

Risk Analysis and Evaluation

Ziyou Tang

Doctor of Philosophy (PHD) Management, LimKoKwing University of Creative Technology,
Cyberjaya, Selangor, 63000, Malaysia

Abstract

The risks facing an organisation and its operations can result from factors both external and internal to the organisation. They can be categorized further into types of risk such as strategic, financial, operational, hazard, etc. 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 prioritization by comprehensive and structured understanding of business activity, instability 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 organizations knowledge base optimizing operational efficiency.

Keywords

Management, organisation, business, quantitative, necessary.

1. Quantitative Risk analysis

Risk management can be divided into four steps: risk identification, risk assessment, risk control, and risk records. In recent years, studies have mostly focused on the risk assessment. Risk assessment is to analyse and measure the size of risks in order to provide information to risk control. Four steps are included in the risk assessment.

According to the results of risk identification and build an appropriate mathematical model. through expert surveys, historical records, extrapolation, etc. to obtain the necessary, basic information or data available, and then choose the appropriate mathematical methods to quantify the information.

Choose proper models and analysis methods to deal with the data and adjust the models according to the specific circumstances.

Determine the size of risks according to certain criteria. In the risk assessment extrapolation, subjective estimation, probability distribution analysis and other methods are used to obtain some basic data or information. Further data analysis often use following basic theory and methods: layer analysis method, mode cangue logical analysis method, Monte Carlo simulation, the gray system theory, artificial neural network method, fault tree analysis, Bayesian theory, an influence diagram method and Markov process theory.

We can divide the methods into qualitative analysis and Quantitative Analysis.

Qualitative analysis:

2. Fault Tree Analysis

Fault Tree Analysis (Fault Tree Analysis, FTA) can be used for qualitative analysis of risk and can also be used for quantitative analysis. It is mainly used for large-scale complicated system

reliability and safety analysis. It is also an effective method to Unification reliability and safety analysis, through hardware, software, environment, human factors. FTA is drawing a variety of possibilities of failure in system failure analysis, from whole to part, according to the tree structure. Fault tree analysis using tree form, the system

The failure of components and composition of the fault system are connected. We are always using fault tree in qualitative or quantitative risk analysis. The difference in them is that the quantitative fault tree is good in structure and it requires use of the same rigorous logic as the formal fault tree, but qualitative fault tree is not. Fault tree analysis system is based on the target which event is not hoped to happen (called the top event), one level down from the top event analysis of the direct cause of their own events (call low event), according to the logical relationship between the upper and lower case, the analysis results are obtained.

3. Event Tree Analysis

Event tree analysis (event tree analysis, ETA) also known as decision tree analysis, is another important method of risk analysis. It is the events of a given system, the analysis of the events may cause a series of results, and thus evaluates the possibility of the system. Event tree is given an initial event all possible ways and means of development, every aspect of the event tree events (except the top incidents) are the implementation of certain functions of measures to prevent accidents, and all have binary outcomes (success or failure). While the event tree illustrates the various incidents causes of the accident sequence group. Through various intermediate steps in the accident sequence group can organize the complexity of the relationship between the initial incident and the probability of systemic risk reduction measurement, and identify the accident sequence group. So we can calculate the probability of each of the key sequence of events occurred.

4. Cause-Consequence Analysis

Cause and consequence analysis is a combination of fault tree analysis and event tree analysis. It uses the cause analysis (fault tree analysis) and the result analysis (event tree analysis), CCA aims to identify the chain of events leading to unexpected consequences, according to the probability of occurrence of different events from CCA diagram to calculate the probability of different results, then the risk level of the system can be determined.

5. Preliminary Risk Analysis

Preliminary risk analysis or hazard analysis is a qualitative technique which involves a disciplined analysis of the event sequences which could transform a potential hazard into an accident. In this technique, the possible undesirable events are identified first and then analyzed separately. ² For each undesirable events or hazards, possible improvements, or preventive measures are then formulated.

This method provides a basis for determining hazard categories and which analysis methods are most suitable. It is proved valuable in the working surrounding to which activities lacking safety measures can be readily identified.

6. Hazard and Operability Studies (HAZOP)

The HAZOP technique was originated in the early 1970s by Imperial Chemical Industries Ltd. HAZOP is firstly defined as the application of a formal systematic critical examination of the process and engineering intentions of new or existing facilities to assess the hazard potential

that arise from deviation in design specifications and the consequential effects on the facilities as a whole.

This technique is usually performed using a set of guidewords: NO/NOT, MORE OR/LESS OF, AS WELL AS, PART OF REVERSE, AND OTHER THAN. These guidewords, a scenario that may result in a hazard or an operational problem is identified. Consider the possible flow problems in a process line, the guide word MORE OF will correspond to high flow rate, while that for LESS THAN, low flow rate. The consequences of the hazard and measures to reduce the frequency with which the hazard will occur are then discussed. This technique is accepted widely in the process industries. It is mostly regarded as an effective tool for plant safety and operability improvements. Detailed procedures on how to perform the technique are available in some relevant literatures.

7. Qualitative Risk Analysis

The Term Risk is an inevitable component of the dynamics of Business today. The Treasury Board has defined risk as "the uncertainty that surrounds future events and outcomes". It is the expression of the likelihood and impact of an event with the potential to influence an organization's achievement of objectives" (TBS 2001). It is though not possible to "create a business that doesn't take risks" (Boulton et al. 2000). Risk, therefore, is the probability that an event in the future, either good or bad, will occur. As uncertainty abounds in today's global economy every organization is to some extent, in the business of risk management, no matter what its products or services are. According to the treasury (2006), in recent years all sectors of economy have focused on management of risk as the key to making organisations successful in delivering their objectives whilst protecting the interests of their stakeholders. (Treasury, 2006)

In the Context of Banking and finance 'Risk' has always been at the heart of banking transactions and to a degree banking can be defined as the business of managing and transforming risks. For a company 'Risk' designates any uncertainty that might trigger losses in the short or long term therefore risk managers constantly attempt to measure and control the risks within their companies. It is not possible to "create a business that doesn't take risks," according to Richard Boulton. "If you try, you will create a business that doesn't make money." (Boulton et al. 2000) Nearly all operational tasks and processes are now viewed through the prism of risk (Hunt 2001). Although the enormous growth and development in financial and electronic technologies, however, have enriched the palette of risk management techniques available to managers, offering an important new opportunity for increasing shareholder value amidst the global liquidity crisis surrounding all the major multinational companies around the World.

The turmoil has affected all the financial institutes from the setting of interest rates to the scale, structure and complexity of market operations. The entire economy has had to face the consequences the financial meltdown. Most developed countries are now in recession and previously strong emerging economies such as India and China are slowing sharply as well because their exports have hampered due to weak demand of their products overseas which is a result of reluctance of the importing countries to import and spend amid difficult financial times.

The issue of 'The credit crisis and bank failures' have highlighted risk issues with executive compensation arrangements that incentivize management to take significant risk in order to achieve financial targets which would entitle management to obtain certain incentive compensation (Section 111, EESA 2008) and therefore the Emergency Economic Stabilization Act of 2008 requires financial institutions participating in certain programs provided under the Act to review executive compensation arrangements and to limit those arrangements that

encourage management to take "unnecessary and excessive risk" that could threaten the value of the institutions.

While there has been a considerable increase in practitioner attention on ERM in recent number of years especially in the past two years, a little academic research exists about ERM and its influence on or after the Financial Crisis and in particular about the Effectiveness of ERM on the organisations performance and its potential significance to the organisation during any kind of market turbulence. As a general practice a large number of companies are now opening up to use ERM as a strategic management tool (Pagach, Donald. P, June 2008). This is a Strategic level activity among the Management of the Firm. Indeed, the goal of enterprise risk management is to maximize value by shaping the firm's risk profile, shedding some risks, while retaining those that are worth some value they can deliver to the company and thereby managers can analyze and control various risks as a part of a unified or integrated, risk management policy.

8. Risk Evaluation

A basic knowledge of health and safety is required before a risk assessment can be completed. The Health and safety at work act is a set of rules which are set to protect the employees, employers, clients and the business itself from any accidents or illness. The health and safety act rules are there for both employees and employers to abide by to ensure the safety of anyone i.e. clients, delivery people, that may have anything to do with the workplace.

A risk assessment is an important element of health and safety for any business as this will help prevent accidents and serious harm to all concerned. A risk assessment is a careful examination of what could cause harm to people within the work place. It is used to prioritise any possible dangers, to assess how dangerous they are and how to prevent them. Huges P (2007) pg 67 states "risk assessment methods are used to decide on priorities and to set objectives for eliminating hazards and reducing risk".

When doing a risk assessment its essential to remember that a hazard is something that can cause harm such as electrical equipment and chemicals. The risk is the chance someone could be harmed and if it's high or low.

Businesslink.gov.uk (2008) states that "you are not expected to eliminate all risk, but you are required to protect people as far as reasonably practical". To perform a sufficient risk assessment there are five steps to ensure a thorough test has been done. The first being to identify serious hazards from the trivial ones and then once these have been established, the second step would be to make a decision on who these may affect this will include anyone who has anything to do with the business. The third element of a risk assessment is to evaluate the level of the risks that have been found. A qualitative assessment can be done in most cases which would enable the assessor to grade them as medium, high or low depending on the potential danger it could cause. The fourth step would be to record your findings and then start to put into place methods of prevention. Lastly the risk assessment should be reviewed on a regular basis. Overall the risk assessment should consist of identifying the hazards, establishing who they may affect, evaluate the risks; record the findings and the make sure that regular checks are kept and recorded up to date. Keeping a record will help to monitor the health and safety within a business.

This assignment is going to look at the most popular facilities within the spa environment which are: Saunas, Jacuzzis, steam rooms, showers, floatation tanks and swimming pools, as regular checks are paramount to avoid water bourn diseases.

When it comes to saunas the daily maintenance routine checks are paramount to keeping the sauna at the right temperature, chemical levels are correct not exceeding or lowering the amount needed. The removal of excess water is to avoid slipping or festering of any bacteria

that may build up; this has to be monitored on a regular basis. In the case of the Jacuzzi and the plunge pool these need to be drained on a regular basis to enable them to be thoroughly cleaned out. Disinfectant may be used for the flooring and the seating areas. The sauna, Jacuzzi and plunge pool all need to have filtration systems that will need to be cleaned on a daily basis to ensure that they are in excellent working order.

Shower areas should be checked and cleaned a number of times a day with disinfectant. The shower heads should be dismantled at least once a week for a deep clean as should all soap dispensers using a light disinfectant to avoid any allergic reactions that might occur. The flooring around all these facilities is to be kept clean and dry whenever possible and clients using the facilities should be advised to wear suitable footwear at all times to avoid accidents such as slipping.

A risk assessment for a shower area may consist of the following possible hazards:-

Injury caused by slipping or falling is a high risk. This risk can be put to a minimal risk by regular visual checks of the area and when need, to remove the excess water.

A risk assessment for the swimming pool, Jacuzzi and plunge pool would be comparable and consist of the following possible hazards:-

Injury due to slipping or a fall. This would be a medium risk and would require action to lower the risk. Life guards would be required to do regular visual checks of the areas concerned and to advise people to wear the correct foot wear.

Chemicals in the pool checks, this poses a medium risk and can be controlled by regular tests. If there are any chemical adjustments to be made these will be implemented and recorded to maintain the waste is kept at the right chemical levels.

Drowning is a hazard. This hazard can be supervised by the life guards being qualified in first aid and having rescue aids in place with easy access. Also the water facilities should be locked when not in use to avoid any accidents.

A sauna and steam room will also have some similarities and consist of these possible hazards:- Becoming ill or injured due to any medical history could pose a threat and put in the medium risk category as medication can have side effects such as blurred vision and faintness. To prevent this from happening an in depth consultation for any persons who uses the facilities is needed and to be kept on record for future reference.

Any injuries from rough or slippery floors pose a medium risk as in this environment it is more than likely to happen. To prevent this from happening, all persons using these areas should be made aware of safety rules such as wearing the correct footwear.

Heat exhaustion poses a medium to high risk as some users of the facilities may not be fully aware of the time scales they should be in there. Ensuring that the users are informed of how long they should be in the sauna/steam room and to drink water at regular intervals to avoid dehydration, this hazard can be avoided.

The timber becoming damaged by mould or softening poses a medium risk. This can be avoided by the door to the sauna being left open at the end of sessions giving the timber time to breathe and dry out at the end of the day.

The possibility of being scolded in the steam room poses a medium threat. The rules for using the equipment must be followed at all times, with care in doing so.

The possibility of a fire breaking out in a sauna poses a medium risk. To ensure this does not happen regular checks on the temperature should be made, regular checks on the water levels should be made along with regular checks to make sure there are no towels lying around where they may catch fire.

This assignment has given information on what a risk assessment is and why a risk assessment should be carried out within all work places. It demonstrates health and safety

and how important it is within the work place for people to follow the procedures they are set for each specific task. The information has been supported by a variety of research incorporating the Health and Safety regulations.

9. Risk Treatment

9.1. External and Internal Factors

The risks facing an organisation and its operations can result from factors both external and internal to the organisation. They can be categorized further into types of risk such as strategic, financial, operational, hazard, etc. 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 prioritization by comprehensive and structured understanding of business activity, instability 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 organizations knowledge base optimizing operational efficiency. 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 national and state legal requirements, its regulatory requirements, its business drivers and objectives, and it must carry out a risk and threat analysis. 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 enterprise risk management, the core components of any risk analysis is made up of the following:

Identify company assets

Assign a value to each asset

Identify each asset's vulnerabilities and associated threats

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. According to Frederick Funston, Stephen Wagner and Henry Ristuccia 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 internal audit function is an integral part of the corporate governance regime of most public companies and a number of larger private companies. The primary goal of internal audit is to evaluate the company's risk management, internal control and corporate governance processes and ensure that they are adequate and are functioning correctly. King II views the existence of an internal audit function as essential

for all affected companies and suggests that where the board of such a company decides not to implement an internal audit function, full reasons for its decision should be advanced in the company's Annual Report. In addition, the board should consider how, in the absence of internal audit, the effectiveness of the company's internal processes and systems will be verified.

Internal audit may be carried out by an in-house division or outsourced, although where the function is outsourced to the same firm that performs the company's external audit, care should be taken to ensure that suitable. The separateness of the external and internal audit functions are essential to proper corporate governance, as the one acts as a system of checks and balances in respect of the other. In practice there is often a high degree of cooperation between the external and internal audit functions of a company, and the external auditors usually affirm in their audit report the extent to which reliance has been placed on the work performed by internal audit. The purpose, authority and responsibility of the internal audit function should be formally defined in a form consistent with the standards of the Institute of Internal Auditors, and a formal Internal Audit Charter should be approved by the board. The charter should define the mission and scope of the internal audit function, its sphere of responsibility, its authority within the company, and its accountability and reporting obligations. The internal audit function should be sufficiently independent of the activities audited to ensure that the fact that internal auditors may be employees of the company does not hamper their independence and their ability to be objective. Internal audit should report at a level within the company that allows it to accomplish its responsibilities without undue interference, preferably to the CEO or the chairman. As previously stated, the head of the company's internal audit function should have regular, independent access to the chairman of the audit committee. The appointment or dismissal of the head of internal audit should be dealt with in consultation with the audit committee. Risks are uncertain future events that could influence the achievement of a company's strategic, operational, financial and compliance objectives. Risks are an unavoidable part of the business process, but good risk management at least protects an organisation against avoidable losses. Risk management is the process of deciding which risks to avoid, control, transfer or tolerate. The overall responsibility for risk management, which includes internal controls, rests with the board of directors. The board is responsible for ensuring that a formal risk assessment is undertaken at least annually for the purposes of making its public statement on risk management, including internal control. The board should acknowledge, in this statement, its responsibility for the risk management process and for reviewing its effectiveness. Management is accountable to the board for designing, implementing and monitoring the process of risk management, and integrating it into the day-to-day activities of the company. Management is also accountable to the board for providing assurances that it has done so. Risk management is multi-faceted and requires a team-based approach. Boards are encouraged to appoint dedicated committees to oversee the risk management process. Members of a risk committee should be executive directors and senior management who are involved with the operational functions of the organisation in addition to non-executive directors with relevant skills or experience.

10. Risk Monitoring & Review

Each organization has its own and unique objectives. These objectives are the reason a company is being established and also guides them for future development. To be able to identify a risk in an enterprise a thorough understanding of the entities objective should be done by the risk managers. If risk managers completely understood the organisations objectives it will enable them to classify threats and opportunities the enterprise will face in the future and can create solutions or prevent risk associated with an organisations future

actions. An example will be a company's objective is to be globally competitive the risk managers will create a plan that will help the organisation achieve its objectives but prevent the risk associated with it like policies and laws of other country or the consumer needs for the product and service.

10.1. Identifying Exposure to Loss

Loss exposures include loss of financial assets, physical property, human loss and loss of good will. These are the risk that a risk manager might identify when assessing possible risk of the company. These losses can be prevented if proper risk identification is done before any untoward event occurs. Loss of financial assets is usually due to liability judgement, non-compliance and lawsuits. Loss of physical property can be because of bad investment, land ownership problems and natural disasters that may damage the property. Human loss is related to death, injury or resignation of employees that can affect the operations of the company. Reputation is very important for a company to function if consumers trust an organisations services and products this will increase their reputation but otherwise it can lead to loss of good will.

10.2. Measure Those Same Exposures

An organisation not only needs to identify the risk or loss but as well as measure the impact of those risks to the organisation. These can be achieve by using different tools is assessing risk for example a client complain and satisfaction survey reports. This survey will help risk managers identify the areas where in they need modifications and improvement let as say in the survey patients complained that the nurses are rude therefore the managers should assess the employees in that department and try to do necessary adjustments to increase client satisfaction at the same time prevent human loss. Another one is incident reports these are usually a common tool used to identify risk it is a report made by employees that includes events that occur beyond the normal daily operations. Others are genetic occurrence screening, employee compensation claims data, contact leases and agreements and informal discussion with managers and staff these can be used to determine the risk and its effect on the organizations operation.

10.3. Select Alternatives

As stated earlier risk is inevitable in handling these risk a risk manager uses risk treatment strategies categorized into two which is risk control and risk financing. Risk control is preventing losses and justifying the effects of losses. It is composed of three techniques which are exposure avoidance, loss prevention and segregation of loss exposure. Exposure avoidance is the reduction of loss to zero if focuses on the eradication of the possibility of loss to occur. It is used when a potential risk can be critical threat to the organization and there is no way to reduce or transfer those risks. Loss prevention gives emphasis on the possibility of an occurrence of an event and reduction of loss by educating staff and reviewing of policies and procedures. Loss reduction reducing the severity of loss an example is having fire drills, alarm system and immediate incident investigation to an event. Segregation of loss exposure this is distribution of assets like supplies to different department to prevent loss for example in the first floor of the facility the flood damaged the supplies of medicines but on the second floor where other supplies are placed these can be used and distributed to the other department reducing the loss and continues the operations of the facility.

10.4. Implement a Solution

Implementation of the solution is putting the plan into action. This will involve the use of the technique identified by the risk management professional which is the best to prevent further organisational loss. This technique will be assumed by other department managers within the

organisation. For example if the risk manager professional identified that the best technique risk financing and risk transfer the risk manager may include selecting an insurer and creating a good insurance policy for the organisation.

10.5. Monitor and Review the Outcomes

The last step in risk management process this is to check the effectiveness of the risk management program. It is an approach done by risk managers, higher management, different department managers, and legal counsel and claim managers to evaluate the risk and its impact to various areas of the organisation. This will enable the organisation to see the flaws and further improve the risk management plan of the organisation. The evaluation is done by comparing the annual report made by the risk manager against the bench mark they have created as well as the previous annual reports in the past years.

Risk assessment process is defines as an organized process for identifying and evaluating events that effects the accomplishment of objectives in a positive or negative way. These events can be related to political, legal, environmental, social and competition. It can also be an internal factor like human resource, organisational processes and infrastructure. Risk assessment like any process is made up off different steps which are:

Identification of relevant business objectives

Identifying events that could affect the achievement of objectives

Determining risk tolerance

Assessing the inherent likelihood and impact of risks

Evaluating the portfolio of risk and determining risk responses

Assessing residual likelihood and impacts of risks

10.6. Identification of Relevant Business Objectives

Objectives are the goals that an organisation wants to achieve in order to prosper in the business world. Each organisation has its own set of objectives that may be the same or different from other organisations. Through these objectives a risk manager will be able to extract different risk that could threaten the organisation. Objectives can be constructed by using the SWOT analysis wherein it determines the strength, weakness, opportunities and threats. After the objective identification and finding out the possible risk a risk management plan can be started.

10.7. Identifying Events that could Affect the Achievement of Objectives

According to an organisation objective the risk managers should create an initial inventory of undertakings that may affect the accomplishment of the organisations objective. These events can be from within the organisation or from the external environment. The internal factors are organisations policies and processes, the human resource, technology and information that are taken from internal sources. Meanwhile, external factors are related to politics, economics, legal, sociological and environmental. After assessing these factors the risk manager can then categorise them as either a threat or an opportunity for the organisation. Written annual reports of internal and external factors will provide the risk manager of accurate numbers and percentage to pinpoint which threats needs immediate action.

10.8. Determining Risk Tolerance

The acceptable level of deviation comparative to the accomplishment of a specific objective of an organisation is called risk tolerance. It is a percentage or level in which a risk can be accepted by the organisation but have a certain range of limitation that could still enable an organization to operate.

10.9. Assess Inherent Likelihood and Impact of Risk

In risk assessment it is part of the process to identify the events that has a potential impact on the accomplishment of the organisational objective. These events should be considered to be risk and has to be evaluated based on the chances of it to occur. It is essential that this event should be assessed on natural basis without bearing in mind the risk response that already exists. An inherent risk map should be assess by a risk manager, it is a portfolio view of risk that aides analysis and action, to determine the which risk has more effect and should be a prioritized for an immediate response.

10.10. Evaluating the Portfolio of Risk and Determining Risk Responses

As we all know risk is inevitable it cannot be fully eliminated if an organisation wanted to have a return of investment they should take on some risk associated for their actions. Evaluating the risk portfolio will enable the risk manager and the organisation to see the impacts of the risk to the organisations objectives and goals. It will also evaluate the effectiveness of the risk response they have made and further improve if such risk arises in the future. Risk tolerance varies depending on the risk type as well as the responses to those risks so it is essential to assist the risk response and the action given and its effectiveness.

10.11. Assessing Residual Likelihood and Impacts of Risks

Assessing residual risk will help evaluate the effectiveness and appropriateness of the risk response if it is in within the acceptable level or within the risk tolerance of the organisation. It is assessing the internal checks and balances are still in place within the organisation.

Therefore, we could see how essential risk management is to an organisations progress. Risk management is not just a simple work just to identify and provide a solution but it is a systematic and scientific way of identifying, implementing and evaluating the effects of risk to the organisation. The organisation will always face risk to be able to move and not stagnate on the current status they are in. It is a must that a risk management professional understand the organisations objective for him or her to extract and create an excellent risk management plan. It is also important to evaluate the effectiveness of the risk management plan and see to it that flaws are modified for better result in the future.

11. Documenting Risk

Documenting the risk management process has become less frustrating today, with the use of the risk management template. This preformatted tool was designed to help reduce the time required for this important document. Because the path to follow, along with the sections required, in this document are already set, the project manager can then concentrate on the details of the process.

The utilisation of a recognised framework is an integral part of assessing a patient in order to identify their needs. Roper et al. (2003, p4) provide a model for nursing based on the Activities of Living. This framework offers a clear structure for nurses to work around with a problem solving approach and also incorporates the nursing process. The Activities of Living framework covers 12 areas including maintaining a safe environment, communicating, breathing, eating and drinking, eliminating, personal cleansing and dressing, controlling body temperature, mobilising, working and playing, expressing sexuality, sleeping and finally, dying. Assessment is the first stage of the Nursing process as identified by Yura and Walsh (1978) and cited by Holland et al. (2003, p.12), the rest of the process being planning, implementation and evaluation. Mallett and Dougherty (2003, p281) suggest that a thorough assessment focuses on the physical, psychological and psychosocial issues relating to a patient. This is necessary to enable identification of any risks and to then aid their prevention. Sharkey (1997, p49-50) suggests that it is of great importance for nurses to be able to make speedy

identification of risks, as no situation is completely risk free. Whitfield (2000) cited by Stevenson (2004) found risk assessment, education and the formulation of protocols to be the most effective prevention strategies when focusing on the prevention of pressure damage. This would suggest that the ability to perform an accurate risk assessment is therefore an essential skill required by each member of the nursing profession. This interpretation is supported by Marks-Maran et al. (1988, p37).

References

- [1] Churchill Livingstone's Dictionary of Nursing (2002). 18th edition. Edinburgh: Churchill Livingstone.
- [2] Dealey, C. (2000). The Care of Wounds – A Guide for Nurses. 2nd edition. Oxford: Blackwell Science.
- [3] Defloor, T. and Grypdonck, M. (2004). Validation of Pressure Ulcer Risk Assessment Scales: A Critique. *Journal of Advanced Nursing*. 48(6), 613-621.
- [4] Harrison, A. (2003). A Guide to Risk Assessment. *Nursing Times*. 99 (9), 44-45.
- [5] Holland, K (2003). An Introduction to the Roper-Logan-Tierney Model for Nursing. Based on Activities of Living. In K. Holland, J. Jenkins, J. Soloman & S. Whittam (eds.) *Applying the Roper-Logan-Tierney Model in Practice*. London: Churchill Livingstone.
- [6] Mallett, J. and Dougherty, L. (2003). *The Royal Marsden Hospital Manual of Clinical Procedures*. 5th edition. Oxford: Blackwell Science.
- [7] Marks-Maran, D. J. Docking, S. P. Maunder, T. and Scott, J. (1988). *Skills for Care Planning – A Guide for Teaching the Nursing Process*. Middlesex: Scutar Press.
- [8] *Mosby Nurses Pocket Dictionary* (2003). 32nd edition. London: Mosby.
- [9] National Institute for Clinical Excellence (2001). *Pressure Ulcer Risk Assessment and Prevention*. London: National Institute for Clinical Excellence.
- [10] Nursing and Midwifery Council (2002). *Code of Professional Conduct*. London: NMC.
- [11] Pang, S. M and Wong, T. K. (1998). Predicting pressure sore risk with Norton, Braden and Waterlow. *Nurse Researcher*. 47 (3), 147-153.