

Session: Thursday 8 October 10:40 am TapRoot® Summit Nashville 2009

What is new in

ISO 31000 :2009

Risk Management - Principles and Guidelines on Implementation

and companion Standard

IEC 31010:2009

Risk Management – Risk Assessment Guidelines

By

Jim Whiting

risk@workplaces.com.au



DRAFT INTERNATIONAL STANDARD ISO/DIS 31000

ISO/PC 992

Secretariat: TMB

Voting begins on:
2008-04-01

Voting terminates on:
2008-09-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Risk management — Principles and guidelines on implementation

Management du risque — Principes et lignes directrices de mise en application

ICS 03.100.01



DRAFT INTERNATIONAL STANDARD IEC/DIS 31010

Secretariat: TMB

Voting begins on
2008-05-23

Voting terminates on
2008-10-24

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОММИСИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Risk management — Risk assessment guidelines

Management du risque — Lignes directrices pour l'évaluation du risque

ICS 03.100.01

WHY implement ISO 31000 in your organization ?

- Increased consistency / reliability in decision-making
- Consistency in terminology and processes
- Confidence in dealing with threats, opportunities
- Integrated enterprise wide risk management
- Improved safety, financial, corporate governance
- Demonstration of due diligence in managing risk
- Reduced legal / regulatory vulnerabilities

- **ISO 31000** is NOT **intended** to be :-
a Certification Instrument or “Standard”
- **ISO 31000** provides principles and guidelines for implementation but not for certification
- How each organization does risk management is up to them

A rose by any other buzz word

- ▶ **TRM** Total Risk Management,
 - ▶ **IRM** Integrated Risk Management,
 - ▶ **HRM** Holistic Risk Management,
 - ▶ **ERM** Enterprise Risk Management
 - ▶ **EWR** Enterprise Wide Risk
-
- ▶ Whatever the buzz word, RM is all about – in the face of **uncertainty** how well can an organization successfully **understand and manage** the **opportunities** to exploit and the associated **threats** that can confront it in **meeting OR not meeting its objectives**
 - ▶ **Corporate Governance & Compliance & Due Diligence** depend on **demonstrating** a strong understanding of risks and appropriate means of successfully managing them.
 - ▶ **Audits** are needed to **provide the assurance** that measures are in place and effectively providing the risk control required.

Integration

- ❑ All **decisions** = risk management
 - ❑ All **planning** = risk management
 - ❑ All **change management** = risk management

 - ❑ Risk management must be **embedded** into every aspect of management of the organization
 - ❑ RM is core to ALL “modern” management
 - when **decisions** are being made
 - when **options** are being devised, framed, evaluated, selected
 - not after the decision is made.
- Application of risk management CAN NEVER be simply :-
- an after-thought
 - a nuisance add-on
 - after a decision, buy some insurance

- **All** aspects of management involve **uncertainty** in achieving objectives such as :-
 - *financial performance targets*
 - *customer satisfaction*
 - *market share*
 - *product life*
 - *reputation*
 - **health & safety**
 - **environment**
 - *quality*
- Important Concept of risk “**domains**” not “**silos**”
- Can **ALL types / domains** of risk be managed in similar ? same ? ways. HSE ? Q ?

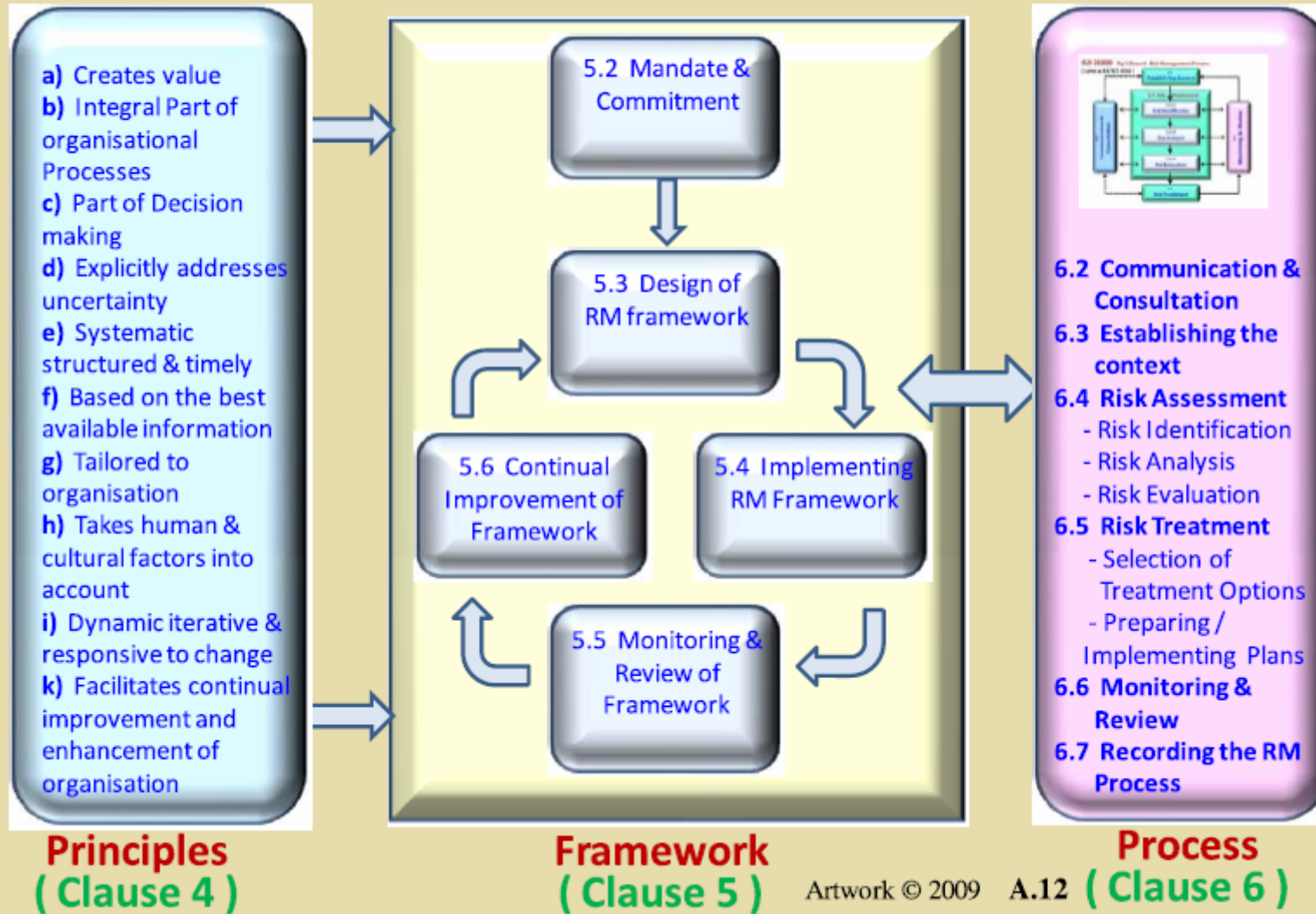
Sample Consequence Scales (different risk domains)

(Arbitrary – to be decided by the top policy-making body - Be cautious in comparing across domains)

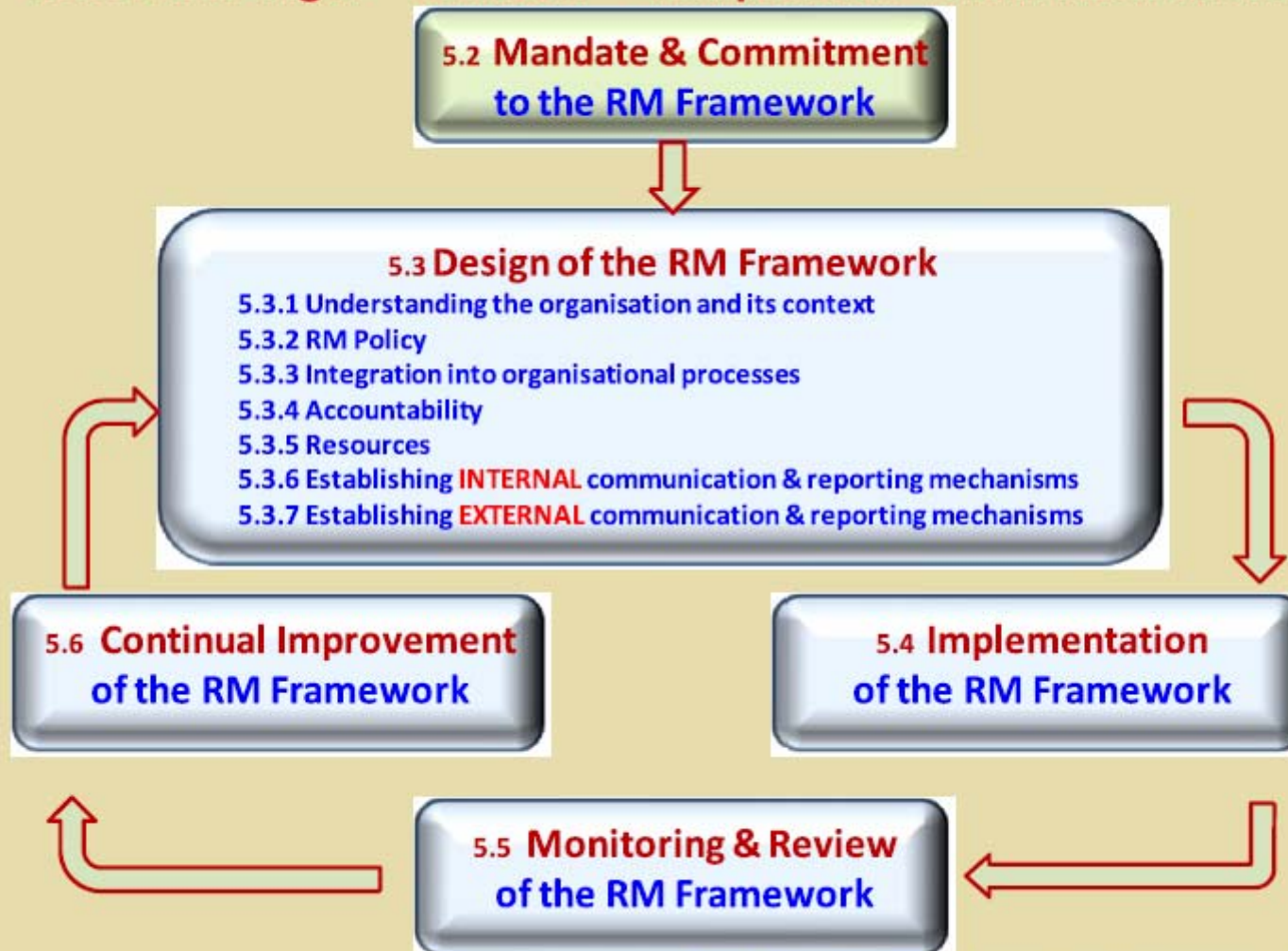
Score	Category Rating	Cost (\$) Property Damage/ Financial Loss	Personal Injury / illness	Environment	Legal Liability	Public Perception
	Verbal					
6	Catastrophic	>\$100 Million	Multiple fatalities / fatal illnesses	Large scale irreversible environmental harm.	Officer jailed. Corporate fine >\$10M. Multiple third party claims totaling >\$50M.	Forced shut down of major installation or curtailment of operations.
5	Disaster	\$10 to 100 Million	Single fatality / fatal illness	Major release of pollutants. Significant, long term environmental harm. Release of pollutants to an extremely sensitive area.	Corporate fine \$1-10M. Personnel fine. Multiple third party claims totaling \$5M-50M.	Extended national/ international adverse media campaign. Parliamentary inquiry.
4	Major	\$1 - 10 Million	Multiple serious injuries illnesses	Release of pollutants to sensitive areas. Immediate offsite contamination which is beyond the normal combatant resources available at site.	Corporate fine \$100K-1M. Third party claim(s) \$500K-5M.	Adverse national media coverage.
3	Serious	\$100K to 1 Million	Serious injury / illness (hospitalisation)	Contamination of property that may cause environmental harm minor off site contamination.	Corporate fine <\$100K. Third party claim (s) \$100K-500K.	Adverse capital city media coverage.
2	Minor	\$10,000 to \$100K	Medical (doctor Treatment)	Contamination of property that does not constitute a threat to the environment.	Third party claim <\$100K.	Local media coverage. Public (telephone) complaints.
1	Low	<\$10,000	First Aid treatment Only or even no treatment	Contamination occurs within the confines of protected areas and can be managed through normal operations.	Third party claim <\$10,000.	Public normally unaware.

Avoid verbal descriptors

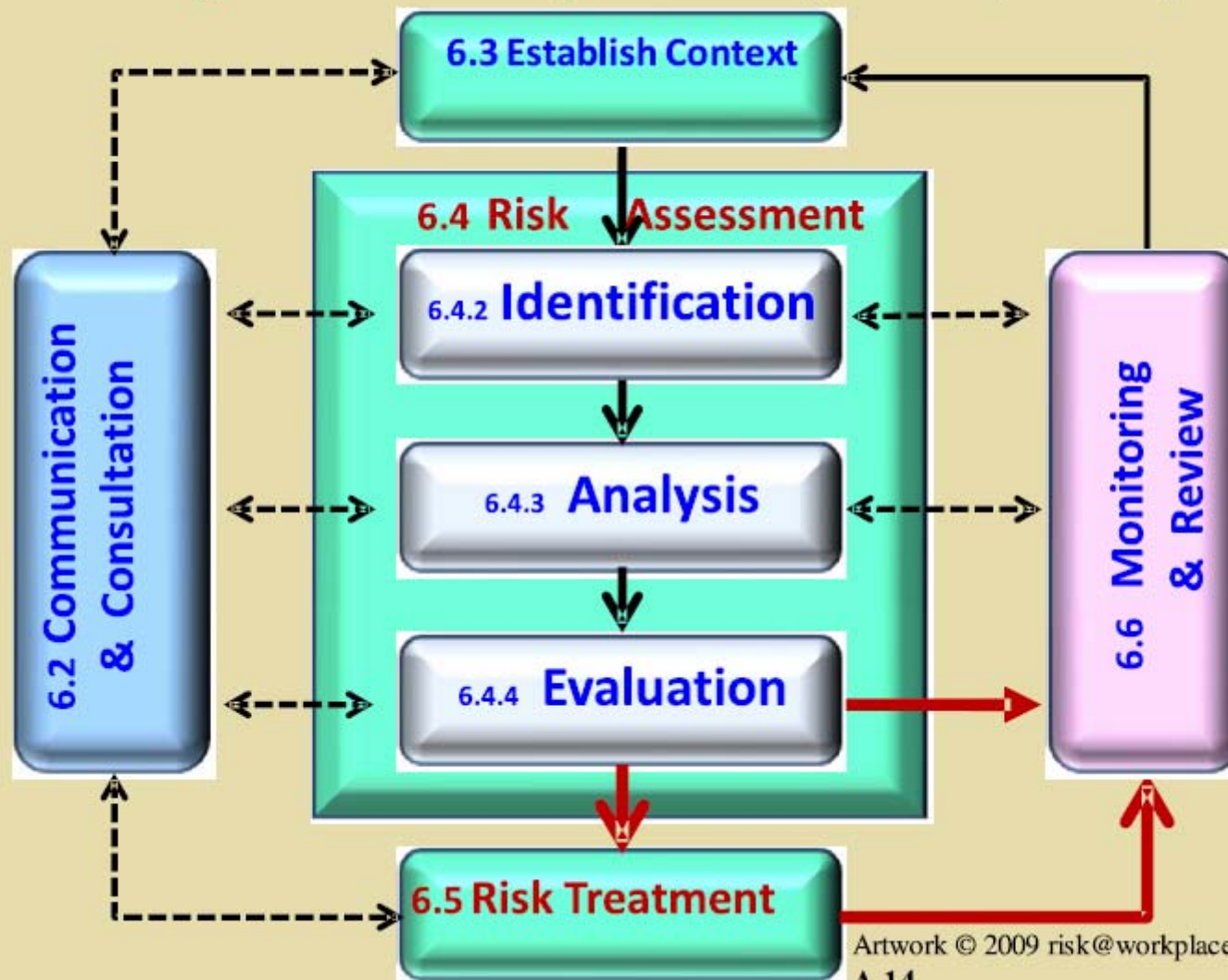
ISO 31000 Fig 1 Relationship between RM Principles / Framework / Process



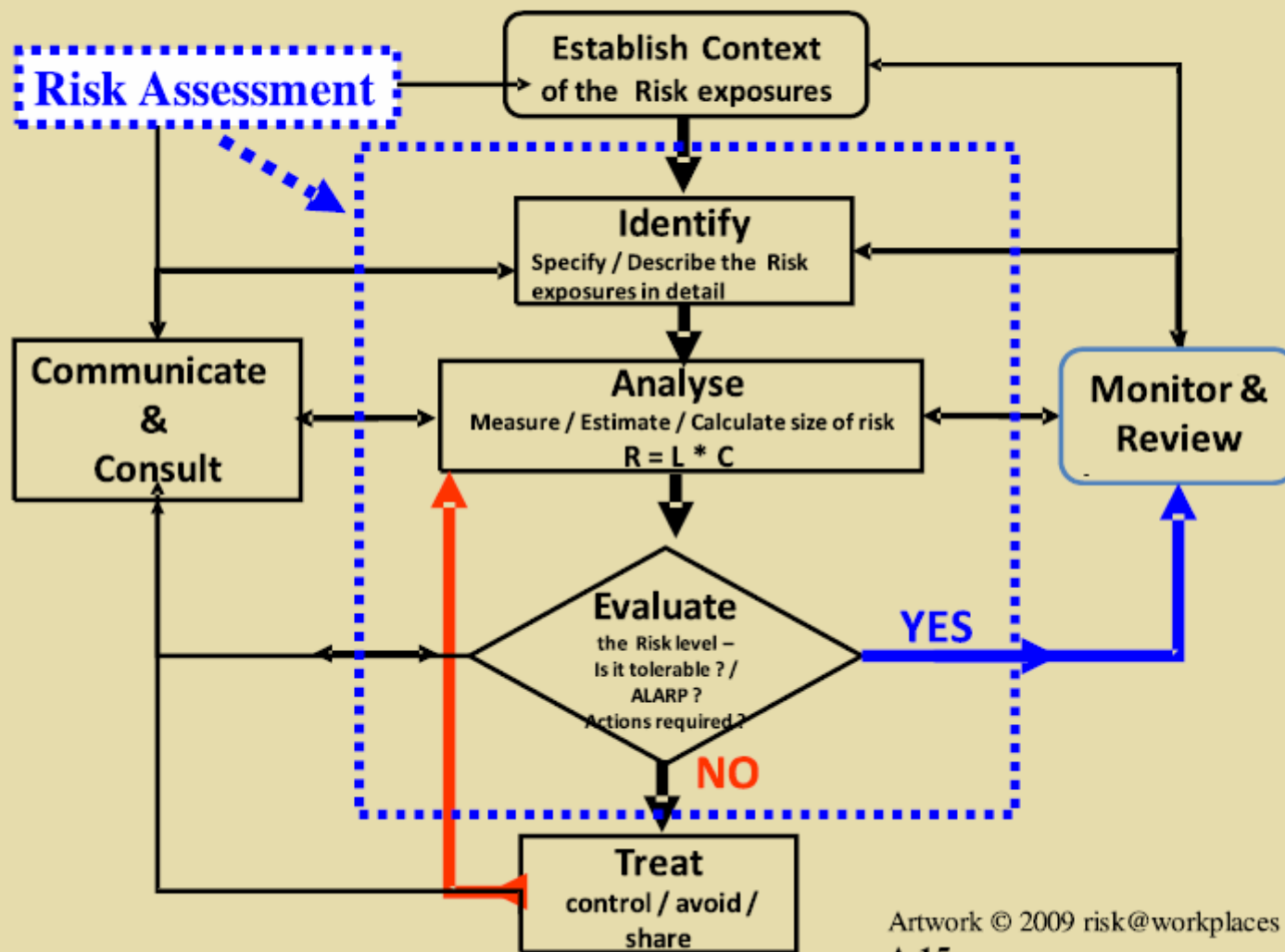
ISO 31000 Fig 2 Clause 5 Components of RM Framework



ISO 31000 Fig 3 Clause 6 Risk Management Process [same as AS/NZS 4360]



ISO 31000: 2009 and AS/NZS 4360: 2004 - Risk Management



Overview of Risk Management Process – ISO 31000 and AS 4360

Concurrent with each Phase in Column 2	Phases / Stages in RM Process	Explanatory Notes for each Phase	Concurrent with each Phase in Column 2
	Establish the Context of the Risk exposures	Ask the appropriate RISK QUESTION in detail, then Why do we want to be exposed to this hazard / opportunity ? Specify the Costs / benefits of exposure to this Risk	
Risk Assessment			
Communicate & Consult	Identify Specify / Describe the Risk exposures In detail	Describe the chosen risk fully in words and/or scenario map. Include the chosen C = Consequence of Most Interest or Most Concern and all details of all credible risk exposures and existing control factors needed to lead to or produce the chosen Consequence	Monitor & Review
Detailed documented processes during each phase	Analyse Measure / Estimate / Calculate size / level of Risk	Estimate the size / level of the risk by estimating the likelihood of all the credible risk exposures and existing control factors being unsuccessful and hence leading to the chosen C	audits / reviews evaluations at each phase
	Evaluate the Risk level	Estimate if risk level is tolerable / intolerable / ALARP and decide priorities for actions against corporate tolerability criteria and action plans	
	Treat the Risk	Decide and implement actions for Avoidance / Sharing / Controlling the risk according to agreed Cost / Benefit criteria	A.16



© copyright 2009

IEC DIS 31010 Table A1- Selection of tools for Risk Assessment					
Tools & Techniques	RISK ASSESSMENT PROCESS				
	SA = strongly applicable A = applicable NA = Not Applicable				
	RISK IDENTIFICATION	RISK ANALYSIS			RISK EVALUATION
CONSEQUENCE		LIKELIHOOD	LEVEL OF RISK		
Failure mode and effect analysis (IEC 60812)	SA	NA	NA	NA	NA
Failure mode, effect and criticality analysis (IEC 60812)	SA	SA	SA	SA	SA
Fault tree analysis (IEC 61025)	NA	A	A	A	A
Hazard and operability studies (HAZOP) (IEC 61882)	SA	SA	NA	NA	SA
Reliability centred maintenance (IEC 60300-3-11)	SA	SA	SA	SA	SA
Markov analysis (IEC 61665)	A	NA	SA	NA	NA
Human reliability analysis	SA	SA	SA	SA	A
Preliminary hazard analysis	SA	NA	NA	NA	NA
Event tree analysis	NA	SA	SA	A	NA
Brainstorming	SA	NA	NA	NA	NA
Structured or Semi-Structured Interviews	SA	NA	NA	NA	NA
Delphi Techniques	SA	NA	NA	NA	NA
Checklists	SA	NA	NA	NA	NA
Consequence/Likelihood Matrix	SA	SA	SA	SA	A
LOPA	SA	NA	NA	NA	NA
SWIFT	SA	SA	SA	SA	SA
Decision Tree	NA	SA	SA	A	A
Bow Tie Analysis	NA	A	SA	SA	A
Monte Carlo	NA	SA	SA	SA	SA
Root Cause Analysis	A	NA	SA	SA	NA
HACCP	SA	SA	NA	NA	SA
Environmental Risk Assessment	SA	SA	SA	SA	SA
Scenario Analysis	SA	SA	A	A	A
Business Impact Analysis	A	SA	A	A	A
Cause & Consequence Analysis	A	SA	NA	A	A
Cause and effect analysis	SA	SA	NA	NA	NA
Sneak Circuit Analysis	A	NA	NA	NA	NA
Bayesian Analysis	NA	NA	SA	NA	SA

See IEC 31010 – Tools & Techniques

IEC 31010 Table A2 – Attributes of a Selection of Risk Assessment tool

Example type of risk assessment method and technique	Description	Relevance of influencing factors		
		Resources & capability	Nature & Degree of uncertainty	Complexity
Fault Tree Analysis	A technique which starts with the undesired event (Top Event) and determines all the ways in which it could occur. These are displayed graphically in a logical tree diagram. Once the fault tree has been developed, consideration should be given to ways of reducing or eliminating potential causes / sources	high	high	high
Event Tree Analysis	Using inductive reasoning to translate likelihood of different initiating events into possible outcomes	med	med	med
Cause consequence Analysis	A combination of fault and event tree analysis that allows inclusion of time delays. Both causes and consequences of an initiating event are considered	high	med	high

Part B Extracts IEC/DIS 31010 - *Risk assessment guidelines*

B.14 Fault Tree Analysis (FTA)

B.14.1 Overview

B.14.2 Use

B.14.3 Inputs

B.14.4 Process

B.14.5 Outputs

B.14.6 Strengths and Limitations

B.14.7 Comparisons and Links

B.14.8 References

ISO DIS 31000

Clause 4 - Principles for managing risk

Risk management

- a) creates value.
- b) is an integral part of organizational processes.
- c) is part of decision making.
- d) explicitly addresses uncertainty.
- e) is systematic, structured and timely.
- f) is based on the best available information.
- g) is tailored / aligned with the organization's external and internal context and risk profile.
- h) takes human and cultural factors into account.
- i) is transparent and inclusive.
- j) is dynamic, iterative and responsive to change.
- k) facilitates continual improvement and enhancement of the organization

ISO DIS 31000

Clause 5.2 Mandate and commitment

Management should:

- articulate and endorse the risk management policy;
- determine risk management performance indicators that align with organizational performance indicators;
- ensure alignment of risk management objectives with the objectives and strategies of the organization;
- ensure legal and regulatory compliance;
- assign management accountabilities and responsibilities at appropriate levels within the organization;
- ensure that the necessary resources are allocated to risk management;
- communicate the benefits of risk management to all stakeholders; and
- ensure that the framework for managing risk continues to remain appropriate

ISO DIS 31000

Clause 5.3 Design of framework

- 5.3.1 Understanding the organization and its context
- 5.3.2 Risk management policy
- 5.3.3 Integration into organizational processes
- 5.3.4 Accountability
- 5.3.5 Resources
- 5.3.6 Establishing **internal** communication and reporting mechanisms
- 5.3.7 Establishing **external** communication and reporting mechanisms

ISO DIS 31000

Clause 5.4 Implementing risk management

5.4.1 Implementing the framework - the organization should:

- define an appropriate **timing and strategy** for implementing the framework;
- apply the risk management **policy and process** to the organizational processes;
- comply with **legal and regulatory requirements**;
- document justified decision making, including the development and setting of objectives which are **aligned with the outcomes** of the risk management process;
- hold **information** and **training** sessions; and
- **communicate** and **consult** with stakeholders to ensure that its risk management framework remains appropriate

ISO DIS 31000

Clause 5.5 Monitoring and review of the framework

The organization should:

- establish performance measures;
- periodically measure progress against, and deviation from the risk management plan;
- periodically review whether the risk management framework, policy, and plan are still appropriate given
- the organizations' internal and external context;
- report on risks, progress with the risk management plan and ensure how well the risk management policy
- is being followed; and
- review the effectiveness of the risk management framework.

ISO DIS 31000

Clause 6 Process for managing risk

6.1 General

Figure 3 — RM process

6.2 Communication and Consultation

6.3 Establishing context - External & Internal Context

- Of the risk management process itself
- Developing risk criteria

6.4 Risk assessment

- Risk Identification
- Risk Analysis
- Risk Evaluation

6.5 Risk Treatment

- Selection of Treatment Options
- Preparing / Implementing Treatment Plans

6.6 Monitoring and Review

6.7 Recording the RM Process

ISO DIS 31000

Informative Annex A.2 Attributes

- A.2.1 An emphasis on **continual improvement** in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.
- A.2.2 Comprehensive, fully defined and **fully accepted accountability** for risks, risk controls and risk treatment tasks. Designated individuals fully accept, are appropriately skilled and have adequate resources to check risk controls, monitor risks, improve risk controls and communicate effectively about risks and their management to internal and external stakeholders.
- A.2.3 All **decision making** within the organization, whatever the level of importance and significance, involves the **explicit consideration of risks** and the application of risk management to some appropriate degree.
- A.2.4 **Continual communications** with internal and external stakeholders including comprehensive and frequent reporting of risk management performance is part of good **governance**.
- A.2.5 Risk management is viewed as central to the organization's management processes so that risks are considered in terms of effect of **uncertainty on objectives**. The organization's governance structure and process are based on the management of risk. Effective risk management is regarded by managers as essential for the achievement of the organization's objectives.