

1. The policy forms part of the institution's internal control and corporate governance arrangements.

2. The policy explains the institution's underlying approach to risk management, documents the roles and responsibilities of the Board of Governors, the senior management team, and other key parties. It also outlines key aspects of the risk management process, and identifies the main reporting procedures.

3. In addition, it describes the process the Board of Governors will use to evaluate the effectiveness of the institution's internal control procedures.

Underlying approach to risk management

4. The following key principles outline the institution's approach to risk management and internal control:

- the Board of Governors has responsibility for overseeing risk management within the institution as a whole

- an open and receptive approach to solving risk problems is adopted by the Board of Governors

- the Vice-Chancellor and the senior management team supports, advises and implements policies approved by the Board of Governors

- the institution makes conservative and prudent recognition and disclosure of the financial and non-financial implications of risks

- Pro Vice Chancellor Deans and Head and Directors of all departments are responsible for encouraging good risk management practice within their faculties and departments

- key risk indicators will be identified by the Board of Governors acting on the advice of the Vice Chancellor and closely monitored on a regular basis.

Role of the Board of Governors

5. The Board of Governors has a fundamental role to play in the management of risk. Its role is to:

    a. Set the tone and influence the culture of risk management within the institution. This includes:

        - determining whether the institution is 'risk taking' or 'risk averse' as a whole or on any relevant individual issue
        - determining what types of risk are acceptable and which are not
        - setting the standards and expectations of staff with respect to conduct and probity.

    b. Determine the appropriate risk appetite or level of exposure for the institution.

    c. Approve major decisions affecting the institution's risk profile or exposure.

    d. Monitor the management of fundamental risks to reduce the likelihood of unwelcome surprises.

e. Satisfy itself that the less fundamental risks are being actively managed, with the appropriate controls in place and working effectively.

f. Annually review the institution's approach to risk management and approve changes or improvements to key elements of its processes and procedures.

Role of the senior management team

6. Key roles of the senior management team are to:

a. Implement policies on risk management and internal control.

b. Identify and evaluate the fundamental risks faced by the institution for consideration by the Board of Governors.

c. Provide adequate information in a timely manner to the Board of Governors and its committees on the status of risks and controls.

d. Undertake an annual review of effectiveness of the system of internal control and provide a report to the Board of Governors.

Risk management as part of the system of internal control

7. The system of internal control incorporates risk management. This system encompasses a number of elements that together facilitate an effective and efficient operation, enabling the institution to respond to a variety of operational, financial, and commercial risks. These elements include:

a. Policies and procedures.

Attached to fundamental risks are a series of policies that underpin the internal control process. The policies are set by the Board of Governors and implemented and communicated by senior management to staff. Written procedures support the policies where appropriate.

b. Reporting.

Comprehensive reporting is designed to monitor key risks and their controls. Decisions to rectify problems are made at regular meetings of the senior management team and the Board of Governors if appropriate.

c. Business planning and budgeting.

The business planning and budgeting process is used to set objectives, agree action plans, and allocate resources. Progress towards meeting business plan objectives is monitored regularly.

d. High level risk framework (fundamental risks only).

This framework is compiled by the senior management team and helps to facilitate the identification, assessment and ongoing monitoring of risks fundamental to the institution. The document is formally appraised annually but emerging risks are added as required, and improvement actions and risk indicators are monitored regularly.

e. Faculty risk frameworks.

Heads of faculty develop and use this framework to ensure that fundamental risks in their faculty are identified, assessed and monitored. The document is formally appraised annually but emerging risks are added as required, and improvement actions and risk indicators are monitored regularly by business units.

f. Audit Committee.

The Audit Committee is required to report to the Board of Governors on internal controls and alert governors to any emerging issues. In addition, the committee oversees internal audit,

external audit and management as required in its review of internal controls. The committee is therefore well-placed to provide advice to the board on the effectiveness of the internal control system, including the institution's system for the management of risk.

g. Internal audit programme.

Internal audit is an important element of the internal control process. Apart from its normal programme of work, internal audit is responsible for aspects of the annual review of the effectiveness of the internal control system within the organisation.

h. External audit.

External audit provides feedback to the Audit Committee on the operation of the internal financial controls reviewed as part of the annual audit.

i. Third party reports.

From time to time, the use of external consultants will be necessary in areas such as health and safety, and human resources. The use of specialist third parties for consulting and reporting can increase the reliability of the internal control system.

Annual review of effectiveness

8. The Board of Governors is responsible for reviewing the effectiveness of internal control of the institution, based on information provided by the senior management team. Its approach is outlined below.

9. For each fundamental risk identified, the board will:

- review the previous year and examine the institution's track record on risk management and internal control
- consider the internal and external risk profile of the coming year and consider if current internal control arrangements are likely to be effective.

10. In making its decision the board will consider the following aspects.

a. Control environment:

- the institution's objectives and its financial and non-financial targets
- organisational structure and calibre of the senior management team
- culture, approach, and resources with respect to the management of risk
- delegation of authority
- public reporting.

b. On-going identification and evaluation of fundamental risks:

- timely identification and assessment of fundamental risks
- prioritisation of risks and the allocation of resources to address areas of high exposure.

c. Information and communication:

- quality and timeliness of information on fundamental risks
- time it takes for control breakdowns to be recognised or new risks to be identified.

d. Monitoring and corrective action:

- ability of the institution to learn from its problems
- commitment and speed with which corrective actions are implemented.

11. The senior management team will prepare a report of its review of the effectiveness of the internal control system annually for consideration by the Board of Governors.

RISK MANAGEMENT POLICY

Approved by the Council on 3 July 2003

1. Introduction

The Council is responsible for overseeing risk management within the institution while the Principal's Steering Group implement policy. All senior staff are responsible for encouraging good risk management practice within their areas of responsibility. Key risk indicators will be identified, monitored and reviewed on a regular basis.

The College has adopted the following definition of risk for the purposes of this policy.

> "A risk is anything than can impede or enhance an organisation's ability to meet its current or future objectives"

In developing this policy, the College has agreed that:

- the main risks which present opportunities or hazards to meeting the College's objectives will be explicitly identified and assessed
- a priority among risks will be agreed, and attention focussed on those priorities.
- control systems to cover the risks will be put in place.

2. Roles and Responsibilities

The Council will through the Principal:

- monitor the management of significant risks to ensure that appropriate controls are in place.
- approve major decisions taking into account the College's risk profile or exposure.
- satisfy itself that less significant risks are being actively managed, and that appropriate controls are in place and working effectively to ensure the implementation of policies approved by the Council.
- review annually the College's approach to risk management and approve changes where necessary to key elements of its processes and procedures.
- ensure the implementation of the risk management policy.
- identify and evaluate the significant risks faced by the College for consideration by Council.
- provide adequate information for the Council and its committees as appropriate, on the status of risks and controls.
- report annually to the Council on the effectiveness of the system of internal controls.

3. Risk Management as part of the Internal Control System

Internal controls encompass a review of the risks inherent in each activity. The under noted controls are in place:

- Significant risks are identified and evaluated.
- Key risks are monitored by the Planning Review Group which is chaired by the Director of Resources
- Regular reports are made to the Principal's Steering Group and Council as appropriate.
- The business planning and budgetary process is used to set objectives, agree action plans and allocate resources. Progress towards meeting objectives is monitored regularly.
- A framework of significant strategic risks and how they are to be managed is agreed and monitored on an annual basis.
- Regular review of the framework ensures that emerging risks can be added as soon as they are identified.
- Senior Managers are required to identify, monitor and review on a regular basis significant risks in their own areas.
- The Audit Committee reports to the Council on the adequacy and effectiveness of the system of internal controls. As part of its remit the Audit Committee reviews the work of the Internal and External Auditors and of the College's management. The Audit Committee is therefore well placed to advise the Council on the adequacy and effectiveness of the system of internal controls.
- Internal Audit is responsible for some aspect of the Annual Review of the adequacy and effectiveness of the system of internal controls of the College.
- As part of the annual audit, External Audit advises the Audit Committee on the operation of the internal financial controls.

4. Annual Review

The Council will review the effectiveness of the internal control system and in doing so will:

- review the previous year and examine the College's track record on risk management.
- consider the internal and external risk profiles of the coming year.
- consider whether the current internal control arrangements are likely to be effective.

As part of its review, the Council will consider:

- the institutional objectives and its financial and non-financial targets.
- the management approach to risk.
- the appropriateness of the level of delegation of authority .
- prioritisation of risks.
- timely identification and assessment of risks.
- the ability of the institution to learn from its problems and apply its learning.

26.vi.2003
DSC 3125a

Risk Management

Delegates attending the Risk Management workshop may wish to take the opportunity of considering the risks to the business in their own area of responsibility.

The full process for risk identification may involve not only a “top-down” approach from the senior management, but also a “bottom-up” view from employees at all levels. This would normally be achieved through small group meetings and/or individual discussion.

This document provides details of three analytical tools that would more usually be used in more conventional strategic planning. These are the models of Porter’s Five Market Forces, SWOT and PEST analysis.

The checklists in each of these three can provide thought-provoking triggers when considering risks and we suggest that this is how they be used. Run through the points and consider from your industry perspective, and whether you have risks in these areas. At this stage, do not attempt to quantify or prioritise items as this is a later stage in the process.

Bring the results of your deliberations to the workshop.

Porter's Five Forces model

Michael E Porter's five forces of competitive position model and diagrams

Michael Porter's famous Five Forces of Competitive Position model provides a simple perspective for assessing and analysing the competitive strength and position of a corporation or business organization.

American Michael Porter was born in 1947. After initially graduating in aeronautical engineering, Porter achieved an economics doctorate at Harvard, where he was subsequently awarded university professorship, a position he continues to fulfill at Harvard Business School. His research group is based at the Harvard Business School, and separately he co-founded with Mark Kramer the Foundation Strategy Group, 'a mission-driven social enterprise, dedicated to advancing the practice of philanthropy and corporate social investment, through consulting to foundations and corporations'. A prime example of someone operating at a self-actualization level if ever there was one.

After his earlier work on corporate strategy Porter extended the application of his ideas and theories to international economies and the competitive positioning of nations, as featured in his later books. In fact in 1985 Porter was appointed to President Ronald Reagan's Commission on Industrial Competitiveness, which marked the widening of his perspective to national economies. By the 1990's Porter had established a reputation as a strategy guru on the international speaking circuit second only to Tom Peters, and was among the world's highest earning academics.

Porter's first book Competitive Strategy (1980), which he wrote in his thirties, became an international best seller, and is considered by many to be a seminal and definitive work on corporate strategy. The book, which has been published in nineteen languages and re-printed approaching sixty times, changed the way business leaders thought and remains a guide of choice for strategic managers the world over.

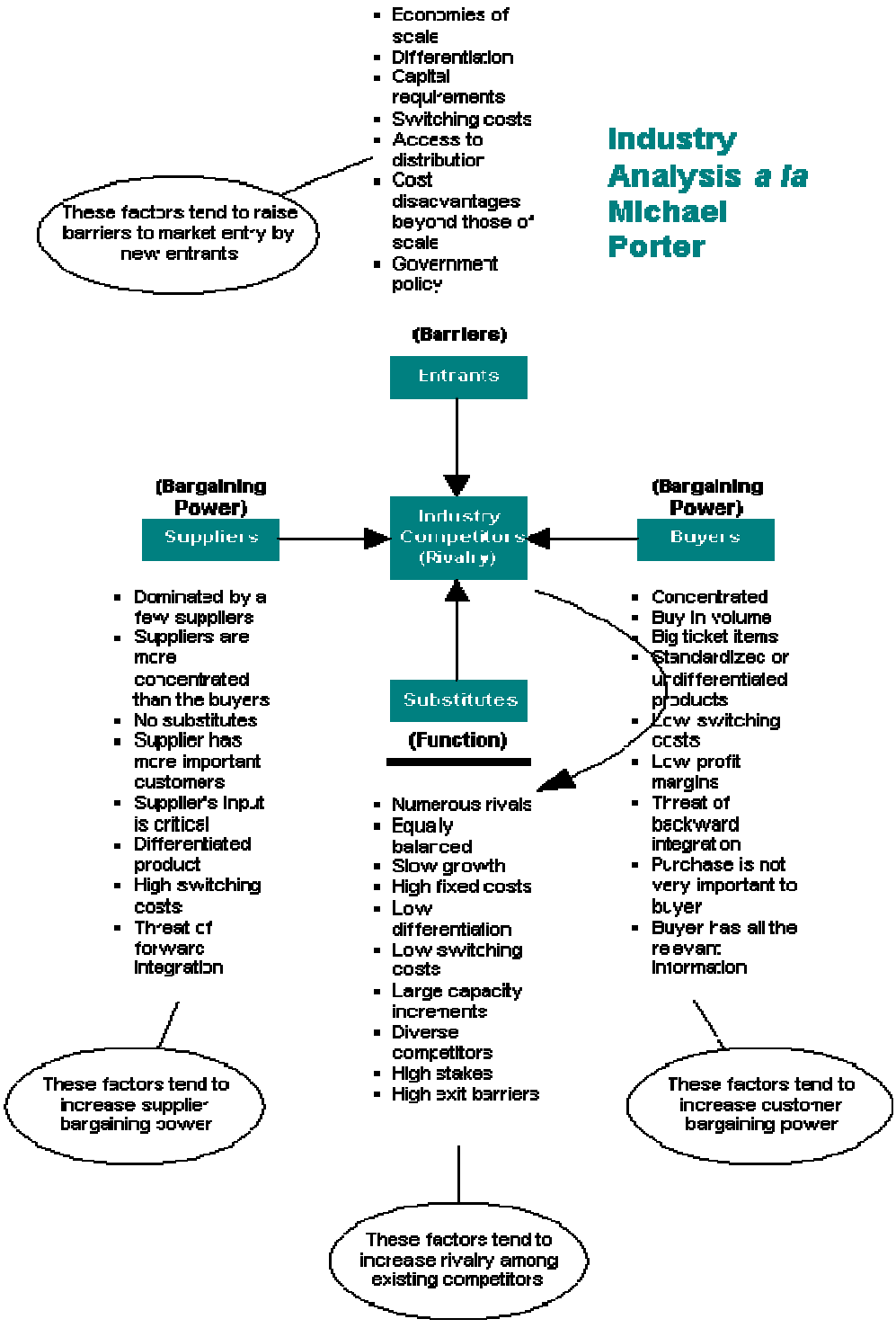
Aside from his innovative thinking, Porter has a special ability to represent complex concepts in relatively easily accessible formats, notably his Five Forces model, in which market factors can be analysed so as to make a strategic assessment of the competitive position of a given supplier in a given market. The five forces that Porter suggests drive competition are:

Porter's Five Forces

1. **Existing competitive rivalry between suppliers**
2. **Threat of new market entrants**

3. **Bargaining power of buyers**
4. **Power of suppliers**
5. **Threat of substitute products (including technology change)**

Typically this five forces model is shown as a series of five boxes in a cross formation, item 1 being central.



Porter's Five Forces model can be used to good analytical effect alongside other models such as the Swot and Pest analysis tools.

Porter's Five Forces model provides suggested points under each main heading, by which you can develop a broad and sophisticated analysis of competitive position, as might be used when creating strategy, plans, or making investment decisions about a business or organization.

Porter is also known for his simple identification of five generic descriptions of industries:

1. **Fragmented** (e.g., shoe repairs, gift shops)
2. **Emerging** (e.g., space travel)
3. **Mature** (e.g., automotive)
4. **Declining** (e.g., solid fuels)
5. **Global** (e.g., micro-processors)

And Porter is also particularly recognised for his competitive 'diamond' model, used for assessing relative competitive strength of nations, and by implication their industries:

1. **Factor Conditions:** production factors required for a given industry, e.g.., skilled labour, logistics and infrastructure.
2. **Demand Conditions:** extent and nature of demand within the nation concerned for the product or service.
3. **Related Industries:** the existence, extent and international competitive strength of other industries in the nation concerned that support or assist the industry in question.
4. **Corporate Strategy, Structure and Rivalry:** the conditions in the home market that affect how corporations are created, managed and grown; the idea being that firms that have to fight hard in their home market are more likely to be able to succeed in international markets.

PEST market analysis tool

PEST analysis method and examples

The PEST analysis is a useful tool for understanding market growth or decline, and as such the position, potential and direction for a business. A PEST analysis is a business measurement tool. PEST is an acronym for Political, Economic, Social and Technological factors, which are used to assess the market for a business or organizational unit. The PEST analysis headings are a framework for reviewing a situation.

A PEST analysis measures a market; a SWOT analysis measures a business unit, a proposition or idea.

N.B. The PEST model is sometimes extended (some would say unnecessarily) to seven factors, by adding Ecological (or Environmental), Legislative (or Legal), and Industry Analysis (the model is then known as PESTELI). Arguably if completed properly, the basic PEST analysis should naturally cover these 'additional' factors: Ecological factors are found under the four main PEST headings; Legislative factors would normally be covered under the Political heading; Industry Analysis is effectively covered under the Economic heading. If you prefer to keep things simple, perhaps use PESTELI only if you are worried about missing something within the three extra headings.

A SWOT analysis measures a business unit or proposition, a PEST analysis measures the market potential and situation, particularly indicating growth or decline, and thereby market attractiveness, business potential, and suitability of access - market potential and 'fit' in other words. PEST analysis uses four perspectives, which give a logical structure, in this case organized by the PEST format, that helps understanding, presentation, discussion and decision-making. The four dimensions are an extension of a basic two heading list of pro's and con's.

PEST analysis can be used for marketing and business development assessment and decision-making, and the PEST template encourages proactive thinking, rather than relying on habitual or instinctive reactions.

Here the PEST analysis template is presented as a grid, comprising four sections, one for each of the PEST headings: Political, Economic, Social and Technological. The free PEST template below includes sample questions or prompts, whose answers are can be inserted into the relevant section of the PEST grid. The questions are examples of discussion points, and obviously can be altered depending on the subject of the PEST analysis, and how you want to use it. Make up your own PEST questions and prompts to suit the issue being analysed and the situation (i.e., the people doing the work and the expectations of them). Like SWOT analysis, it is important to clearly

identify the subject of a PEST analysis, because a PEST analysis is four-way perspective in relation to a particular business unit or proposition - if you blur the focus you will produce a blurred picture - so be clear about the market that you use PEST to analyse.

A market is defined by what is addressing it, be it a product, company, brand, business unit, proposition, idea, etc, so be clear about how you define the market being analysed, particularly if you use PEST analysis in workshops, team exercises or as a delegated task. The PEST subject should be a clear definition of the market being addressed, which might be from any of the following standpoints:

- a company looking at its market
- a product looking at its market
- a brand in relation to its market
- a local business unit
- a strategic option, such as entering a new market or launching a new product
- a potential acquisition
- a potential partnership
- an investment opportunity

Be sure to describe the subject for the PEST analysis clearly so that people contributing to the analysis, and those seeing the finished PEST analysis; properly understand the purpose of the PEST assessment and implications.

PEST analysis template

Other than the four main headings, the questions and issues in the template below are examples and not exhaustive - add your own and amend these prompts to suit your situation, the experience and skill level of whoever is completing the analysis, and what you aim to produce from the analysis.

If Environmental is a more relevant heading than Economic, then substitute it. Ensure you consider the three additional 'PESTELI' headings: Ecological (or Environmental), Legislative (or Legal), and Industry Analysis.

The analysis can be converted into a more scientific measurement by scoring the items in each of the sections. Whether there are established good or bad reference points is for you to decide. Scoring is particularly beneficial if more than one market is being analysed, for the purpose of comparing which market or opportunity holds most potential and/or obstacles. This is useful when considering business development and investment options, i.e., whether to develop market A or B; whether to concentrate on local distribution or export; whether to acquire company X or company Y., etc. If helpful when comparing more than one different market analysis, scoring can also be weighted according to the more or less significant factors.

Subject of PEST analysis: (define the standpoint and market here)

political

- ecological/environmental issues
- current legislation home market
- future legislation
- European/international legislation
- regulatory bodies and processes
- government policies
- government term and change
- trading policies
- funding, grants and initiatives
- home market lobbying/pressure groups
- international pressure groups

economic

- home economy situation
- home economy trends
- overseas economies and trends
- general taxation issues
- taxation specific to product/services
- seasonality/weather issues
- market and trade cycles
- specific industry factors
- market routes and distribution trends
- customer/end-user drivers
- interest and exchange rates

social

- lifestyle trends
- demographics
- consumer attitudes and opinions
- media views
- law changes affecting social factors
- brand, company, technology image
- consumer buying patterns
- fashion and role models
- major events and influences
- buying access and trends
- ethnic/religious factors
- advertising and publicity

technological

- competing technology development
- research funding
- associated/dependent technologies
- replacement technology/solutions
- maturity of technology
- manufacturing maturity and capacity
- information and communications
- consumer buying mechanisms/technology
- technology legislation
- innovation potential
- technology access, licencing, patents
- intellectual property issues

SWOT analysis

SWOT analysis method and examples

The SWOT analysis is an extremely useful tool for understanding and decision-making for all sorts of situations in business and organizations. SWOT is an acronym for Strengths, Weaknesses, Opportunities, Threats. The SWOT analysis headings provide a good framework for reviewing strategy, position and direction of a company or business proposition, or any idea.

A SWOT analysis measures a business unit, a proposition or idea; a PEST analysis measures a market.

A SWOT analysis is a subjective assessment of data which is organized by the SWOT format into a logical order that helps understanding, presentation, discussion and decision-making. The four dimensions are a useful extension of a basic two heading list of pro's and con's.

SWOT analysis can be used for all sorts of decision-making, and the SWOT template enables proactive thinking, rather than relying on habitual or instinctive reactions.

The SWOT analysis template is normally presented as a grid, comprising four sections, one for each of the SWOT headings: Strengths, Weaknesses, Opportunities, and Threats. The free SWOT template below includes sample questions, whose answers are inserted into the relevant section of the SWOT grid. The questions are examples, or discussion points, and obviously can be altered depending on the subject of the SWOT analysis. Note that many of the SWOT questions are also talking points for other headings - use them as you find most helpful, and make up your own to suit the issue being analysed. It is important to clearly identify the subject of a SWOT analysis, because a SWOT analysis is a perspective of one thing, be it a company, a product, a proposition, and idea, a method, or option, etc.

Here are some examples of what a SWOT analysis can be used to assess:

- a company (its position in the market, commercial viability, etc)
- a method of sales distribution
- a product or brand
- a business idea
- a strategic option, such as entering a new market or launching a new product
- a opportunity to make an acquisition
- a potential partnership
- changing a supplier
- outsourcing a service, activity or resource
- an investment opportunity
- risk management

Be sure to describe the subject for the SWOT analysis clearly so that people contributing to the analysis, and those seeing the finished SWOT analysis, properly understand the purpose of the SWOT assessment and implications.

SWOT analysis template

Subject of SWOT analysis: (define the subject of the analysis here)

strengths

- Advantages of proposition?
- Capabilities?
- Competitive advantages?
- USP's (unique selling points)?
- Resources, Assets, People?
- Experience, knowledge, data?
- Financial reserves, likely returns?
- Marketing - reach, distribution, awareness?
- Innovative aspects?
- Location and geographical?
- Price, value, quality?
- Accreditations, qualifications, certifications?
- Processes, systems, IT, communications?
- Cultural, attitudinal, behavioural?
- Management cover, succession?

weaknesses

- Disadvantages of proposition?
- Gaps in capabilities?
- Lack of competitive strength?
- Reputation, presence and reach?
- Financials?
- Own known vulnerabilities?
- Timescales, deadlines and pressures?
- Cashflow, start-up cash-drain?
- Continuity, supply chain robustness?
- Effects on core activities, distraction?
- Reliability of data, plan predictability?
- Morale, commitment, leadership?
- Accreditations, etc?
- Processes and systems, etc?
- Management cover, succession?

opportunities

- Market developments?
- Competitors' vulnerabilities?
- Industry or lifestyle trends?
- Technology development and innovation?
- Global influences?
- New markets, vertical, horizontal?
- Niche target markets?
- Geographical, export, import?
- New USP's?
- Tactics - surprise, major contracts, etc?
- Business and product development?
- Information and research?
- Partnerships, agencies, distribution?
- Volumes, production, economies?
- Seasonal, weather, fashion influences?

threats

- Political effects?
- Legislative effects?
- Environmental effects?
- IT developments?
- Competitor intentions - various?
- Market demand?
- New technologies, services, ideas?
- Vital contracts and partners?
- Sustaining internal capabilities?
- Obstacles faced?
- Insurmountable weaknesses?
- Loss of key staff?
- Sustainable financial backing?
- Economy - home, abroad?
- Seasonality, weather effects?