Risk Assessment, Evaluation &Management

Learning Outcomes

By the end of this unit, the learner will be able to

- ✓ describe the objectives of assessing risks.
- ✓ explore Risk-evaluation procedures.
- ✓ examine Risk-response strategies.

Risk Assessment, Evaluation & Management

Introduction

The objective of the risk-assessment stage is to offer an evaluation of the possibility and the impact of risks and opportunities that have been identified. Undertaking the assessment provides several benefits, such as providing an order of pain or gain for each opportunity and risk.

The following three principles are important for assessing risk:

- Ensure that a clearly structured process is in place in which both possibility and impact are considered for each risk;
- Distinguish between residual and inherent risk; and
- Record the risk assessment in a manner that facilitates observing and identifying risk priorities.

In the absence of risk assessment, ask these questions:

- How will a preferred option be selected from many potential solutions?
- How will risk management activities be prioritised?
- How will an organisation decide if it should increase market share through acquisition?
- How will a manager know if it is more economical to transfer a risk to a counterparty or retain it within the organization?
- How will a manager judge whether or not a new market should be entered into?

The risk-assessment process is adequate when it fulfils these subgoals:

- The process was comprehensive and incorporated, to an extent possible, andall the risks in the risk register that were developed in the identify risk stage were evaluated.
- The people involved were those who could make informed and well-reasoned valuations of the risks involved.
- Consistent definitions of impact and probability were adopted.
- Risk-management expertise was available to assist with the assessment.
- The financial banding used for each risk was appropriate and not too broad or open-ended in terms of the upper band if a probability impact matrix was used.
- Adequate time was assigned for the assessment process.

Process

Process Inputs

Inputs to the assessment process may include the following:

Risk Identification

In the identificationstage of risk management, the risks are debated and documented in the risk register.

Risk Register

The risk register is an outcome of the preceding process. The register should contain at least a complete description of the risks and the risk categories, with each risk having a unique reference number. The risks should be listed under the related risk categories. Furthermore, the risk owner and risk manager should be named whenever possible. If deemed useful, the register may include supplementary columns, namely notes to record background information on the risk and impact and to describe the impact of each individual risk on the business.

Profit and Loss Account

The projected profit and loss account has already been discussed. This provides information on the expected profit for a specified period. Low levels of projected profits will expose a company to a number of related risks in terms of business durability and operating practicalities.

Balance Sheet

Similarly, the projected balance sheet should beexamined critically to ensure the reliability of the projections with reference to the validity of the assumptions made and the completeness of the input data. The balance sheet will provide an indication of the vulnerability of a business to bad debts or late payments.

Activities that form the risk assessment process are essential for identification of the possibility of the occurrence of the risks and the impact, if they occur, and should be recorded in the risk log, list or register.

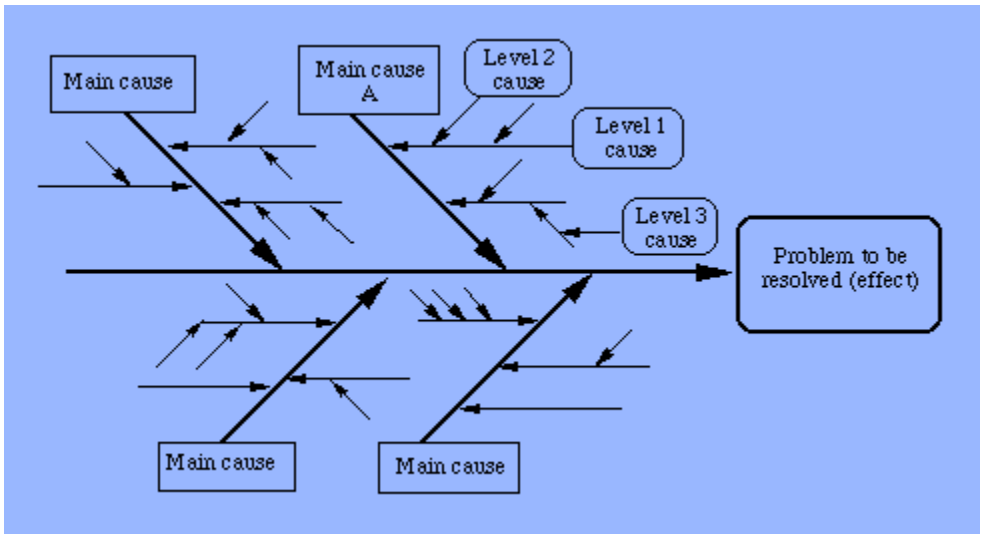
These include:

- Understanding and assessing the probability of the opportunity or risk occurring;
- Evaluating the impact of the opportunity or risk in terms of the project or business objectives;
- Understanding the interdependence between the risks and asking if they would occur sequentially, so that one risk potentially triggers another, concurrently, or in parallel;
- Documenting the findings; and
- Updating the risk log, register or list.

Causal Analysis

Causal analysis exhibits the relation between an effect and its potential causes to get to the basic source of a risk. Its objective is to avert problems by establishing the problem's root cause.

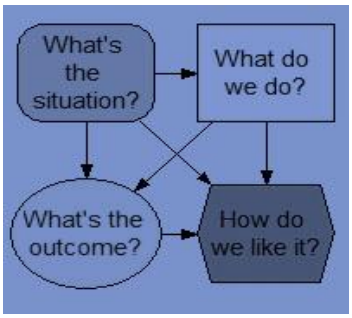
The premise behind causal analysis is that, if a risk or error has occurred once, it could occur again, unless something is done to prevent it. Therefore, learning from past errors averts future errors. One of the techniques for causal analysis is the cause-and-effect diagram. It has no statistical foundation but works in an excellent manner to uncover the sources of risk and plot their relationships. This diagram is also known as a fishbone diagram because its appearance looks like the skeleton of a fish.



Decision Analysis

Decision analysis is used to help structure decisions and represent real-life problems by using models that can be analysed to gain understanding and insights. The elements of a decision model are the uncertain events, decisions and values of outcomes.

Once these decision elements have been identified, a model is created using the influence diagram technique. The term *influence* refers to the reliance of one variable on the level of another variable.



The influence diagram is a formal technique that can be transformed into a comparable decision tree and evaluated further. Common notations are used:

- Squares represent decision nodes.
- Diamonds represent values.
- Circles represent uncertain or chance events.
- Double circles represent those outcomes that are known at the time when inputs are given.

There are several advantages of influence diagrams. First, they provide a framework around which decision makers and experts can discuss the interrelationship of decisions and events and the management of the problem, without requiring any formal statistical, mathematical or probabilistic method. Second, they contribute significantly towards reducing large quantities of data to those statistics which are necessary for decision-making. Third, they provide a degree of sensitivity analysis to demonstrate the extent of the effect that specific decisions or uncertain events have upon the final outcomes.

Pareto Analysis

Pareto analysis is the expression given to the simple process of ranking or ordering risks once they have been evaluated to establish the order in which they should be managed. This technique is used to help management focus its efforts on risks that have the potential of causing the greatest damaging impact on a business or a project's objectives.

The Pareto principle is useful for a variety of problem-solving and continual improvement actions. Here are some examples:

- 80% of complaints are about the same 20% of the services.
- 80% of an equipment budget comes from 20% of the items.
- 80% of benefit comes from the first 20% of effort.
- 80% of the decisions taken in meetings come from 20% of the time spent in the meeting.
- 80% of innovation comes from 20% of the staff.
- 80% of success comes from 20% of the business efforts.
- 20% of customers account for 80% of the sales volume.
- 20% of advertising yields 80% of the campaign results.

By combining Pareto diagrams with EMV calculations, risk significance can be communicated readily to the team involved in the risk analysis for the company.

CAPM Analysis

The capital asset pricing model (CAPM) provides a precise definition of what we mean by risk and also relates the expected return on an asset to its risk. The main concept of the CAPM is that investors can expect a reward for investing in a high-risk profile asset.

Some types of risk can be diagnosed numerically, specifically financial risk. For other kinds of risks, such as reputational risk, it is only possible to make a far more subjective diagnosis. Based on this interpretation, risk assessments are often more of an art than a science. However, it is necessary to develop a framework for assessing risks. To whatever extent possible, the assessment must use unbiased independent evidence, take into consideration the opinions of an entire range of stakeholders affected by the risk and not confuse objective assessment about the acceptability of the risk with objective assessments of the risk.

The likelihood of a risk being realized, as well asthe impact if a risk is realized, must be assessed. A categorisation of *high*, *medium* or l*ow* with respect to each risk may be adequat, and should be the lowest level of categorisation which produces a *3x3* risk matrix. If a more quantitative evaluation can be applied to the particular risk, a more detailed analytical scale may then be appropriate, specifically a*5x5* matrix.Impact will be shown on a scale of *insignificant, minor, moderate, major* or *catastrophic* and probability on a scale of *rare, unlikely, possible, likely* or *almost certain*. No absolute standard exists for the scale used on risk matrices. People should make a decision about which level of analysis would be most practical for the situation. Colour or traffic lights can be used to further clarify the significance of risks.

Information about the inherentrisk should also be captured. This is important so that the company will know what its exposure will be if control measures fail. Information about the inherent risk also leads to better understanding of situations where over-control is taking place. If the inherent risk is within the company's risk appetite, resources may not have to be spent to control that risk. The need to be knowledgeable about both, inherent and residual risk, means that the assessment of risk is a stage in the risk-management process that cannot be separated from addressing risk. The extent to which the risk needs to be addressed is shown by the inherent risk, while the adequacy of the means chosen to address the risk can only be selected once the residual risk has been identified.

Risk-assessment documentation should be performed in such a manner that the stages of the process are recorded. Documenting risk assessments creates a risk profile for the company which

- assists the process of identifying risk priorities, more specifically to identify the most important risk issues that should concern senior management.
- documents the reasons behind decisions about what is and is not acceptable risk exposure.
- facilitates managing and re-evaluation of risks.
- helps document the way that has been selected to address risks.

- provides an overall view of the risk profile for all those concerned with the risk assessment and the particular areas of responsibility that fit into it.

The risk priorities for the company will become apparent once risks have been assessed. The less acceptable the exposure of a risk, the greaterthe priority that should be given to dealing with it. High-priority risks or key risks should receive regular attention by those at the highest level in the company and should also be addressed regularly by the board. The particular risk priorities will change over time as specific risks are dealt with and consequently the prioritisation will change.

A number of well-known techniques can be used to identify the significance of specific risks, for which suitable actions can then be prioritised to manage them. Using a matrix that combines the following factors is a technique that risk experts and commentators commonly use:

- Likelihood: The perceived possibility of the occurrence of the risk
- Impact: The expected consequences if the risk does actually occur

Each specific risk is assigned a rating for each factor, such as *very high*, *high*, *medium*, *low* or *very low*. The combination of those two factors, likelihood and impact, is used to assign an overall risk rating for the specific risk. This approach involves a degree of judgement and is neither a scientific nor mathematical exercise. However, it is important that, as far as possible, the evaluation of risks is done in a methodical way that avoids bias due to perceived personal or commercial interests. By conducting tests within different levels and functions of the company, this objective can be achieved.

The diagram shown below is accepted by risk advisors and helps to set out a possible representation of the assessment of a risk.

While considering the influence of a specific risk, if it occurs, it may be useful to take into consideration the various kinds of consequences that may be involved, instead of the sources of the risk. Keeping in mind the information about the SERM approach, different methods of categorisation might be feasible. The table given below describes two plausible approaches:

Type-of-impact method	Site-of-impact method
Financial: e.g. loss of revenue, impairment of cash flow, or incorrect pricing	Assets: an impact on the assets of the business, whether tangible or intangible
Reputational: e.g. damage to the perceived standing or reputation of the organisation with its stakeholders and the public at large	Business processes: an impact affecting effective functioning or performance of particular systems or processes within the
Operational: e.g. impairment of the organisation's ability to carry out its day-to-day activities organization	Revenue: loss of earned income or cash receipts
Strategic: e.g. impairment of the organisation's ability to meet its strategic objectives	Costs: an increase in cost base or the loss of an opportunity to decrease costs
Legal: e.g. potential liability for claims or loss of ability to enforce rights or claims	People: an impact on the human resources or staff of the organisation

While considering such classifications and approaches compared to other kinds of categorisations, it should always be kept in mind that the classification of kinds of consequences must not be perceived as prescriptive.It is important to adapt them so that they become meaningful for the concerned business.

Risk Evaluation

As its name suggests, the risk-evaluation stage includes the evaluation of the outcomes of the assessment stage. This stage is fundamental for understanding a prospective opportunity that may arise or the likelihood of risk exposure for a business activity. This important step facilitates understanding of the relationship between the individual opportunities and risks, so that, when they are combined, their full net effect is identified. Results from the first set of calculations raise questions about the inputs. Thus, it is highly probable that the previous process will be revisited. In other words, developing the evaluation process is a repetitive process of testing and refining the information acquired during the assessment process and its input into the evaluation process.

The principal goal in the process of risk evaluation is to assess both the opportunities and risks to the organisation in terms of their collective impact on either the entire company or on specific projects. The risk evaluation process will be effective when has fulfilled these subgoals:

- The goal of the aggregation process has been made obvious.
- Any limitations of the aggregation process were recorded and stated along with the results.

- Sufficient time was allotted for the evaluation process.
- Staff members who were involved were able to make informed and well-reasoned evaluations of the relationships between the risks.
- An appropriate and recognised method of aggregation was used.
- People with risk-management expertise assisted in the evaluation;
- Sensitivity analysis can be conducted on the results. This is a model that can be rerun to apply a what-if analysis to evaluate what the outcome would be if any specific figure is changed.
- Assumptions used in the evaluation process were made known.

Risk Register

The output of the risk assessment process is the creation of the risk register. From the risk-identification process, the risk register will contain at least a complete description of the risks and their categories. The risks will be listed under the risk category to which they relate and specific risks will have unique reference numbers. Where possible, the risk owner and risk manager should be identified.

Additional columns for information such as notes can be added to provide background information about each risk.

Risk Planning

The risk evaluation stage is where the opportunities and risks are combined to ascertain their net effect. The planning stage uses all of the information acquired so far to manage the identified opportunities and risks and produce specific responses and action plans to secure the business objectives. This stage is responsible for making sure that these plans are prepared, considered, refined and implemented. Spending time, effort and energy in identifying and assessing the potential opportunities and risks, yet not planning responses to them, would be a poor use of resources.

The mechanisms used can be methods, tools, techniques, or other aids that provide structure to the process activities.

There are two primary process mechanisms:

- resolution strategy; techniques or tools
- risk response flow chart

A resolution strategy is a pre-defined plan intended for responding to a specific, reoccurring risk. A risk-response flowchart illustrates the possible choices that are made to arrive at the desired risk response category. It is an aid in making decisions about whether an appropriate and applicable strategy would be to remove a risk or to transfer it.

Tasks required for transforming a prioritised list of risks into a concrete plan of action for risk resolution is the aim of the risk-planning process.

These tasks comprise the following:

- Where suitable, conduct research into the risk to acquire essential information for making an informed decision about the risk response.
- Develop one or more risk response(s) for each identified opportunity and risk.
- If applicable, develop alternative responses so that the most beneficial option is selected.
- Assess the cost of the response versus the impact of the risk if it occurs.
- Identify the risk owner or the organisation who will maintain ownership of the risk.
- Identify the risk manager or the individual who will ensure that the identified response is implemented.
- Identify the risk actionee or the person who will be responsible for implementing the risk response action previously agreed on with the risk manager.
- Select the time when the responses need to be implemented;
- Define the company's risk appetite.
- Evaluate the possibility of secondary risks arising from the planned risk response.
- Create early warning indicators that measure the success or failure of the risk response.

Risk Appetite

The risk appetite is defined as the amount of risk a business is prepared to accept or be exposed to at any point in time. Risk appetite is also known as *risk preference*, *attitude*, *tolerance* or *capacity*. A company's risk appetite is its ability to absorb risk. Each company's risk tolerance is unique, although organisations can benchmark their own tolerance levels with other organisations in their market or industry, if such information is available. A company's appetite for risk will vary depending on its culture, objectives and changing conditions in the current business environment. Within the insurance industry, a board defines and communicates the company's risk appetite or risk tolerance as a three-stage process (Pricewaterhousecoopers 2004).

First, the goals for shareholder value creation are defined based on a combination of aspects like the business processes, regulatory requirements or the market. Second, the organisation establishes its tolerance for earnings variance based on these stated goals. Third, business units bid for a portion of the company's overall risk tolerance in pursuit of their business plans.

The risk tolerance can be expressed as *earnings variance*, *liquidity and balance sheet activities*, *capital*, and*investment guidelines*. Categories for attitude towards risk are *risk-seeking*, *risk-neutral* or *risk-averse*. A company's risk appetite or the amount of risk that a business is prepared to tolerate may change depending on such aspects as the attitude of individual board members, perceived financial exposure of particular risks, the current success of the business, and trends in the economy.

A company's point of view may also be influenced by other initiatives that have already been taken of, which the outcome is not yet known, based on whether the whole company would be affected if the

outcome were bad or if the company's reputation would be irreparably damaged. When a company has developed its level of tolerance, the business-risk culture can be used to inform senior management about risk-tolerance levels for individual projects and programmes when they apply for approval. While boards try to make informed decisions inside their risk tolerance, there are many factors which may reduce the quality of the information with which they are presented, as reflected in the checklist below. Boards will have to evaluate how accurate the information is that they are given. They would have to evaluate the quality of the information used to do the analysis, the experience level of the analyst, how effective risk management activity will be, and if risk exposure has been hidden deliberately to gain project approval.

Checklist for risk evaluation and assessment of the company's degree of preparedness to take on risk.

- Is the timing and level of risk management planned, agreed on and implemented appropriate to the different acquisition lifecycle stages, risk appetites, decision complexities, and level of risk exposure?
- Is the organisation's risk appetite clear?
- Is there an understanding of and commitment to the level of risk that is acceptable for a project, and is there an ability to communicate this?
- Does this reflect the potential for increasing organisational performance?
- Is a consistent approach and degree of effort being adopted throughout an analysis to assess the potential impact and probability of identified threats?
- Is there a good understanding of the relationship between the potential impact and the probability of the risk occurring, such as very high impact but extremely low probability?
- Is the risk information required being communicated effectively to support the necessary decision making process in a timely, clear and cost effective manner?
- Is there a clear understanding of the difference between the resolution of a known problem or issue and responding to risks, and is there an appropriate mechanism for moving an issue to the risk register and *vice versa*?
- Is a consistent approach being taken regarding the identification and prioritisation of the risks in the risk management process and in any related issue-management process?
- Are the appropriate skills required available to carry out the analysis?
- Are the risks being understated or overstated when assessed and evaluated as a consequence of commercial, political or individual reasons?
- Is there buy-in at all levels of the organisation for the process of assessing and evaluating the threats? How was this established and is the process embedded?
- Can risk management processes be implemented sufficiently quickly to be able to support rapid change? For example, e-commerce developments increasingly require IT developers, business

relationship managers, human resources and facility management to gear up to deliver a solution to the market within very tight timescales.

- Is there a demonstrable correlation between the planned risk management activities,including assessment, and the level of risk exposure?

Source: Based on Office of Government Commerce (2002) "Management of Risk: Guidance for Practitioners," the Stationery Office, London.

Risk Response Strategies

Risk Reduction

Risk responses, which are also known as risk reductions, may also be called *treat* or *mitigate*. Risk diversification is a form of risk reduction whereby risk is dispersed, such as investing in multiple stocks rather than a single stock. Diversification is the technique used by people who do not want *to* put all theireggs in one basket. In his focus on the treatment of hazardous materials in a manufacturing context to prevent personal injury, Wilkinson (2003) describes two general approaches that may be taken to reduce risk: reducing the likelihood of a risk occurring and limiting the loss should the risk materialise. Wilkinson describes methods to reduce the likelihood of occurrence of risks through strategies including protection, controls and maintenance. Methods of risk reduction include the act of risk spreading, such as dispersing chemical storage.

The petrochemical industry, while not being able to remove the threat of adverse weather conditions, designs rigs to withstand high winds. Contractors, while not being able to remove the threat of plant failure, regularly maintain their plants and keep critical spares close at hand. Credit card companies, while not being able to remove default risk, reduce the impact by setting interest rates at a level which compensates the risk and outsource debt recovery. Many companies lose critical personnel. A business cannot prevent this from happening, but as Brent Callinicos of Microsoft explains, it is possible to examine companies that have suffered a sudden departure (McCarthy and Flynn 2004). In this way, it can be seen how that company responded, establish what the public reaction was, examine how the market moved and use this information to make a well-designed response when it happens. You cannot stop a tsunami from happening, but it is definitely helpful if you can have advance warning.

Risk Removal

Risk responses or risk removal is also known by the descriptions: *avoid*, *eliminate*, *exclude* and *terminate*. A strategy adopted for eliminating a risk completely when a negative outcome is anticipated is called risk removal. The best time to eradicate a risk is at the start of a business activity or project. For example, although third-world sections of the globe represent very attractive, untapped market. However,, the political uncertainty that often affects the host nations may be too high, so the risk of doing business with them may be considered too high to consider the opportunity worthwhile.

At times, risks may be accepted due to the failure to examine and appreciate their true potential. If these risks materialise, they significantly decrease the advantages of the project or completely erode its business case. When the company realises a risk's true potential impact after a project has started, abandoning the project or even postponing it in the hope of better circumstances can be very expensive.

Three tests must be applied before selecting risk removal:

1. *Opportunity*: Assess whether or not a substantial opportunity is being lost if a risk is removed because of the risk/opportunity balance being assessed incorrectly.
2. *Business objective*: After removal of the risk or risks, ensure that the alternative course of action selected will satisfy the original business objective.
3. *Cost*: Does the cost of removing the risk outweigh the impact it is likely to cause if it occurs? The true cost of removal may not be visible if removal is done incrementally rather than in one single move.

Risk Transfer or Reassign

Risk response or transfer risk is also known as *deflect*. Risk transfer is the method used to move a risk onto an external organisation, entity or business. The main techniques in which risks are often transferred are contracts and financial agreements.

Transferring a risk does not decrease its possible severity.Instead, the risk is simply shifted to another party. Sometimes transfer can increase the effect of the risk significantly, especially if the receiving party is not aware that it is expected to absorb it. Taking out insurance is a common form of risk transfer. However, insurance transfer doesn't transfer all the risk as insurance contracts often include exclusions or excesses, as with motor insurance. The company that owns the risk will be responsible for initiating this system of risk response. Considering the merit of transferring a risk necessitates a business considering both its and the other parties' objectives, the relative abilities of the parties to assume the risk, the degree of control over the context of the risk, and the potential gain or loss incentive (Perry 1986).

Four tests must be applied when considering risk transfer:

1. Objectives of the parties: What is a party's reason to transfer or accept the risk and is it transparent?
2. Cost effectiveness: Customarily, premiums are charged by the party accepting the risk. A calculation needs to be made about whether or not the premium to be paid is less than the cost of the financial impact of the risk if it occurs. An example of risk transfer is when a business procures a new industrial property and passes on the risk of poor ground conditions to the contractor. This type of risk transfer is not cost effective as the risk may or may not occur and the contractor will have made provisions for this risk in his price. The contractor showing the full cost of the risk in his price will depend on his knowledge of the area, the competition in the market place, the quality and extent of the soil survey, his order book and whether he is in competitive tender.

3. Ability to manage: Successful transfer can occur only if the recipient of the risk or the party that takes on the risk is able to manage the risk. In other words, whether they can implement an action or actions to either remove or reduce the risk.
4. Risk context: The ability of a company to take direct action to manage a risk is important, but so is the context of the risk. In other words, how stable or unstable is the source of the risk, and what degree of fluctuation is present in the probability of the risk will affect the risk context?

A business is not totally protected from the effect of a risk even when it has transferred it. For example, a company will still have to deal with the consequences of a late project even if the risk is transferred to a contractor by means of a penalty clause for late delivery or if the contractor fails to manage the project.

Risk Retention

Risk response or retentionis also known by the terms *absorb*, *tolerate* and *accept*. Risk retention is the appropriate strategy when there is no alternative strategy or it is more expensive to use another strategy, such as transfer, reduce or remove.

Three tests must be applied before using risk retention:

1. Options: If a decision to retain risk has been taken because it is believed that no other alternative is present, has it been ensured that all possible options for removal, reduction or transfer have been evaluated?
2. Ability to absorb: If the conscious decision has been made to retain a risk as it is more economical to do so, is it obvious what the impact is likely to be if it does materialise. or is there the possibility of its occurrence? Does the risk contain only one isolated event or could it be formed of a series of events? Will there be a ripple effect if the risk occurs? Is there just a financial risk or will it also affect other areas of the business, such as market share, staff turnover, reputation, or share price?
3. Timing: The business environment never remains stagnant and alternatives may arise even in the short term, regarding contract terms, insurance, pursuing alternative markets or outsourcing. Therefore, it will be important to monitor the context of the risk through regular risk reviews and recognise when a decision has to be made. Proactive risk management will be essential to ensure that alternative courses of action are not missed.

Risk Management

The previous section describes the risk-planning stage. This section describes what is generally understood to be the last stage within the risk management process, known as the management stage. It is important to understand that each individual stage within the practice of risk management as a whole is iterative, as it is frequently essential to revisit previous stages when circumstances change or more information becomes available.Each stage depends on inputs from earlier stages. Stage 6 is critical for successful implementation of the risk-management process as a whole. All risk-management process

maps state a need to ensure that risk responses for identified risks are implemented and that this implementation is managed proactively.

The following four key activities must be managed for risk management process:

1. *React* to early warning indicators to forewarn executives of the need for developing risk management interventions.
2. *Register* alterations in the details of the opportunities and/or risks on the risk register.
3. *Review* whether the risk managers and actioneers are implementing the responses they are responsible for.
4. *Report* on the success or failure of the opportunity and risk management actions and the changes in the overall risk profile.

The most important process goal of risk management is to observe the performance of risk response actions to notify authorities about the need for proactive risk management intervention.

The risk-management process is adequate when it has achieved these subgoals:

- Early-warning indicators have been created and are used to alert managers of the need to develop risk management interventions.
- Risk actioneers and managers are applying the opportunity and risk responses that are their responsibilities in a well-timed manner.
- Risk registers are updated frequently. Risk events, which have either occurred or are time-expired are removed. Newly-defined opportunities and risks are added to the register. Furthermore, the register is updated to show any changes in the assessment of a risk, for example, if there are changes in its possibility of occurrence or its potential effect, primary or secondary risks categories, managers or owners, the expenses of risk-management action or percentage of completion of risk management actions.
- Reports are sent out on a regular basis, which ensures the successful or ineffective progress made with the risk management actions is visible. The risk management process outputs are regular updates of the risk register and report on the effectiveness of the risk response actions. Each report provides an opportunity and risk status, recording the headway or lack of it, made against actions assigned to each opportunity and risk. Key Performance Indicators (KPIs) are a useful method for monitoring business sensitive issues so that if specified levels are reached, corrective action will be prompted.
- Depending on the nature of the business, the following elements should be measured by the KPIs: absenteeism, sickness, staff turnover, stock levels, sales, changes in the share price, liquidity, customer complaints, customer losses, late payments, supplier defaults, fleet vehicles involved in accidents, and vehicle breakdowns, etc..

- The company risk-management culture will restrain the risk identification process in terms of the degree of commitment, importance and enthusiasm devoted to the process and the degree of support provided when the risk-management process is started.
- The risk-management resources will constrain risk identification in terms of cost, resources and time. When time is an issue, quicker techniques can be used. When money is a constraint, less experienced and thus less expensive staff can be assigned to the project, particularly when external consultants are too expensive. When departmental managers are not available, deputies can be sent or fewer attendees can be invited to participate in the risk identification. If internal risk-management resources are constrained, the process can be accelerated. All of these constraints will probably affect process effectiveness, particularly the breadth of risk identification, potentially leaving blind spots.
- Actionees and managers will constrain the risk-management process if they don't have the necessary time to implement risk management actions, pursue opportunities, evaluate the success of their actions, or attend meetings to report on the successful or unsuccessful performance of the response actions.
- Infrequency of risk meetings will constrain the process, especially if they are the only means used to monitor the implementation of risk-management actions, discuss new risks that arise, and debate alternate courses of action if the initial risk management actions are ineffective.

The Activities of the Risk Management Process

Risk-management process activities are the tasks essential to ensure that risk management is a proactive process which executes, manages and then intervenes to implement corrective action.

Thus, these activities comprise:

- executing: risk response actions
- monitoring: the efficiency of risk management actions
- controlling: intervening when events are not adhering to the plan

Executing

If the actions that were developed to respond to the identified opportunities and risks are not executed, then the time, effort and energy spent on the earlier stages of the risk-management process will be wasted. As described in the previous section, the *what*,*when* and *who* of execution will have been agreed upon and recorded in the plan process.

Monitoring

After executing the activities in the Plan, it is important to monitor the progress against any original plan and evaluate the progress. While monitoring is important, it must be accepted for what it is; a process of

observation. It is neutral like any other outside event. For monitoring to succeed, it has to be embedded into a business and be part of the culture. It must focus on the success or otherwise of the planned responses to previously identified risk and opportunities and should also observe fluctuations in the company that might signal new risks. The environments in which organisations operate are never static. In high-risk environments, the only thing that can be expected is that nothing will go according to plan. Increased absenteeism among employees, decreased sales, late deliveries by suppliers, an increase in the number of returned products, or a reduction in margins may all indicate the emergence of new risks.

Early Warning Indicators (EWI's) are a system of predetermined trigger points which make managers aware that the risk-management actions are being ineffective or that changes have occurred in essential measures. The first question to ask when selecting the measures to use is "What do we measure," not "How do we measure," The selection of appropriate measures will be done by establishing the sets of events that are identified to be important events. Events considered important should include both measurable or quantifiable events and unquantifiable events. The measurable results are things that happened and are in the past. There are no known facts about the future. Developments made by competitors in their products are not measurable until it is too late to have any control.

Therefore, achieving a balance between measurable andnonmeasurable indicators is a fundamental problem for management. Monitoring, which does not look ahead as well as backward, at least in terms of boundaries and restraints, will possibly misdirect and misinform. Furthermore, when more effort is focused on previously identified risks, there is a greater threat that what may appear to be effective monitoring may in fact signify less effective risk management and control. One of the objectives of monitoring is to gather information on risks for later use. Future risk management processes can be improved through lessons learnt during the management process.

Monitoring activities should enable a better understanding of whether

- actionees and managers are working well together.
- the risk register is updated frequently.
- new opportunities and risks are being recognised across all business areas.
- risks that have not occurred or have been overtaken by events, such as fluctuations in the market, have been removed.
- the changes in compliance and legislation give rise to new risks to the business.
- previous market analysis is still valid.
- hedging opportunities have altered.
- funding opportunities have changed.
- current insurance arrangements are still adequate.

Controlling

Controlling is not a neutral activity, like monitoring. Control necessitates intervention. Control techniques focus on using the information collected from monitoring to inform decision making. Controlling means understanding who needs what information for what purpose and when.

To provide control to a manager, the controls must fulfil seven specifications (Drucker 1977):

- They must be economical
- They must be meaningful
- They must be appropriate
- They must be congruent
- They must be timely
- They must be simple
- They must be operational

Control is a Principle of Economy

The better the control design, the less effort is required to gain control of the process. The fewer controls that are needed, the more effective they will be. Generally, adding more controls simply creates confusion, rather than giving better control. When creating a control system, the first question that should be asked is "What is the least amount of information I need, to know I have control?" The answer will differ depending on the type of company and the risk management structure that has been established. Having proprietary computer software or database that produces large amounts of data does not create better controls. On the contrary, what gives control is asking the question:"What is the minimum number ofreports and statistics required to be able to anticipate and understand a phenomenon?"

Controls Must be Meaningful

The events to be measured must be significant in themselves or they must be indicators of potentially significant occurrences, such as emerging new risks, e.g. a competitor introducing a new rival product. The controls should concentrate on the risks that have the greatest effect on the organisation. Additionally, they should be associated with the actual objectives of the risk-management process and produce questions such as "Have the risk responses been employed, were they successful and what risk remains?'"

Controls Have to be Appropriate to the Character and Nature of the Phenomenon Measured

The controls must offer the right vision and information for effective action. It is of little benefit just to report that a risk-response action has not been completed by the due date. There must be a concise description of what this means for the business. If a new risk has been identified, what are its characteristics? If a previously identified risk is now seen as a bigger threat, how great is the threat now, what is its likelihood, is the risk stable or unstable, and has the company's capacity to control it increased

or decreased? If a new opportunity has been identified, what is the window for taking advantage of the prospective benefits, what are the chances that rivals have identified the same benefit, are they better positioned to react, and what are the expected rewards?

Measurements Have to be Congruent with the Events Measured

It is extremely important for managers in the field of risk management to choose what type of measurement is suitable for the event it is measuring. They need to know when 'approximate' is more appropriate than a firm-looking figure that has been calculated with great detail.

Managers have to understand when a range is actually more accurate than an approximate figure. They also should know that *larger* and *smaller*, *earlier* and *later*, and *up* and *down* are quantitative terms and often more precise and reliable than any specific numbers or range of numbers.

It is also important to realise that some events can only be described within a range or as a magnitude and cannot be measured precisely. To say *"*We have 33% of the *market*"sounds comfortingly precise; however, even if it might have been relevant at one point in time, the statement is probably so inaccurate that it is essentially meaningless. What it really means is that "We are not a leading factor in the market place, butneither are we marginal."

Controls Have to be Timely

Conducting frequent measurements and providing very rapid reporting back does not automatically provide better control. The time dimension of control has to parallel the time span of the measured event. Real time controls are controls that inform immediately and constantly. There are events where real time controls are required, such as during drug production in the pharmaceutical industry. However, few events ever require such controls. Most risks have an event window when they are likely to occur, therefore controls should be adapted around these windows.

Controls Need to be Simple

Creating complicated controls does not work. They confuse and discourage the participants. They focus attention on the mechanics of control rather than on what should be controlled. The *how, what, when* and *why* have to be transparent. Controls have to suit the specific circumstances, not be a carbon copy of what was applied in another situation. They need to be revised on a regular basis to ensure that they are still efficient.

Controls Must be Operational

Finally, the controls need to be focused on action rather than information. Have the planned risk-responseactions been executed?Have the potential opportunities been evaluated and results acquired? The results must always reach the individuals who are able to take controlling actions. Controls must be flexible enough to suit the circumstances and should not be restricted by pre-arranged meeting dates.

Further Reading:

- ✓ *Linda S. Spedding, Adam Rose, (2008), Business Risk Management Handbook: a Sustainable Approach*
- ✓ *David Vose, (2008), Risk Analysis: a Quantitative Guide*
- ✓ *James Lam, (2003), Enterprise Risk Management: From Incentives to Controls*