International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 6 Issue 8|| August 2017 || PP. 68-79

Assessing and Controlling Risk in Industrial Organization

*Engr. Dr. Uzorh, A.C
Department of Mechanical Engineering, Federal University of Technology Owerri, Imo State, Nigeria
Corresponding Author: Engr. Dr. Uzorh, A.C

Abstract: *Risk management is an activity which integrates recognition of risk, risk assessment, developingstrategies to manage it, and mitigation of risk using managerial resources. Some traditional risk managementsare focused on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, death).Industrial risk management, on the other hand, focuses on risks that can be managed using effective risk assessment techniques. Objective of risk management is to reduce different risks related to a pre-selected domain to anacceptable. It may refer to numerous types of threats caused by environment, technology, humans,organizations and politics. The paper describes the different steps in the risk management process whichmethods are used in the different steps, and provides some examples for risk and control measures.*

Keywords*: Risk, Risk management, Safety, Risk matrix, Hazard*

Date of Submission: 17-07-2017 Date of acceptance: 31-08-2017

I. INTRODUCTION

1.1 Risk

Organizations face a wide range of risks each day that can affect their ability to achieve certain business objectives and stay in business. Risk assessment is an important and sophisticated process used to assess an organization'srisks so that it can mitigate and reduce risks to an acceptable level.

Risk is unavoidable and present in every human situation. It is present in daily lives, publicand private sector organizations. Depending on the context (insurance, stakeholder, technicalcauses), there are many accepted definitions of risk in use.

The common concept in all definitions is uncertainty of outcomes. Where they differ is inhow they characterize outcomes. Some describe risk as having only adverse consequences, whileothers are neutral.

One description of risk is the following: risk refers to the uncertainty that surrounds futureevents and outcomes. It is the expression of the likelihood and impact of an event with the potentialto influence the achievement of an organization's objectives.

The phrase "the expression of the likelihood and impact of an event" implies that, as aminimum, some form of quantitative or qualitative analysis is required for making decisionsconcerning major risks or threats to the achievement of an organization's objectives. For each risk,two calculations are required: its likelihood or probability; and the extent of the impact orconsequences.

Finally, it is recognized that for some organizations, risk management is applied to issuespredetermined to result in adverse or unwanted consequences. For these organizations, thedefinition of risk which refers to risk as "a function of the probability (chance, likelihood) of anadverse or unwanted event, and the severity or magnitude of the consequences of that event" will bemore relevant to their particular public decision-making contexts.

1.2 Risk Management

Two different safety management principles are possible: consequence based safetymanagement will claim that the worst conceivable events at an installation should not haveconsequences outside certain boundaries, and will thus design safety systems to assure this. Riskbased safety management (usually called risk management) maintains that the residual risk shouldbe analysed both with respect to the probabilistic and the nature of hazard, and hence giveinformation for further risk mitigation. This implies that very unlikely events might, but notnecessarily will, be tolerated.

Risk management is not new tool and a lot of standards and guidance documents are available

(ACT 2004, AZ/NZS 2004, Committee 2004, HB 2004, IEC 2008, ON2008, Rio Tinto 2007, Treasury Board of Canada 2001). It is an integral component of goodmanagement and decision-making at all levels of an organization. All departments in anorganization manage risk continuously whether they realize it or not, sometimes more rigorouslyand systematically, sometimes less. More rigorous risk management occurs most visibly in thosedepartments whose core mandate is to protect the environment and public health and safety. Atpresent, a further generic standard on risk management is in preparation as a common ISO/IECstandard (IEC

2007) describing a systemic top down as well as a functional bottom up approach(see Fig. 1) This standard is intended to support existing industry or sector specific standards.

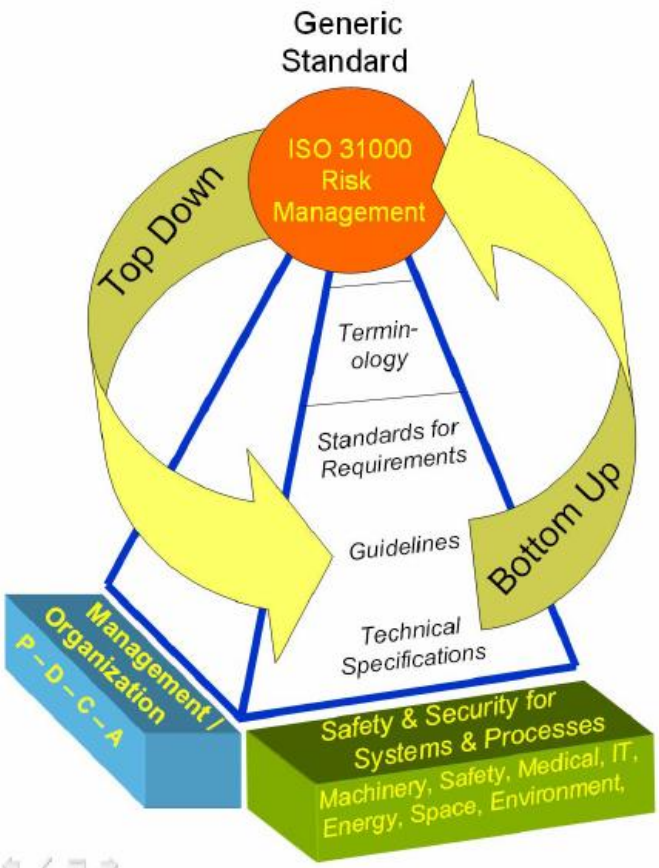

Fig. 1: Approach of the planned generic standard on risk management.

As with the definition of risk, there are equally many accepted definitions of risk managementin use. Some describe risk management as the decision-making process, excluding the identificationand assessment of risk, whereas others describe risk management as the complete process, includingrisk identification, assessment and decisions around risk issues.

One well accepted description of risk management is the following: risk management is asystematic approach to setting the best course of action under uncertainty by identifying, assessing,understanding, acting on and communicating risk issues.

In order to apply risk management effectively, it is vital that a risk management culture bedeveloped. The risk management culture supports the overall vision, mission and objectives of anorganization. Limits and boundaries are established and communicated concerning what areacceptable risk practices and outcomes.

Since risk management is directed at uncertainty related to future events and outcomes, it isimplied that all planning exercises encompass some form of risk management. There is also a clearimplication that risk management is everyone's business, since people at all levels can provide someinsight into the nature, likelihood and impacts of risk. Risk management is about making decisions that contribute to the achievement of anorganization's objectives by applying it both at the individual activity level and in functional areas.

It assists with decisions such as the reconciliation of science-based evidence and other factors; costswith benefits and expectations in investing limited public resources; and the governance and controlstructures needed to support due diligence, responsible risk-taking, innovation and accountability.

A typical decision support for risk and safety management at strategic, normative andoperational level is provided in (JCSS 2008).

1.3 Integrated Risk Management

The current operating environment is demanding a more integrated risk managementapproach (Bolvin et al. 2007 and Treasury Board of Canada 2001). It is no longer sufficient tomanage risk at the individual activity level or in functional silos. Organizations around the worldare benefiting from a more comprehensive approach to dealing with all their risks.

Today, organizations are faced with many different types of risk (e.g., policy, program,operational, project, financial, human resources, technological, health, safety, political). Risks thatpresent themselves on a number of fronts as well as high level, high -impact risks demand a coordinated,systematic corporate response.

Thus, integrated risk management is defined as a continuous, proactive and systematicprocess to understand, manage and communicate risk from an organization-wide perspective. It isabout making strategic decisions that contribute to the achievement of an organization's overallcorporate objectives.

Integrated risk management requires an ongoing assessment of potential risks for anorganization at every level and then aggregating the results at the corporate level to facilitatepriority setting and improved decision-making. Integrated risk management should becomeembedded in the organization's corporate strategy and shape the organization's risk managementculture. The identification, assessment and management of risk across an organization helps revealthe importance of the whole, the sum of the risks and the interdependence of the parts.

Integrated risk management does not focus only on the minimization or mitigation of risks,but also supports activities that foster innovation, so that the greatest returns can be achieved withacceptable results, costs and risks.

From a decision-making perspective, integrated risk management typically involves theestablishment of hierarchical limit systems and risk management committees to help to determinethe setting and allocation of limits. Integrated risk management strives for the optimal balance at thecorporate level. However, companies still vary considerably in the practical extent to whichimportant risk management decisions are centralised (Basel Committee on Banking Supervision2003).

1.4 Safety management

Apart from reliable technologies, the operational management of a industrial plant with highrisk potential is also a highly important factor to ensure safe operation. Owing to the liberalization of the markets and resulting cost pressure to the industries, the importance of operationalmanagement is growing since cost savings in the areas of personnel and organization result inreducing the number of personnel together with changes in the organizational structure and tighterworking processes.

For small- and medium-sized companies, specific support is necessary and provided in (Rheinland-Pfalz 2008).

Experience with accidents in different branches of industry shows the importance of safeoperational management. Today, effective safety management is seen as one crucial element of safeoperational management (Hess &Gaertner 2006).

The term safety management subsumes the entirety of all activities relating to the planning,organization, management and supervision of individuals and work activities with a view to theefficient achievement of a high degree of safety performance, i.e. the achievement of a high qualityof all activities that are important to safety, and to the promotion of a highly developed safetyculture. Safety management is not limited to certain organization units but comprises the entiresafety-related organization of the company. Safety management is the responsibility of themanagement level of a company.

For example in case of nuclear power plant in Germany (ICBMU 2004), the licensee is according to the Atomic Energy Act responsible for the safety of the plant he operates. To fulfill theconditions associated with this responsibility, he has to implement an effective safety managementsystem that complies with the requirements of the current regulations and with internationalstandards. Typical management systems in nuclear power plants are described.

Sometimes risk management and safety management are seen as the same type ofmanagement, but in practice safety management is a main and important part of the riskmanagement which also covers, e.g. financial risks.

II. RISK MANAGEMENT STEPS AND TOOLS

The risk management steps (see Fig. 2) are:

1. Establishing goals and context (i.e. the risk environment),
2. Identifying risks,
3. Analysing the identified risks,
4. Assessing or evaluating the risks,
5. Treating or managing the risks,
6. Monitoring and reviewing the risks and the risk environment regularly, and
7. Continuously communicating, consulting with stakeholders and reporting.

Some of the risk management tools are described in (IEC 2008) and (Oehmen 2005).

2.1 Establish goals and context

The purpose of this stage of planning enables to understand the environment in which therespective organization operates, that means to thoroughly understand the external environment andthe internal culture of the organization. The analysis is undertaken through:

- establishing the strategic, organizational and risk management context of the organization,and
- identifying the constraints and opportunities of the operating environment.

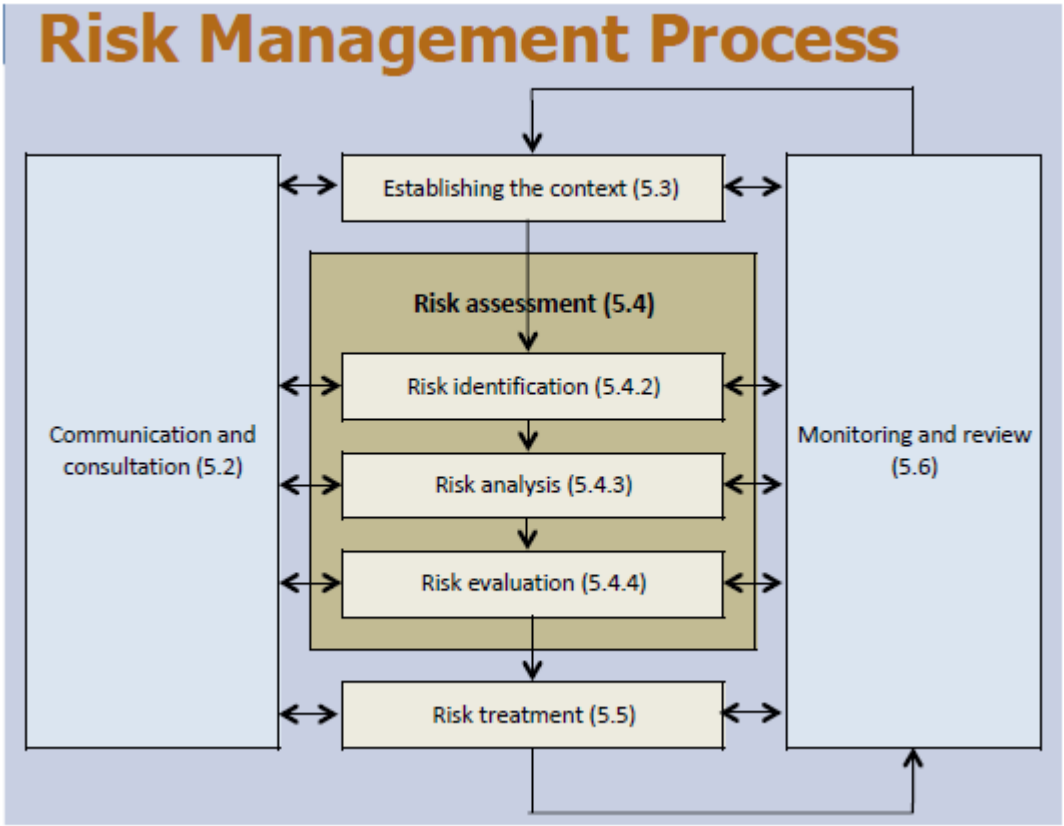

Fig. 2: Risk management process.

The establishment of the context and culture is undertaken through a number ofenvironmental analyses that include, e.g., a review of the regulatory requirements, codes andstandards, industry guidelines as well as the relevant corporate documents and the previous year'srisk management and business plans.

Part of this step is also to develop risk criteria. The criteria should reflect the context defined,often depending on an internal policies, goals and objectives of the organization and the interests ofstakeholders. Criteria may be affected by the perceptions of stakeholders and by legal or regulatoryrequirements. It is important that appropriate criteria be determined at the outset.

Although the broad criteria for making decisions are initially developed as part of establishingthe risk management context, they may be further developed and refined subsequently as particularrisks are identified and risk analysis techniques are chosen. The risk criteria must correspond to thetype of risks and the way in which risk levels are expressed.

Methods to assess the environmental analysis are SWOT (Strength, Weaknesses,Opportunities and Threats) and PEST (Political, Economic, Societal and Technological)frameworks, typically shown as tables.

2.2 Identify the risks

Using the information gained from the context, particularly as categorised by the SWOT and PEST frameworks, the next step is to identify the risks that are likely to affect the achievement ofthe goals of the organization, activity or initiative. It should be underlined that a risk can be anopportunity or strength that has not been realised.

Key questions that may assist your identification of risks include:

- For us to achieve our goals, when, where, why, and how are risks likely to occur?
- What are the risks associated with achieving each of our priorities?

− What are the risks of not achieving these priorities?

− Who might be involved (for example, suppliers, contractors, stakeholders)?

The appropriate risk identification method will depend on the application area (i.e. nature ofactivities and the hazard groups), the nature of the project, the project phase, resources available,regulatory requirements and client requirements as to objectives, desired outcome and the requiredlevel of detail.

The use of the following tools and techniques may further assist the identification of risks:

− Examples of possible risk sources,

− Checklist of possible business risks and fraud risks,

− Typical risks in stages of the procurement process,

− Scenario planning as a risk assessment tool,

− Process mapping, and

− Documentation, relevant audit reports, program evaluations and / or research reports.

Specific lists, e.g. from standards, and organizational experience support the identification ofinternal risks. To collect experience available in the organization regarding internal risks, peoplewith appropriate knowledge from the different parts of the organization should be involved inidentifying risks. Creativity tools support this group process (see Fig. 3).

The identification of the sources of the risk is the most critical stage in the risk assessmentprocess. The sources are needed to be managed for pro-active risk management. The better theunderstanding of the sources, the better the outcomes of the risk assessment process and the moremeaningful and effective will be the management of risks.

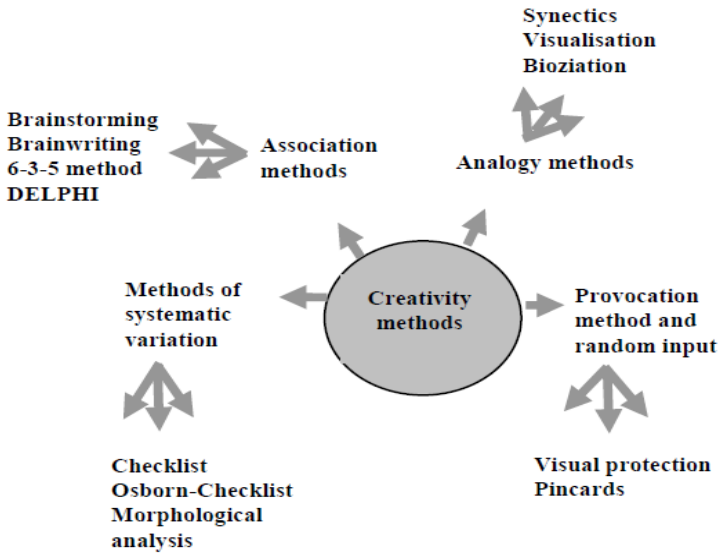

Fig. 3: Creativity tools.

Key questions to ask at this stage of the risk assessment process to identify the impact of therisk are:

− Why is this event a risk?

− What happens if the risk eventuates?

− How can it impact on achieving the objectives/outcomes?

Risk identification of a particular system, facility or activity may yield a very large number ofpotential accidental events and it may not always be feasible to subject each one to detailedquantitative analysis. In practice, risk identification is a screening process where events with low ortrivial risk are dropped from further consideration. However, the justification for the events not studied in detail should be given. Quantificationis then concentrated on the events which will give rise to higher levels of risk. Fundamental methods such as Hazard and Operability (HAZOP) studies, fault trees, event tree logic diagramsand Failure Mode and Effect Analysis (FMEA) are tools which can be used to identify the risks andassess the criticality of possible outcomes. An example of a systematic method for identifying technical risks of a plant is the elaborationof a risk register where different types of risks and damage classes are correlated to local areas of aplant (see Fig. 4).

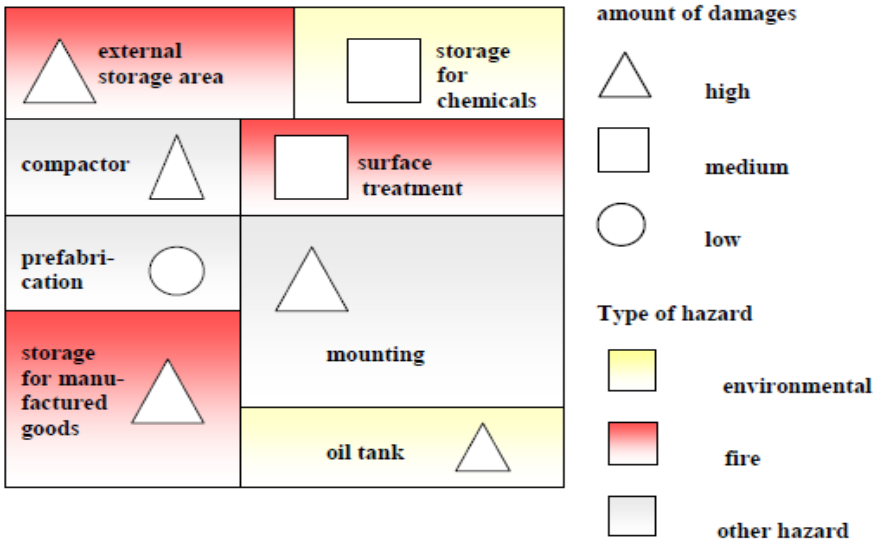

Fig. 4: Example of a risk register.

2.3 Analyse the risk

Risk analysis involves the consideration of the source of risk, the consequence and likelihoodto estimate the inherent or unprotected risk without controls in place. It also involves identificationof the controls, an estimation of their effectiveness and the resultant level of risk with controls inplace (the protected, residual or controlled risk). Qualitative, semi-quantitative and quantitativetechniques are all acceptable analysis techniques depending on the risk, the purpose of the analysisand the information and data available.

Often qualitative or semi-quantitative techniques can be used for screening risks whereashigher risks are being subjected to more expensive quantitative techniques as required. Risks can beestimated qualitatively and semi-quantitatively using tools such as hazard matrices, risk graphs, riskmatrices or monographs but noting that the risk matrix is the most common. Applying the risk matrix, it is required to define for each risk its profile using likelihood andconsequences criteria. Typical definitions of the likelihood and consequence are contained in therisk matrix (see Table 1). Using the consequence criteria provided in the risk matrix, one has to determine theconsequences of the event occurring (with current controls in place).

To determine the likelihood of the risk occurring, one can apply the likelihood criteria (againcontained in the risk matrix). As before, the assessment is undertaken with reference to theeffectiveness of the current control activities. To determine the level of each risk, one can again refer to the risk matrix. The risk level isidentified by intersecting the likelihood and consequence levels on the risk matrix.

Complex risks may involve a more sophisticated methodology. For example, a differentapproach may be required for assessing the risks associated with a significantly large procurement.

Table 1: Example of a risk matrix

Risk Rating Matirx

	Likelihood				
Impact	Rare	Unlikely	Possible	Likely	Almost certain
Catastrophic	moderate	moderate	high	critical	critical
Major	low	moderate	moderate	high	critical
Moderate	low	moderate	moderate	moderate	high
Minor	very low	low	moderate	moderate	moderate
Insignificant	very low	very low	low	low	moderate

Special approaches exist to analyse major risk in complex projects, e.g. described in (Cagnoet al. 2007).

2.4 Evaluate the risk

Once the risks have been analysed they can be compared against the previously documentedand approved tolerable risk criteria. When using risk matrices this tolerable risk is generallydocumented with the risk matrix. Should the protected risk be greater than the tolerable risk then thespecific risk needs additional control measures or improvements in the effectiveness of the existingcontrols.

The decision of whether a risk is acceptable or not acceptable is taken by the relevantmanager. A risk may be considered acceptable if for example:

- The risk is sufficiently low that treatment is not considered cost effective, or
- A treatment is not available, e.g. a project terminated by a change of government, or
- A sufficient opportunity exists that outweighs the perceived level of threat.

If the manager determines the level of risk to be acceptable, the risk may be accepted with nofurther treatment beyond the current controls. Acceptable risks should be monitored andperiodically reviewed to ensure they remain acceptable. The level of acceptability can beorganizational criteria or safety goals set by the authorities.

2.5 Treat the risk

An unacceptable risk requires treatment. The objective of this stage of the risk assessmentprocess is to develop cost effective options for treating the risks. Treatment options (see Fig. 5),which are not necessarily mutually exclusive or appropriate in all circumstances, are driven byoutcomes that include:

- Avoiding the risk,
- Reducing (mitigating) the risk,
- Transferring (sharing) the risk, and
- Retaining (accepting) the risk.

Avoiding the risk - not undertaking the activity that is likely to trigger the risk.

Reducing the risk - controlling the likelihood of the risk occurring, or controlling the impactof the consequences if the risk occurs.

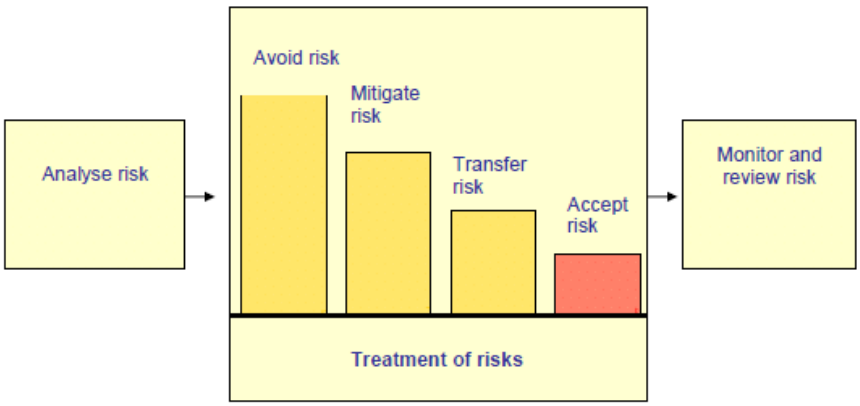

Fig. 5: Treatment of risks

Factors to consider for this risk treatment strategy include:

- Can the likelihood of the risk occurring be reduced? (through preventative maintenance, orquality assurance and management, change in business systems and processes), or
- Can the consequences of the event be reduced? (through contingency planning, minimizingexposure to sources of risk or separation/relocation of an activity and resources).

Examples for the mitigation activity effectiveness are described in (Wirthin 2006).

Transferring the risk totally or in part - This strategy may be achievable through moving theresponsibility to another party or sharing the risk through a contract, insurance, or partnership/jointventure. However, one should be aware that a new risk arises in that the party to whom the risk istransferred may not adequately manage the risk!

Retaining the risk and managing it - Resource requirements feature heavily in this strategy.

The next step is to determine the target level of risk resulting from the successfulimplementation of the preferred treatments and current control activities.
The intention of a risk treatment is to reduce the expected level of an unacceptable risk. Usingthe risk matrix one can determine the consequence and likelihood of the risk and identify theexpected target risk level.

2.6 Monitoring the risk

It is important to understand that the concept of risk is dynamic and needs periodic and formal review. The currency of identified risks needs to be regularly monitored. New risks and their impact on the organization may to be taken into account.

This step requires the description of how the outcomes of the treatment will be measured. Milestones or benchmarks for success and warning signs for failure need to be identified.
The review period is determined by the operating environment (including legislation), but as ageneral rule a comprehensive review every five years is an accepted industry norm. This is on thebasis that all plant changes are subject to an appropriate change process including risk assessment.
The review needs to validate that the risk management process and the documentation is still valid. The review also needs to consider the current regulatory environment and industry practices which may have changed significantly in the intervening period.

The organisation, competencies and effectiveness of the safety management system should also be covered. The plant management systems should have captured these changes and the reviewshould be seen as a 'back stop'.

The assumptions made in the previous risk assessment (hazards, likelihood and consequence), the effectiveness of controls and the associated management system as well as people need to be monitored on an on-going basis to ensure risk are in fact controlled to the underlying criteria.
For an efficient risk control the analysis of risk interactions is necessary.

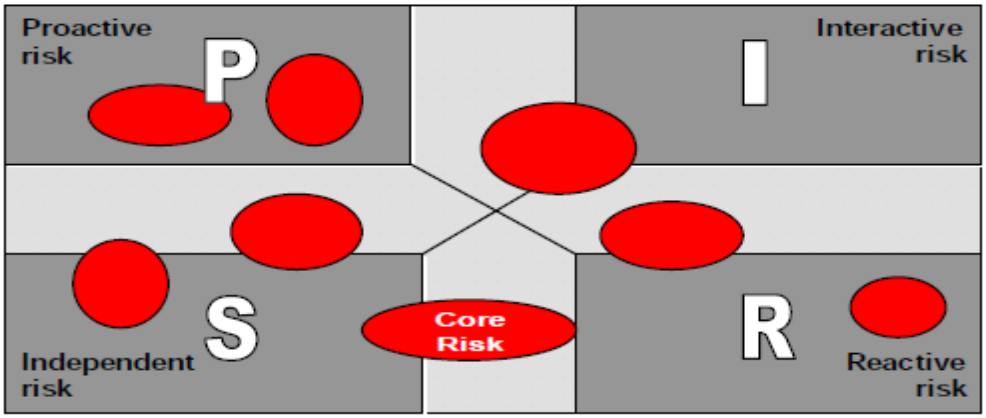

Fig. 6: Results of a cross impact analysis.

This ensures that the influences of one risk to another is identified and assessed. Usual method for that purpose are a cross impact analysis (see Fig. 6), Petri nets or simulation tools.
A framework needs to be in place that enables responsible officers to report on the followingaspects of risk and its impact on organizations´ operations:

- What are the key risks?
- How are they being managed?
- Are the treatment strategies effective? – If not, what else must be undertaken?
- Are there any new risks and what are the implications for the organization?

2.7 Communication and reporting

Clear communication is essential for the risk management process, i.e. clear communicationof the objectives, the risk management process and its elements, as well as the findings and requiredactions as a result of the output.

Risk management is an integral element of organization´s management. However, for itssuccessful adoption it is important that in its initial stages, the reporting on risk management isvisible through the framework. The requirements on the reporting have to be fixed in a qualifiedand documented procedure, e. g., in a management handbook. The content of such a handbook isshown in Figure 7.

Fig. 7: Structure of a risk management handbook.

Documentation is essential to demonstrate that the process has been systematic, the methodsand scope identified, the process conducted correctly and that it is fully auditable. Documentationprovides a rational basis for management consideration, approval and implementation including anappropriate management system.
A documented output from the above sections (risk identification, analysis, evaluation andcontrols) is a risk register for the site, plant, equipment or activity under consideration. Thisdocument is essential for the on-going safe management of the plant and as a basis forcommunication throughout the client organisation and for the on-going monitor and reviewprocesses. It can also be used with other supporting documents to demonstrate regulatorycompliance.

III. RISK CONTROL

Urgent action is required for risks assessed as Critical or High risks. The actions required may include:
- Instructions for the immediate cessation of the work, process, activity, etc.
- Isolation of the hazard until more permanent measures can be implemented.

Documented control plans with responsibilities and completion dates may need to be developed for Moderate risks. Having established the relative importance of dealing with the identified risk, the risk control hierarchy ranks possible risk control measures in decreasing order of effectiveness. Risk control measures should always aim as high in the list as practicable. Control of any given risk generally involves a number of measures drawn from the various options (except if option 1 is selected).

3.1 Risk Control Hierarchy

G. Elimination of hazard: examples include the proper disposal of redundant items of equipment that contain substances such as asbestos or PCBs, the removal of excess quantities of chemical accumulated over time in a laboratory, etc. The elimination of hazards is 100% effective
H. Substitution of hazard: examples include the replacement of solvent-based printing inks with water-based ones, of asbestos insulation or fire-proofing with synthetic fibres or rock wool, the use of titanium dioxide white pigment instead of lead white, etc. The effectiveness of substitution is wholly dependent on the choice of replacement.
I. Isolation of hazard: examples include placing a particular piece of machinery in a place where only trained staff are required to interact with it (i.e removing or separating workers from a particular hazard where possible).
J. Engineering controls: examples include the installation of machine guards on hazardous equipment, the provision of local exhaust ventilation over a process area releasing noxious fumes, fitting a muffler on a noisy exhaust pipe, etc. The effectiveness of engineering solutions is around 70–90%.
K. Administrative controls: include training and education, job rotation to share the load created by demanding tasks, planning, scheduling certain jobs outside normal working hours to reduce general exposure (eg planning demolition and building works during summer recess), early reporting of signs and symptoms, instructions and warnings, etc. The effectiveness of administrative controls ranges from 10 to 50%. They typically require significant resources to be maintained over long periods of time for continuing levels of effectiveness.

L. Personal protective equipment: includes safety glasses and goggles, earmuffs and earplugs, hard hats, toe-capped footwear, gloves, respiratory protection, aprons, etc. Their effectiveness in realistic work situations does not exceed 20%.

You will need to develop work procedures in relation to the new control measures, which may involve clearly defining responsibilities of management, supervisors and workers.
If, like many businesses, you find there are quite a lot of improvements that you could make, big and small, don't try to do everything at once. Make a plan of action to deal with the most important things first. Health and safety inspectors acknowledge the efforts of businesses that are clearly trying to make improvements.
A good plan of action often includes a mixture of different things such as:
priority and quick attention to hazards associated with high or critical risks
a few cheap or easy improvements that can be done quickly, perhaps as a temporarysolution until more reliable controls are in place long-term solutions to those risks most likely to cause accidents or ill health long-term solutions to those risks with the worst potential consequences arrangements for training workers on the main risks that remain and how they are to be controlled regular checks to make sure that the control measures stay in place; and clear responsibilities – who will lead on what action, and by when.

Remember, prioritise and tackle the most important things first. As you complete each action, tick it off your plan. You should inform all relevant persons about the control measures being implemented, in particular, the reasons for the changes. You should also provide adequate supervision to verify that the new control measures are being implemented and used correctly. Any maintenance in relation to the control measures is an important part of the process. Work procedures should detail maintenance requirements and verification of the maintenance to ensure the ongoing effectiveness of the control measures.

3.2 Documenting the Process

Documenting the process will help ensure that identified control measures are implemented in the way that they were intended. It will also assist in managing other hazards and risks that may be in some way similar to ones already identified and dealt with. Adequate record keeping of the risk management process will also help demonstrate to the Office of Regulatory Services, or in litigation, that you have been actively working to ensure safety at your workplace. Records should show that the process has been conducted properly including information about the hazards, associated risks and control measures that have been implemented. Information should include:

- hazards identified
- assessment of the risks associated with those hazards
- decisions on control measures to manage exposure to the risks
- how and when the control measures are implemented
- evidence of monitoring and review of the effectiveness of the controls any checklist used in the process.

3.3 Monitoring and Reviewing

Whichever method of controlling the hazard is determined, it is essential that an evaluation of its impact on the use of the equipment, substance, system or environment is carried out to ensure that the control does not contribute to the existing hazard or introduce a new hazard to the area. It is also essential that all people concerned be informed about the changes and where necessary provided with the appropriate information, instruction, training and supervision as are reasonably necessary to ensure that each worker is safe from injury and risks to health. It is also recommended that after a period of time the area supervisor carry out a review of the system or control to determine its suitability.

Hazard identification and risk assessment and control are ongoing processes. Make sure that you undertake a hazard identification and risk assessment and control process when there is a change to the workplace, including when work systems, tools, machinery or equipment changes occur, or simply when the existing process was done some time ago and is potentially out of date or no longer valid

IV. DESCRIPTION

4.1 Nigerian Civil Aviation Authority (NCAA) risk management to the NCATprogramm

NCAA and NASRDA have been working together to create Nigerian College of Aviation Technology (NCAT). NCAT is a Boing 747SP (SpecialPerformance) aircraft, extensively modified to accommodate a 2.5 meter reflecting telescope andairborne mission control system. In (Datta 2007) it is shown how the NCAT program handled onesafety issue through appropriate use of NCAT`s Risk Management Process based on (NCAT 2002).

4.1.1 Risk identification

The safety issue was identified while reviewing the Probabilistic Risk Assessment of adepressurization scenario in the telescope cavity. The failure scenario itself was previously knownwhere a leak in the telescope cavity door seal sucks air out from the telescope cavity creating anegative pressure differential between the telescope cavity and the aft cavity. Two negative pressurerelief valves were designed to handle this and other cavity negative pressure scenarios. However,the proposed new scenario had a leak area that was beyond the original design basis. Nevertheless,this failure scenario was deemed credible but with a lower probability of occurrence.

4.1.2 Risk analysis

After identification of the safety issue, both the risk management and the engineeringprocesses required an analysis of this depressurization scenario. Multiple models of thedepressurization scenarios were created and analyzed at peak dynamic pressures. The resultsrevealed that under some failure scenarios the relief valves might not be redundant. Both valvesneed to function for adequate pressure equalization without exceeding structural design loads.These conditions created a program risk state that needed to be mitigated.
All considerations within the risk analysis were based on prescribed project risk definitions.

4.1.3 Risk control

As a result, the program started a risk mitigation plan where a test will be performed tocharacterize the seal failure scenario by intentionally deflating the seal at lower dynamic pressure. This risk continues to reside in the NCAT program risk list so as to ensure that the riskmitigation plan is carried out in the future. The risk list is the listing of all identified risks in priorityorder from highest to lowest risk, together with the information that is needed to manage each riskand document its evolution over the course of the program. The highest risks are extracted from thelist. The negative pressure relief valve risk has not yet reached among the top fifteen list of risks(Datta 2007).

V. CONCLUSION

Risk management is, at present, implemented in many large as well as small and mediumsized industries. In (Gustavsson 2006) it is outlined how a large company can handle its risks inpractice and contains a computer based method for risk analysis that can generate basic data fordecision-making in the present context. In that study, Trelleborg AB has been chosen as an exampleto illustrate the difficulties that can be encountered concerning risk management in a large companywith different business areas. One typical difficulty is reaching the personnel. Another typicalweakness is a missing system for controlling and following up on the results of the risk analysis thathas been performed.

However, not only industries but also governmental organizations, research institutes andhospitals are now introducing risk management to some extent.

In case of hospitals, patient safety is endangered, e. g., by adverse events during medicaltreatment. Patient safety can be increased through risk management which reduces errors througherror prevention. This presupposes the recognition of causes for errors and near misses which canbe achieved through a critical incident reporting system (CIRS) with a detailed incident reportingform. CIRS is seen as an important instrument in the process of risk management and is, at present,of increasing importance.
Why is it important to have risk management in mind when performing risk assessment? Thedifferent tools support the answer to the following questions:

- risk analysis – how safe is the system, process or item to be investigated,
- risk evaluation – how safe is safe enough, e.g. by comparing the results of the risk analysiswith prescribed safety criteria,
- risk management – how to achieve and ensure an adequate level of safety.

Thus, the results of technical risk assessments are one (often very important) part of an overallrisk or safety assessment of an organization.

REFERENCES

[1] ACT Insurance Authority 2004. *Risk Management Toolkit.* February 2004.
[2] AZ/NZS 4360 2004. Risk Management. Standards Australia International Ltd, Sydney.
[3] Basel Committee on Banking Supervision 2003. Trends in Risk Integration and Aggregation, Basel,August 2003.
[4] Bolvin C., Farret, R., Salvi, O. 2007. Convergence towards integrated risk management: results fromthe European SHAPE-RISK project and other initiatives. Proc. ESREL 2007: 1683 – 1687.
[5] Cagno, E., Caron, F., &Mancini, M. 2007.A multi-dimensional analysis of major risks in complexprojects. Risk Management: 1–18.
[6] Committee for European Banking Supervisors 2005. Consultation Paper on the Supervisory ReviewProcess under Pillar II of the Revised Basel Accord, Basel II), June 2005.
[7] Committee of Sponsoring Organizations of the Treadway Commission (ed.) 2004.Enterprise Risk Management – Integrated Framework – Application Techniques. September 2004.

[8] Datta, K. 2007. The application of the NASA risk management to the SOFIA program.Proc.
[9] Reliability and Maintainability Symposium 2007, Orlando, January 2007, 410 – 413.
[10] ICBNU 2004,A Risk Management StandardJune 2004.
[11] Gustavsson, H. 2006. A Risk Management Framework Designed for Trelleborg AB. Report 5195.
[12] HB 436 2004.Handbook Risk Management Guidelines. Standards Australia International Ltd.,
[13] Sydney 2004.
[14] Hess, S.M.,&Gaertner, J. P. 2006.Application of risk management as a cornerstone in ensuringnuclear plant safety.Proc. of the 8th International Conference on Probabilistic Safety Assessment and Management, May, 14 – 18, 2006, New Orleans, paper PSAM-0477.
[15] International Electrotechnical Commission (IEC) 2008. Draft IEC 31010 Ed. 1.0, Risk Management– Risk Assessment Techniques. May 2008.
[16] International Standardization Organization 2007. Draft ISO 31000, Risk Management Guidelines onPrinciples and Implementation of Risk Management. Final version to be issued in 2009.
[17] NCAT 2002.Risk Management Procedural Requirements. NPR 8000.4, April 2002.
[18] Oehmen, J. 2005. Approaches to Crisis Prevention in Lean Product Development by High Performance Teams and through Risk Management. Munich, September 2005.
[19] OesterreichischesNormungsinstitut (ON) 2008.ONR 49000 RisikomanagementfürOrganisationen und Systeme. (in German).
[20] Rheinland-Pfalz 2008.SGU-Leitfaden. (in German).
[21] Rio Tinto 2007. Risk Policy and Standard. August 2007.
[22] Treasury Board of Canada 2001.Integrated Risk Management Framework. April 2001.
[23] Wirthin, R. 2006. Managing Risk and Uncertainty: Traditional Methods and the Lean Enterprise. MIT/LAI, Presentation April 18, 2006.
[24] World Economic Forum (WEF) 2008. Global Risks 2008, A Global Risk Network Report. Cologny/Geneva, January 2008.

Engr. Dr. Uzorh. “Assessing and Controlling Risk in Industrial Organization .” International Journal of Engineering Science Invention (IJESI), vol. 6, no. 8, 2017, pp. 68–79.