Subject: Tech.inf 2018-02

Offshore Operations Risk Assessment For MWS.

Number: 32/96/0090

Date: 16.01.2018

موضوع:اطلاعیه فنی ۲۰۱۸-۰۲

ارزیابی ریسک در عملیاتهای فراساحلی برای بازرسان تضمین عملیات

شماره: ۳۲/۹۶/۰۰۹۰

تاریخ : ۱۳۹۶/۱۰/۲۶

All respectful ICS' Surveyors
With Gratitude,

With respect to need of the attitude based on risk in offshore operations, the attached technical information about Offshore Operations Risk Assessment for MWS, has been sent for your kind information.

The electronic file of this document could be found at the following address:

\\server\ICS Organization\Convention and Legislation Department\Publications\ Tech\tech.inf 2018-02

Also this Electronic File will be sent via email to all respectful ICS Surveyors.

A.M.Rezvan Panah
Manager of Convention & Legislation Department
ICS

Disclaimer: Although all possible efforts have been made to ensure correctness and completeness of the information and guides contained in this technical information, the Iranian classification society is not responsible for any errors ,damages ,penalties or emissions made herein, nor held for any actions taken by any party as a result of information retrieved from this technical information.

کلیه بازرسان محترم ICS

با سلام و احترام

با توجه به ضرورت نگرش بر مبنای ریسک در عملیات دریایی، بپیوست اطلاعیه فنی در خصوص ارزیابی ریسک در عملیاتهای فراساحلی برای بازرسان تضمین عملیات، حضورتان ایفاد می گردد.

نسخه الکترونیکی اطلاعیه فنی مذکور در شبکه داخلی موسسه با آدرس ذیل قابل دسترسی می‌باشد:

server\ICS Organization\Convention and Legislation Department\Publications\Tech\tech.inf 2018-02

همچنین نسخه الکترونیکی این سند از طریق پست الکترونیکی به کلیه مشتریان و بازرسان محترم موسسه ارسال می گردد.

رضوان پناه

مدیر واحد کنوانسیون ها و مقررات دریایی

موسسه رده بندی ایرانیان

ترک دعوی: اگرچه در گردآوری کلیه راهنماهای فنی ارائه شده توسط موسسه رده بندی ایرانیان ،تا حد ممکن تلاش در دقت و صحت محتوا صورت گرفته است،این موسسه متحمل مسئولیتی در قبال هرگونه اشتباهات ،خسارت های احتمالی و جرائمی که ممکن است در ارتباط با بکار گیری مفاهیم و مطالب ارائه شده رخ دهد،نمیباشد.

Code: ICS32F016/2

Offshore Operations Risk Assessment for Marine Warranty Surveyors:

The objective of risk assessment for marine warranty surveyors is to identify and mitigate risks to an acceptable level. If the risks cannot be mitigated to an acceptable level the work should not proceed in its present form.

Each party involved in an operation must have in place an appropriate procedure for carrying out their own risk assessments, if appropriate.

Risk Assessments should include all parties involved in the operations to which they relate.

Risk Assessment should be performed for the complete process or operation and should include relevant emergency response arrangements.

Personnel performing the Risk Assessment must be trained and competent in this matter.

Risk Assessments should identify the following:

1. All hazards associated with the proposed operation.
2. The probability of a hazard causing harm to personnel, assets or environment.
3. The likely extent of the harm that may be caused.
4. Mitigation measures.
5. Assessment of the residual risk.

Associated with Item 4 above trigger points or any other changes in circumstances which will prompt the work being stopped or the management of change process being invoked should be identified.

Personnel performing tasks are required to understand the outcome of the Risk Assessment, including trigger points or other changes which would require the management of change process to be initiated.

All relevant parties are responsible for ensuring that the Risk Assessment is suitable and sufficient for their own particular tasks.

Definition of Risk

Basic Expressions of Risk

The term ‘risk’ is according to international standards (such as ISO 2002) ‘combination of the probability or an event and its consequence’. Other standards, like ISO 13702 (ISO 1999b), have a similar definition: ‘A

term which combines the chance that a specified hazardous event will occur and the severity of the consequences of the event.'

Risk may be expressed in several ways, by distributions, expected values, single probabilities of specific consequences, etc. Most commonly used is probably the expected value.

Organizations of all types and sizes face a range of risks that may affect the achievement of their objectives. These objectives may relate to a range of the organization's activities, from strategic initiatives to its operations, processes and projects, and be reflected in terms of societal, environmental, technological, safety and security outcomes, commercial, financial and economic measures, as well as social, cultural, political and reputation impacts.

All activities of an organization involve risks that should be managed. The risk management process aids decision making by taking account of uncertainty and the possibility of future events or circumstances (intended or unintended) and their effects on agreed objectives.

Risk management includes the application of logical and systematic methods for:

- ✓ communicating and consulting throughout this process;
- ✓ establishing the context for identifying, analyzing, evaluating, treating risk associated with any activity, process, function or product;
- ✓ monitoring and reviewing risks;
- ✓ reporting and recording the results appropriately.

Risk assessment is that part of risk management which provides a structured process that identifies how objectives may be affected, and analyses the risk in term of consequences and their probabilities before deciding on whether further treatment is required.

Risk assessment attempts to answer the following fundamental questions:

- ✓ what can happen and why (by risk identification)?
- ✓ what are the consequences?
- ✓ what is the probability of their future occurrence?
- ✓ are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?

Is the level of risk tolerable or acceptable and does it require further treatment? This standard is intended to reflect current good practices in selection and utilization of risk assessment techniques, and does not refer to new or evolving concepts which have not reached a satisfactory level of professional consensus.

This standard is general in nature, so that it may give guidance across many industries and types of system. There may be more specific standards in existence within these industries that establish preferred methodologies and levels of assessment for particular applications. If these standards are in harmony with this standard, the specific standards will generally be sufficient.

Risk assessment concepts

Purpose and benefits

The purpose of risk assessment is to provide evidence-based information and analysis to make informed decisions on how to treat particular risks and how to select between options.

Some of the principal benefits of performing risk assessment include:

- ✓ understanding the risk and its potential impact upon objectives;
- ✓ providing information for decision makers;
- ✓ contributing to the understanding of risks, in order to assist in selection of treatment options;
- ✓ identifying the important contributors to risks and weak links in systems and organizations;
- ✓ comparing of risks in alternative systems, technologies or approaches;
- ✓ communicating risks and uncertainties;
- ✓ assisting with establishing priorities;
- ✓ contributing towards incident prevention based upon post-incident investigation;
- ✓ selecting different forms of risk treatment;
- ✓ meeting regulatory requirements;
- ✓ providing information that will help evaluate whether the risk should be accepted when compared with pre-defined criteria;
- ✓ assessing risks for end-of-life disposal.

Risk assessment and the risk management framework

A risk management framework provides the policies, procedures and organizational arrangements that will embed risk management throughout the organization at all levels.

As part of this framework, the organization should have a policy or strategy for deciding when and how risks should be assessed.

In particular, those carrying out risk assessments should be clear about:

- ✓ the context and objectives of the organization,
- ✓ the extent and type of risks that are tolerable, and how unacceptable risks are to be treated,
- ✓ how risk assessment integrates into organizational processes,
- ✓ methods and techniques to be used for risk assessment, and their contribution to the risk management process,

- ✓ accountability, responsibility and authority for performing risk assessment,
- ✓ resources available to carry out risk assessment,
- ✓ how the risk assessment will be reported and reviewed.

Risk assessment and the risk management process

Risk assessment comprises the core elements of the risk management process which are defined in ISO 31000 and contain the following elements:

- ✓ communication and consultation;
- ✓ establishing the context;
- ✓ risk assessment (comprising risk identification, risk analysis and risk evaluation);
- ✓ risk treatment;
- ✓ monitoring and review.

Risk assessment is not a stand-alone activity and should be fully integrated into the other components in the risk management process.

Communication and consultation

Successful risk assessment is dependent on effective communication and consultation with stakeholders.

Involving stakeholders in the risk management process will assist in

- ✓ developing a communication plan,
- ✓ defining the context appropriately,
- ✓ ensuring that the interests of stakeholders are understood and considered,
- ✓ bringing together different areas of expertise for identifying and analyzing risk,
- ✓ ensuring that different views are appropriately considered in evaluating risks,
- ✓ ensuring that risks are adequately identified,
- ✓ securing endorsement and support for a treatment plan.

Stakeholders should contribute to the interfacing of the risk assessment process with other management disciplines, including change management, project and program management, and also financial management.

Establishing the context

Establishing the context defines the basic parameters for managing risk and sets the scope and criteria for the rest of the process. Establishing the context includes considering internal and external parameters relevant to the organization as a whole, as well as the background to the particular risks being assessed.

In establishing the context, the risk assessment objectives, risk criteria, and risk assessment program are determined and agreed.

For a specific risk assessment, establishing the context should include the definition of the external, internal and risk management context and classification of risk criteria:

a) Establishing the external context involves familiarization with the environment in which the organization and the system operates including:

- ✓ cultural, political, legal, regulatory, financial, economic and competitive environment factors, whether international, national, regional or local;
- ✓ key drivers and trends having impact on the objectives of the organization; and
- ✓ perceptions and values of external stakeholders.

b) Establishing the internal context involves understanding

- ✓ capabilities of the organization in terms of resources and knowledge,
- ✓ information flows and decision-making processes,
- ✓ internal stakeholders,
- ✓ objectives and the strategies that are in place to achieve them,
- ✓ perceptions, values and culture,
- ✓ policies and processes,
- ✓ standards and reference models adopted by the organization, and
- ✓ structures (e.g. governance, roles and accountabilities).

c) Establishing the context of the risk management process includes

- ✓ defining accountabilities and responsibilities,
- ✓ defining the extent of the risk management activities to be carried out, including specific inclusions and exclusions,
- ✓ defining the extent of the project, process, function or activity in terms of time and location,
- ✓ defining the relationships between a particular project or activity and other projects or activities of the organization,
- ✓ defining the risk assessment methodologies,
- ✓ defining the risk criteria,
- ✓ defining how risk management performance is evaluated,
- ✓ identifying and specifying the decisions and actions that have to be made, and
- ✓ identifying scoping or framing studies needed, their extent, objectives and the resources required for such studies.

d) Defining risk criteria involves deciding

- ✓ the nature and types of consequences to be included and how they will be measured,
- ✓ the way in which probabilities are to be expressed,
- ✓ how a level of risk will be determined?
- ✓ the criteria by which it will be decided when a risk needs treatment,
- ✓ the criteria for deciding when a risk is acceptable and/or tolerable,
- ✓ whether and how combinations of risks will be taken into account.

Criteria can be based on sources such as

- ✓ agreed process objectives,
- ✓ criteria identified in specifications,
- ✓ general data sources,
- ✓ generally accepted industry criteria such as safety integrity levels,
- ✓ organizational risk appetite,
- ✓ legal and other requirements for specific equipment or applications.

Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risks can be assessed at an organizational level, at a departmental level, for projects, individual activities or specific risks. Different tools and techniques may be appropriate in different contexts.

Risk assessment provides an understanding of risks, their causes, consequences and their probabilities. This provides input to decisions about:

- ✓ whether an activity should be undertaken;
- ✓ how to maximize opportunities;
- ✓ whether risks need to be treated;
- ✓ choosing between options with different risks;
- ✓ prioritizing risk treatment options;
- ✓ the most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level.

Risk treatment

Having completed a risk assessment, risk treatment involves selecting and agreeing to one or more relevant options for changing the probability of occurrence, the effect of risks, or both, and implementing these options.

This is followed by a cyclical process of reassessing the new level of risk, with a view to determining its tolerability against the criteria previously set, in order to decide whether further treatment is required.

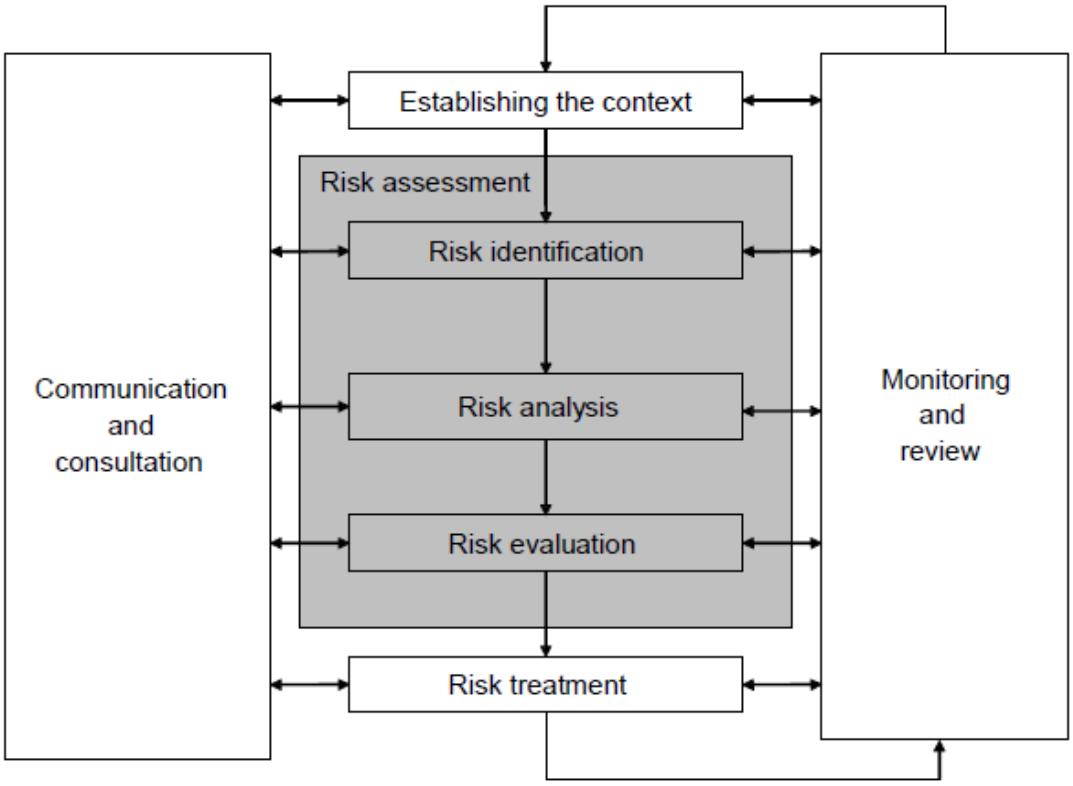
Monitoring and review

As part of the risk management process, risks and controls should be monitored and reviewed on a regular basis to verify that

- ✓ assumptions about risks remain valid;
- ✓ assumptions on which the risk assessment is based, including the external and internal context, remain valid;
- ✓ expected results are being achieved;
- ✓ results of risk assessment are in line with actual experience;
- ✓ risk assessment techniques are being properly applied;
- ✓ risk treatments are effective.

Accountability for monitoring and performing reviews should be established.

Risk assessment process



Risk assessment provides decision-makers and responsible parties with an improved understanding of risks that could affect achievement of objectives, and the adequacy and effectiveness of controls already in place. This provides a basis for decisions about the most appropriate approach to be used to treat the risks. The output of risk assessment is an input to the decision-making processes of the organization.

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. The manner in which this process is applied is dependent not only on the context of the risk management process but also on the methods and techniques used to carry out the risk assessment.

Risk assessment may require a multidisciplinary approach since risks may cover a wide range of causes and consequences.

Risk identification

Risk identification is the process of finding, recognizing and recording risks.

The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organization. Once a risk is identified, the organization should identify any existing controls such as design features, people, processes and systems.

The risk identification process includes identifying the causes and source of the risk (hazard in the context of physical harm), events, situations or circumstances which could have a material impact upon objectives and the nature of that impact Risk identification methods can include:

- ✓ evidence based methods, examples of which are check-lists and reviews of historical data;
- ✓ systematic team approaches where a team of experts follow a systematic process to identify risks by means of a structured set of prompts or questions;
- ✓ inductive reasoning techniques such as HAZOP.

Various supporting techniques can be used to improve accuracy and completeness in risk identification, including brainstorming, and Delphi methodology.

Irrespective of the actual techniques employed, it is important that due recognition is given to human and organizational factors when identifying risk. Hence, deviations of human and organizational factors from the expected should be included in the risk identification process as well as "hardware" or "software" events.

Risk analysis

Risk analysis is about developing an understanding of the risk. It provides an input to risk assessment and to decisions about whether risks need to be treated and about the most appropriate treatment strategies and methods.

Risk analysis consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls. The consequences and their probabilities are then combined to determine a level of risk.

Risk analysis involves consideration of the causes and sources of risk, their consequences and the probability that those consequences can occur. Factors that affect consequences and probability should be identified. An event can have multiple consequences and can affect multiple objectives. Existing risk controls and their effectiveness should be taken into account.

Risk analysis normally includes an estimation of the range of potential consequences that might arise from an event, situation or circumstance, and their associated probabilities, in order to measure the level of risk. However, in some instances, such as where the consequences are likely to be insignificant, or the probability is expected to be extremely low, a single parameter estimate may be sufficient for a decision to be made conditions, or where the specific event is not identified. In this case, the focus of risk assessment is on analyzing the importance and vulnerability of components of the system with a view to defining treatments which relate to levels of protection or recovery strategies.

Methods used in analyzing risks can be qualitative, semi-quantitative or quantitative. The degree of detail required will depend upon the particular application, the availability of reliable data and the decision-making needs of the organization. Some methods and the degree of detail of the analysis may be prescribed by legislation.

Qualitative assessment defines consequence, probability and level of risk by significance levels such as “high”, “medium” and “low”, may combine consequence and probability, and evaluates the resultant level of risk against qualitative criteria.

Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship; formulae used can also vary.

Quantitative analysis estimates practical values for consequences and their probabilities, and produces values of the level of risk in specific units defined when developing the context. Full quantitative analysis may not always be possible or desirable due to insufficient information about the system or activity being analyzed, lack of data, influence of human factors, etc. or because the effort of quantitative analysis is not warranted or required. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

In cases where the analysis is qualitative, there should be a clear explanation of all the terms employed and the basis for all criteria should be recorded.

Even where full quantification has been carried out, it needs to be recognized that the levels of risk calculated are estimates. Care should be taken to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and methods employed.

Levels of risk should be expressed in the most suitable terms for that type of risk and in a form that aids risk evaluation. In some instances, the magnitude of a risk can be expressed as a probability distribution over a range of consequences.

Controls assessment

The level of risk will depend on the adequacy and effectiveness of existing controls.

Questions to be addressed include:

- ✓ what are the existing controls for a particular risk?
- ✓ are those controls capable of adequately treating the risk so that it is controlled to a level that is tolerable?
- ✓ in practice, are the controls operating in the manner intended and can they be demonstrated to be effective when required?

These questions can only be answered with confidence if there are proper documentation and assurance processes in place.

The level of effectiveness for a particular control, or suite of related controls, may be expressed qualitatively, semi-quantitatively or quantitatively. In most cases, a high level of accuracy is not warranted. However, it may be valuable to express and record a measure of risk control effectiveness so that judgments can be made on whether effort is best expended in improving a control or providing a different risk treatment.

Consequence analysis

Consequence analysis determines the nature and type of impact which could occur assuming that a particular event situation or circumstance has occurred. An event may have a range of impacts of different magnitudes, and affect a range of different objectives and different stakeholders. The types of consequence to be analyzed and the stakeholders affected will have been decided when the context was established.

Consequence analysis can vary from a simple description of outcomes to detailed quantitative modelling or vulnerability analysis.

Impacts may have a low consequence but high probability, or a high consequence and low probability, or some intermediate outcome. In some cases, it is appropriate to focus on risks with potentially very large

outcomes, as these are often of greatest concern to managers. In other cases, it may be important to analyses both high and low consequence risks separately.

For example, a frequent but low-impact (or chronic) problem may have large cumulative or long-term effects. In addition, the treatment actions for dealing with these two distinct kinds of risks are often quite different, so it is useful to analyze them separately.

Consequence analysis can involve:

- ✓ taking into consideration existing controls to treat the consequences, together with all relevant contributory factors that have an effect on the consequences;
- ✓ relating the consequences of the risk to the original objectives;
- ✓ considering both immediate consequences and those that may arise after a certain time has elapsed, if this is consistent with the scope of the assessment;
- ✓ considering secondary consequences, such as those impacting upon associated systems, activities, equipment or organizations.

Likelihood analysis and probability estimation

Three general approaches are commonly employed to estimate probability; they may be used individually or jointly:

a) The use of relevant historical data to identify events or situations which have occurred in the past and hence be able to extrapolate the probability of their occurrence in the future.

The data used should be relevant to the type of system, facility, organization or activity being considered and also to the operational standards of the organization involved. If historically there is a very low frequency of occurrence, then any estimate of probability will be very uncertain. This applies especially for zero occurrences, when one cannot assume the event, situation or circumstance will not occur in the future.

b) Probability forecasts using predictive techniques such as fault tree analysis and event tree analysis. When historical data are unavailable or inadequate, it is necessary to derive probability by analysis of the system, activity, equipment or organization and its associated failure or success states. Numerical data for equipment, humans, organizations and systems from operational experience, or published data sources are then combined to produce an estimate of the probability of the top event.

When using predictive techniques, it is important to ensure that due allowance has been made in the analysis for the possibility of common mode failures involving the coincidental failure of a number of different parts or components within the system arising from the same cause. Simulation techniques may be required to generate probability of equipment and structural failures due to ageing and other degradation processes, by calculating the effects of uncertainties.

c) Expert opinion can be used in a systematic and structured process to estimate probability. Expert judgements should draw upon all relevant available information including historical, system-specific, organizational-specific, experimental, design, etc. There are a number of formal methods for eliciting expert judgement which provide an aid to the formulation of appropriate questions. The methods available include the Delphi approach, paired comparisons, category rating and absolute probability judgements.

Preliminary analysis

Risks may be screened in order to identify the most significant risks, or to exclude less significant or minor risks from further analysis. The purpose is to ensure that resources will be focused on the most important risks. Care should be taken not to screen out low risks which occur frequently and have a significant cumulative effect

Screening should be based on criteria defined in the context. The preliminary analysis determines one or more of the following courses of action:

- ✓ decide to treat risks without further assessment;
- ✓ set aside insignificant risks which would not justify treatment;
- ✓ proceed with more detailed risk assessment.

The initial assumptions and results should be documented.

Uncertainties and sensitivities

There are often considerable uncertainties associated with the analysis of risk. An understanding of uncertainties is necessary to interpret and communicate risk analysis results effectively. The analysis of uncertainties associated with data, methods and models used to identify and analyze risk plays an important part in their application. Uncertainty analysis involves the determination of the variation or imprecision in the results, resulting from the collective variation in the parameters and assumptions used to define the results. An area closely related to uncertainty analysis is sensitivity analysis.

Sensitivity analysis involves the determination of the size and significance of the magnitude of risk to changes in individual input parameters. It is used to identify those data which need to be accurate, and those which are less sensitive and hence have less effect upon overall accuracy.

The completeness and accuracy of the risk analysis should be stated as fully as possible.

Sources of uncertainty should be identified where possible and should address both data and model/method uncertainties. Parameters to which the analysis is sensitive and the degree of sensitivity should be stated.

Risk evaluation

Risk evaluation involves comparing estimated levels of risk with risk criteria defined when the context was established, in order to determine the significance of the level and type of risk.

Risk evaluation uses the understanding of risk obtained during risk analysis to make decisions about future actions. Ethical, legal, financial and other considerations, including perceptions of risk, are also inputs to the decision.

Decisions may include:

- ✓ whether a risk needs treatment;
- ✓ priorities for treatment;
- ✓ whether an activity should be undertaken;
- ✓ which of a number of paths should be followed.

The nature of the decisions that need to be made and the criteria which will be used to make those decisions were decided when establishing the context but they need to be revisited in more detail at this stage now that more is known about the particular risks identified.

The simplest framework for defining risk criteria is a single level which divides risks that need treatment from those which do not. This gives attractively simple results but does not reflect the uncertainties involved both in estimating risks and in defining the boundary between those that need treatment and those that do not.

The decision about whether and how to treat the risk may depend on the costs and benefits of taking the risk and the costs and benefits of implementing improved controls.

A common approach is to divide risks into three bands:

a) an upper band where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its cost;

b) a middle band (or 'grey' area) where costs and benefits, are taken into account and opportunities balanced against potential consequences;

c) a lower band where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed.

The 'as low as reasonably practicable' or ALARP criteria system used in safety applications follows this approach, where, in the middle band, there is a sliding scale for low risks where costs and benefits can be directly compared, whereas for high risks the potential for harm must be reduced, until the cost of further reduction is entirely disproportionate to the safety benefit gained.

Documentation

The risk assessment process should be documented together with the results of the assessment. Risks should be expressed in understandable terms, and the units in which the level of risk is expressed should be clear.

The extent of the report will depend on the objectives and scope of the assessment. Except for very simple assessments, the documentation can include:

- ✓ objectives and scope;
- ✓ description of relevant parts of the system and their functions;
- ✓ a summary of the external and internal context of the organization and how it relates to the situation, system or circumstances being assessed;
- ✓ risk criteria applied and their justification;
- ✓ limitations, assumptions and justification of hypotheses;
- ✓ assessment methodology;
- ✓ risk identification results;
- ✓ data, assumptions and their sources and validation;
- ✓ risk analysis results and their evaluation;
- ✓ sensitivity and uncertainty analysis;
- ✓ critical assumptions and other factors which need to be monitored;
- ✓ discussion of results;
- ✓ conclusions and recommendations;
- ✓ references.

If the risk assessment supports a continuing risk management process, it should be performed and documented in such a way that it can be maintained throughout the life cycle of the system, organization, equipment or activity. The assessment should be updated as significant new information becomes available and the context changes, in accordance with the needs of the management process.

Monitoring and reviewing risk assessment

The risk assessment process will highlight context and other factors that might be expected to vary over time and which could change or invalidate the risk assessment. These factors should be specifically identified for on-going monitoring and review, so that the risk assessment can be updated when necessary.

Data to be monitored in order to refine the risk assessment should also be identified and collected.

The effectiveness of controls should also be monitored and documented in order to provide data for use in risk analysis. Accountabilities for creation and reviewing the evidence and documentation should be defined.

Application of risk assessment during life cycle phases

Many activities, projects and products can be considered to have a life cycle starting from initial concept and definition through realization to a final completion which might include decommissioning and disposal of hardware.

Risk assessment can be applied at all stages of the life cycle and is usually applied many times with different levels of detail to assist in the decisions that need to be made at each phase.

Life cycles phases have different requirements and need different techniques For example, during the concept and definition phase, when an opportunity is identified, risk assessment may be used to decide whether to proceed or not.

Where several options are available risk assessment can be used to evaluate alternative concepts to help decide which provides the best balance of positive and negative risks.

During the design and development phase, risk assessment contributes to

- ✓ ensuring that system risks are tolerable,
- ✓ the design refinement process,
- ✓ cost effectiveness studies,
- ✓ identifying risks impacting upon subsequent life-cycle phases.

As the activity proceeds, risk assessment can be used to provide information to assist in developing procedures for normal and emergency conditions.