MS IEC/ISO 31010 – Risk Management - Risk Assessment Techniques

Mohamad Bin Mohamad Zain
Vice Chairman TC Risk Management
Chief Procurement Officer
Telekom Malaysia Bhd

Establish Context

Risk Assessment

Risk Treatment

Implement & Review
• Overview of Risk Management Standards

• Setting the Scene – Risk Management Framework (MS ISO/IEC 31000)
  • Framework for managing risk
  • Risk Management Process

• MS IEC/ISO 31010 – Risk Management – Risk Assessment Techniques
  • Risk Assessment Process
  • Support Decision Making Process
  • Risk Assessment Techniques
  • Benefit of Risk Assessment

• Conclusion
Risk Management Standard

  - MS ISO/IEC 31000:2010 Risk Management – Principles and Guidelines
- ISO/IEC 31000:2009
- IEC/ISO 31000:2009
  - ISO/IEC 31000:2009
MS ISO/IEC 31000:2010
Risk Management – Principles & Guidelines
MS ISO/IEC 31000:2010
Risk Management – Principles & Guidelines

Process For Risk Management

6.3 Establishing the context

6.4 Risk assessment
   6.4.2 Risk identification
   6.4.3 Risk analysis
   6.4.4 Risk evaluation

6.5 Risk treatment

6.6 Monitoring and review

6.2 Communication and consultation
Risk Identification

- The organization should identify sources of risk, areas of impacts, events and their causes and their potential consequences.

- Generate a comprehensive list of risks based on those events that might enhance, prevent, degrade or delay the achievement of the objectives.

- Identify the risks associated with not pursuing an opportunity.

- Identification should include risks whether or not their source is under control of the organization.

- The organization should apply risk identification tools and techniques which are suited to its objectives and capabilities, and to the risks faced.

- Relevant and up-to-date information is important in identifying risks.

- People with appropriate knowledge should be involved in identifying risks.

- After identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes should be considered.
Risk analysis is about developing an understanding of the risk.

Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated and on the most appropriate risk treatment strategies and methods.

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. It is important to consider the interdependence of different risks and their sources.

An event can have multiple consequences and can affect multiple objectives. Existing risk controls and their effectiveness should be taken into account.

Analysis of risk can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances. In practice, qualitative analysis is often used first to obtain a general indication of the level of risk and to reveal the major risks.

Consequences can be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data. Consequences can be expressed in terms of tangible and intangible impacts.
The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment to prioritize treatment implementation.

Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. If the level of risk does not meet risk criteria, the risk should be treated.

Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefit from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing risk controls. This decision will be influenced by the organization’s risk appetite or risk attitude and the risk criteria that have been established.
Risk assessment involve process of risk identification, risk analysis and risk evaluation.
What can happen and Why?
What are the consequences?
What is the probability of future occurrence?
Factors that mitigate consequence or reduce probability of risk

Four KEY Questions

• Is the level of risk tolerable/acceptable?
• Does it require further treatment?

Risk Assessment

Understand the Risks

Understand the Root Cause

Understand the Consequence

Understand the Risk Probabilities

Do I take the activity?

Which treatment will bring risk level to my tolerance limit

I need to prioritize the risk treatments

Do I need to treat the risk?

How to maximize opportunities?

Six Broad Cluster of Techniques

- Look-Up Methods (2)
- Supporting Methods (4)
- Scenario Analysis (8)
- Functional Analysis (5)
- Statistical Methods (3)
- Controls Assessment (2)

Type of Risk Assessment Techniques (24)

Six Broad Cluster of Techniques

- Check-Lists
- Preliminary Hazard Analysis

Six Broad Cluster of Techniques

- Structured Interview & Brainstorming
- Delphi Technique
- SWIFT Structured (What If)
- Human Reliability Analysis

Six Broad Cluster of Techniques

- Scenario Analysis
- Root Cause Analysis
- Toxicological Risk Assessment
- Business Impact Analysis
- Fault Tree Analysis
- Event Tree Analysis
- Cause/Consequence Analysis
- Cause and Effect Analysis

Six Broad Cluster of Techniques

Six Broad Cluster of Techniques

LOPA
Layers of Protection Analysis

Control Assessments

Bow Tie Analysis

Six Broad Cluster of Techniques

- Monte Carlo Analysis
- Bayesian Analysis
- Statistical Analysis
- Markov Analysis

MS IEC/ISO 31010:2011
Risk Management – Risk Assessment Techniques

**Benefit**

- Provide evidence-based information and analysis to make decision
- Understand the risk & its potential impact to objectives
- Assist in the selection of appropriate risk treatment options
- Assist in prioritizing the risk treatment execution
- Provide information for decision making based on risk tolerance
- Meeting Regulatory requirement where appropriate
• MS IEC/ISO 31010 complement the MS ISO/IEC 31000 – focusing on risk assessment techniques

• The standard provide general guidance on selection and application of systematic techniques for risk assessment

• Risk Assessment provides structured process to understand how the risk will impact the objectives in term of consequence and probability before we review the treatment options

• This standard is not intended for certification, regulatory or contractual use.
The END