

# A Risk Management Standard

Maria Passa

29<sup>th</sup> October, 2007



## Introduction

### Issued in 2002 by:

- The Institute of Risk Management (**IRM**)
- The Association of Insurance and Risk Managers (**AIRMIC**)
- and **ALARM** The National Forum for Risk Management in the Public Sector



## Introduction

**Standard aims to ensure that there is an agreed:**

- terminology related to the words used (ISO/IEC Guide 73)
- process by which risk management can be carried out
- organisation structure for risk management
- objective for risk management

## Introduction

### Purpose:

- To represent best practice against which organisations can benchmark
- To enable organisations to report compliance to the standard
- Not to provide a prescriptive, box ticking approach nor to establish a certifiable process
- Feedback from organisations is appreciated

# 1. Risk

## Definition:

- Risk is the combination of the probability of an event and its consequences (ISO/IEC Guide 73)
- Both opportunities for benefit (upside risk) and threats to success (downside risk) are considered
- Safety risk (only downstream) is focused on prevention and mitigation of harm

## 2. Risk Management

Objective => to add maximum sustainable value to all the activities of the organisation

Principles:

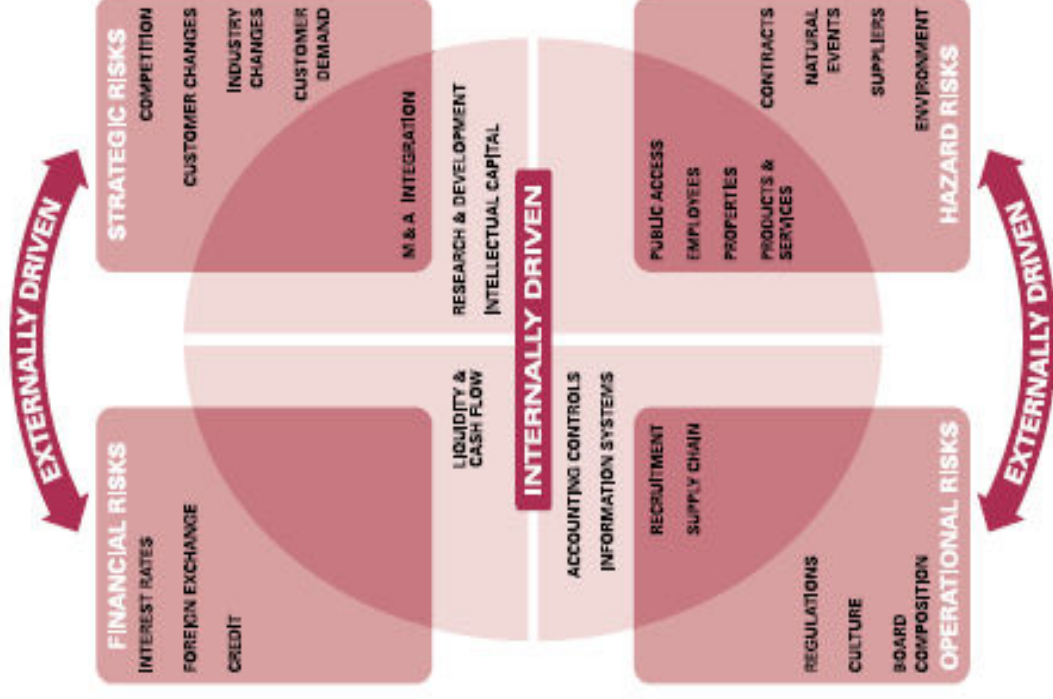
- continuous & developing process throughout organisation's strategy
- implementation of that strategy
- methodical address all risks surrounding organisation's activities

## 2. Risk Management

### Principal means:

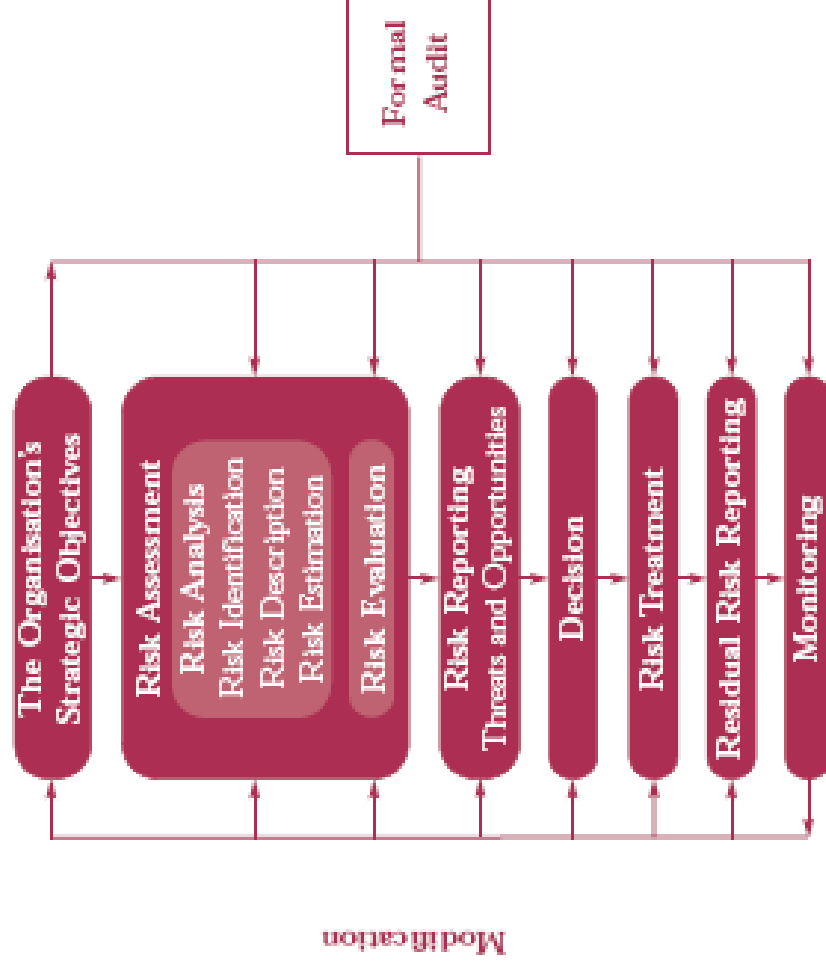
- Policy
- Risk management Programme
- Tactical & Operational Objectives
- Assigned Responsibilities

## 2. Risk Management External & Internal Drivers of Key Risks



## 2. Risk Management

- Provides a framework enabling consistent & controlled implementation of activities
- Improves decision making, planning and prioritisation
- Contributes to more efficient use/allocation of capital and resources
- Reduces volatility in the non essential areas of the business
- Protects and enhances assets & company image
- Develops and supports people & the organisation's knowledge base
- Optimises operational efficiency



### 3. Risk Assessment

Risk Assessment is defined by ISO/ IEC Guide 73 as  
the overall process of **risk analysis & risk evaluation**.

## 4. Risk Analysis

### 4.1 Risk Identification

- **Methodical** approach to ensure identification of all significant activities and their risks

Business activities include:

- Strategic
- Operational
- Financial
- Knowledge management
- Compliance

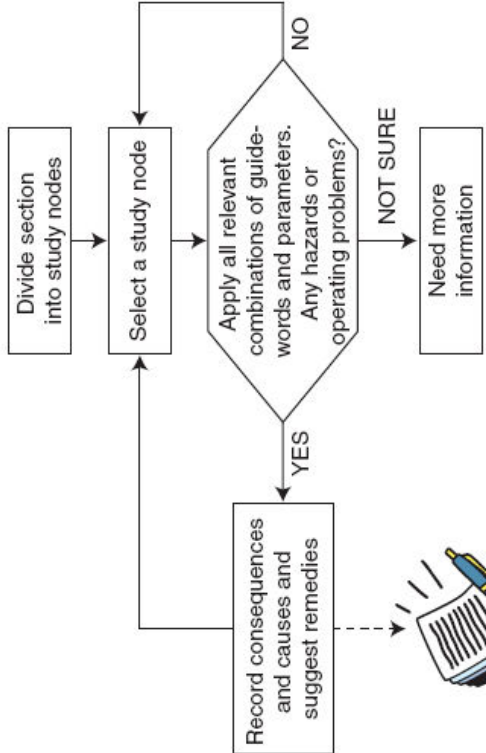
## 4. Risk Analysis

### Examples of Risk Identification Techniques:

- Brainstorming
- Questionnaires
- Business process studies
- Industry benchmarking
- Scenario analysis
- Risk assessment workshops
- Incident investigation
- Auditing and inspection
- HAZOP (Hazard & Operability Studies)

# 4. Risk Analysis

## HAZOP Method



### Examples of Process Parameters

Flow	Composition	pH
Pressure	Addition	Sequence
Temperature	Separation	Signal
Mixing	Time	Start/stop
Stirring	Phase	Operate
Transfer	Speed	Maintain
Level	Particle size	Services
Viscosity	Measure	Communication
Reaction	Control	

### Basic Guide-words

Guide-word	Meaning	Example
No (not, none)	None of the design intent is achieved	No flow when production is expected
More (more of, higher)	Quantitative increase in a parameter	Higher temperature than designed
Less (less of, lower)	Quantitative decrease in a parameter	Lower pressure than normal
As well as (more than)	An additional activity occurs	Other valves closed at the same time (logic fault or human error)
Part of	Only some of the design intention is achieved	Only part of the system is shut down
Reverse	Logical opposite of the design intention occurs	Back-flow when the system shuts down
Other than (other)	Complete substitution - another activity takes place	Liquids in the gas piping

### Example

Attribute	Guide word	Cause	Consequence	Recommendation
Supply voltage	No	Cable fault	Lack of sensor signal, system shuts down	Consider overvoltage protection
Sensor current	More	Regulator fault	Possible damage to sensor	Monitor supply current
	More	Sensor fault	Incorrect temperature reading	
	Less	Sensor fault		

## 4. Risk Analysis

### 4.2 Risk Description

1. Name of Risk	Qualitative description of the events, their size, type, number and dependencies
2. Scope of Risk	
3. Nature of Risk	Eg. strategic, operational, financial, knowledge or compliance
4. Stakeholders	Stakeholders and their expectations
5. Quantification of Risk	Significance and Probability
6. Risk Tolerance/ Appetite	Loss potential and financial impact of risk Value at risk Probability and size of potential losses/gains Objective(s) for control of the risk and desired level of performance
7. Risk Treatment & Control Mechanisms	Primary means by which the risk is currently managed Levels of confidence in existing control Identification of protocols for monitoring and review Recommendations to reduce risk
8. Potential Action for Improvement	
9. Strategy and Policy Developments	Identification of function responsible for developing strategy and policy

## 4. Risk Analysis

### 4.3 Risk Estimation

- Quantitative
  - Semi-quantitative or
  - Qualitative
- in terms of the probability of occurrence and the possible consequence

**Table 4.3.1 Consequences - Both Threats and Opportunities**

High	Financial impact on the organisation is likely to exceed £x Significant impact on the organisation's strategy or operational activities Significant stakeholder concern
Medium	Financial impact on the organisation likely to be between £x and £y Moderate impact on the organisation's strategy or operational activities Moderate stakeholder concern
Low	Financial impact on the organisation likely to be less than £y Low impact on the organisation's strategy or operational activities Low stakeholder concern

## 4. Risk Analysis

### 4.3 Risk Estimation

**Table 4.3.2 Probability of Occurrence - Threats**

Estimation	Description	Indicators
High (Probable)	Likely to occur each year or more than 25% chance of occurrence.	Potential of it occurring several times within the time period (for example - ten years). Has occurred recently.
Medium (Possible)	Likely to occur in a ten year time period or less than 25% chance of occurrence.	Could occur more than once within the time period (for example - ten years). Could be difficult to control due to some external influences. Is there a history of occurrence?
Low (Remote)	Not likely to occur in a ten year period or less than 2% chance of occurrence.	Has not occurred. Unlikely to occur.

## 4. Risk Analysis

### 4.3 Risk Estimation

**Table 4.3.3 Probability of Occurrence - Opportunities**

Estimation	Description	Indicators
High (Probable)	Favourable outcome is likely to be achieved in one year or better than 75% chance of occurrence.	Clear opportunity which can be relied on with reasonable certainty to be achieved in the short term based on current management processes.
Medium (Possible)	Reasonable prospects of favourable results in one year of 25% to 75% chance of occurrence.	Opportunities which may be achievable but which require careful management. Opportunities which may arise over and above the plan.
Low (Remote)	Some chance of favourable outcome in the medium term or less than 25% chance of occurrence.	Possible opportunity which has yet to be fully investigated by management. Opportunity for which the likelihood of success is low on the basis of management resources currently being applied.

## 4. Risk Analysis

### 4.4 Risk Analysis Methods & Techniques – examples:

#### **Upside risk**

- Market survey
- Research and Development
- Business impact analysis

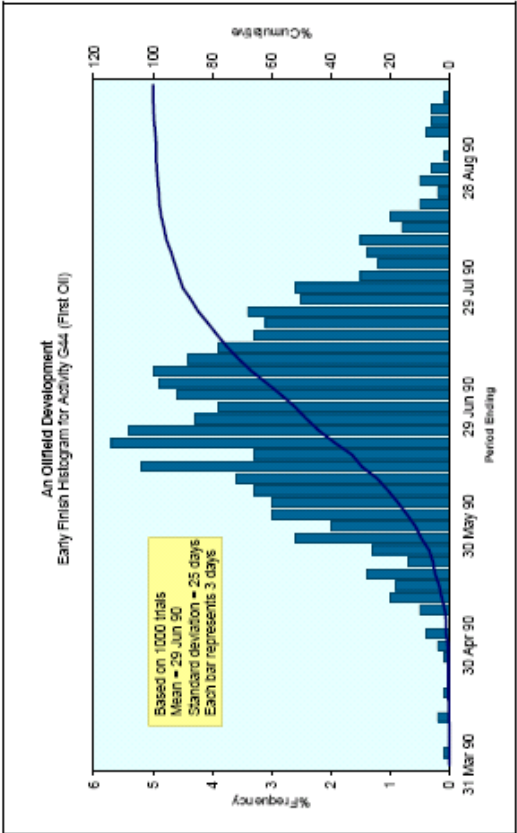
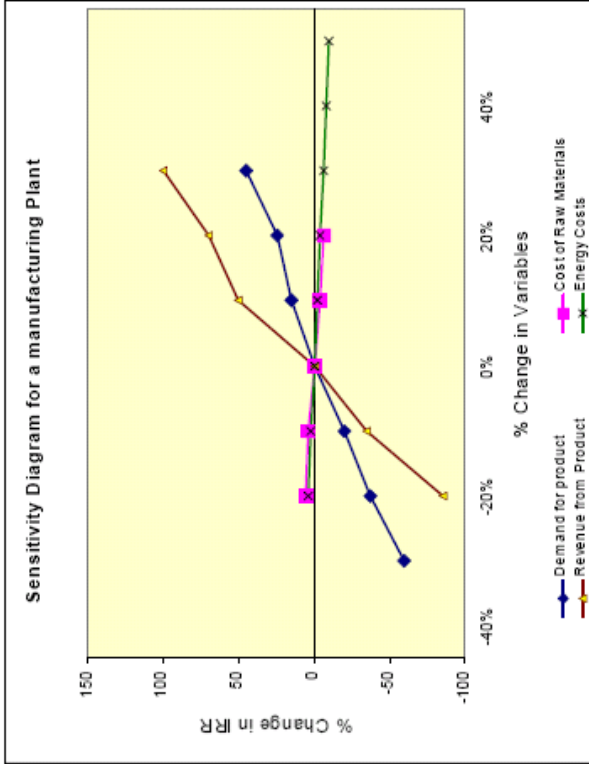
#### **Both**

- SWOT / BPEST / PESTLE analysis
- Statistical inference
- Measures of central tendency and dispersion

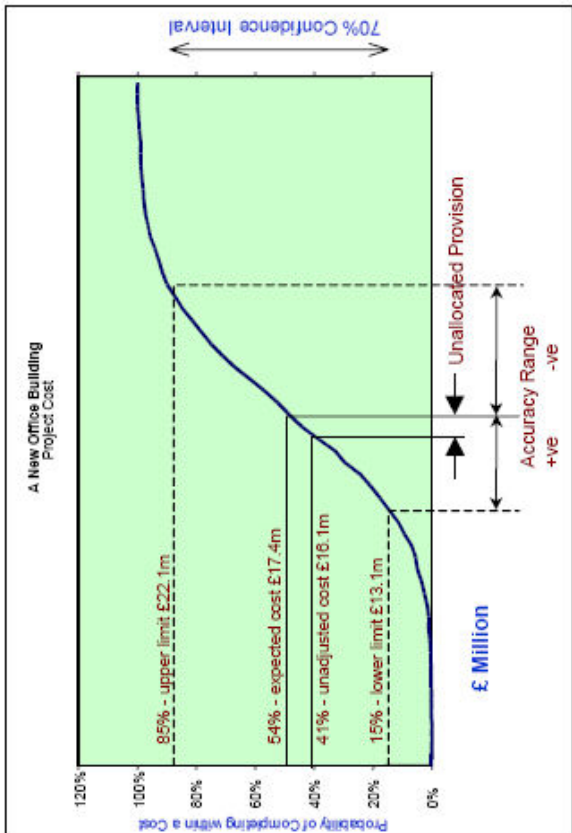
#### **Downside risk**

- Threat analysis
- Fault tree analysis
- FMEA (Failure Mode & Effect Analysis)

# 4. Risk Analysis



## Probabilistic Monte Carlo analysis



## 4. Risk Analysis

### 4.5 Risk Profile

- Gives a significance rating to each risk and provides a tool for prioritising risk
- Describes the primary control procedures in place & indicates areas where the level of risk control investment might be increased, decreased or reapportioned.

## 5. Risk Evaluation

- compare the estimated risks against established risk criteria
- Decision making tool for the significance of risks and their acceptance or treatment

## 6. Risk Reporting & Communication

### **Internal Reporting** for:

- Board of Directors
- Business Unit Managers
- Individuals

### **External Reporting** for:

- Stakeholders

### **Formal Reporting** should address:

- the control methods
- the risk identification processes
- the primary risk control systems
- the monitoring & review system in place

## 7. Risk Treatment

- Risk treatment is the process of selecting and implementing measures to modify the risk, providing as minimum:
- effective and efficient operation of the organisation
  - effective internal controls
  - compliance with laws and regulations

## 8. Monitoring & Review of the Risk Management Process

### Requirements:

- a reporting & review structure
- regular audits of policy and standards compliance

### Process should determine whether:

- measures adopted resulted what was intended
- procedures adopted & information gathered for undertaking the assessment were appropriate

## 9. The Structure & Administration of Risk Management

### 9.1 Risk Management Policy:

- sets out the approach to and appetite for risk and risk management
- sets out responsibilities for risk management
- refers to any legal requirements for policy statements

## 9. The Structure & Administration of Risk Management

- 9.2 Role of the Board is to consider as minimum:
- the nature and extent of downside acceptable risks
  - the likelihood of such risks becoming a reality
  - how unacceptable risks should be managed
  - the company's ability to minimise the probability and impact of risks
  - the costs and benefits of the risk control activity
  - the effectiveness of the risk management process
  - the risk implications of board decisions

## 9. The Structure & Administration of Risk Management

- 9.3 Role of the Business Units includes:
- responsibility for managing risk on a day to-day basis
  - responsibility for promoting risk awareness and introduction of risk management objectives into their business
  - regular risk management reviews to allow consideration of exposures and to reprioritise work in the light of effective risk analysis
  - Incorporation of risk management at the conceptual stage of projects as well as throughout a project

## 9. The Structure & Administration of Risk Management

- 9.4 Role of the Risk Management function should include:
- setting policy & strategy for risk management
  - leading risk management at strategic and operational level
  - building a risk aware culture within the organisation
  - establishing internal risk policy & structures for business units
  - designing & reviewing processes for risk management
  - developing risk response processes, including contingency and business continuity programmes
  - preparing reports on risk for the board and the stakeholders

## 9. The Structure & Administration of Risk Management

- ### 9.5 Role of the Internal Audit may include:
- focusing the internal audit work on the significant risks
  - providing assurance on the management of risk
  - providing active support and involvement in the risk management process
  - facilitating risk identification/assessment and educating line staff in risk management and internal control
  - co-ordinating risk reporting

## 9. The Structure & Administration of Risk Management

### 9.5 Resources & Implementation:

- Resources should be clearly established at each level of management and within each business unit
- Special reference to resources for risk management, audit and internal control

Risk management should be:

- embedded through strategy & budget
- highlighted in induction and all other training and development as well as within operational processes

[www.theirm.org](http://www.theirm.org)

[enquiries@theirm.org](mailto:enquiries@theirm.org)



Institute of Risk Management  
6 Lloyd's Avenue  
London  
EC3N 3AX  
United Kingdom

