



# COMPLIANCE & RISK MANAGEMENT THE FOUNDATION

Presented By:

Mr Graham Caddies  
(CPRM, FRMIA, FSIA, FAIM, Grad MAICD)  
Advance Profitplan  
173 Ross River Road  
Mundingburra Qld 4812  
Phn: 47 253 955  
Fax: 47 754 024  
Email: [enquiry@advanceprofitplan.com.au](mailto:enquiry@advanceprofitplan.com.au)

## 1. INTRODUCTION

### 1.1. General

Compliance and Risk Management is the most misunderstood and misapplied and yet the most vital to any organisation. It is central, if applied properly, to any organisations, viability, direction, effectiveness and the ongoing health and safety of the individual and the protection of the environment.

It will only work if the principles and concepts are understood, the focus is right, applied for the right reason, the process followed and it becomes the culture at the individual, section, project and organisational level and it is an integral part of the business, project and decision making process..

### 1.2. Misconception/Misapplication

The following are some of the common things that result in compliance and risk not working:

#### a. Not Seeing It as a Management System

They see it as a tack on and don't see it should be an integral part of the Business Management System and the planning process at business or project level.

#### b. Not following the process

There is a process but most don't understand the various steps involved and in most cases leave out a couple of the vital steps.

#### c. Reactive Not Proactive

Many see it only relating to emergencies, where as if applied at the right stage can be very proactive.

#### d. Only apply at Task Level

Organisations operate on a range of processes. Some are directly involved in producing the product or service or supporting the organisation. Every process is made up of various steps and the steps made up of activities/tasks. Many start the risk process at the task level rather than at the process level.

#### e. Focus on the Risk Assessment Tools

Many put the emphasis on the assessment process using various tools such as risk matrix, fines tie line risk score calculator etc.

#### f. Only as Good as the Level Of Experience

The outcome is only as good as the experience, skills and competency of the person carrying it out. If the individual doesn't perceive that something is a risk then they wont identify it and more importantly wont apply properly.

#### g. Australian Standard 4360 doesn't apply to Safety because doesn't Cover Hazard

If the process is understood it can apply to any Safety Situation.

#### h. Got to Separate and Define Hazard and Risk

Too much emphasis is placed on defining hazard and risk when all we need to focus on is what could go wrong and why and if it does how would it impact the product, process, individual, environment etc.

**i. Turning into Robotic Application**

Many organisations are making staff do a risk assessment and J.S.A. (Job Safety Analysis) for everything they do. They are using a template that involves mainly tick and flick. Many are doing it robotically without thinking it through. It is becoming a bottom covering exercise.

**j. Forced on Individuals**

If it is forced onto people without fully understanding the process it will not work. It has to become part of the culture.

**k. One Person Involved**

Many approach it by only having one person carry out the process. The best and most effective is a team involvement and acceptance.

**l. Only Relates to Insurance/Finance**

Risk and Compliance applies to all activities and functions of any organisation.

**1.3 Integral to Everything**

Risk and Compliance is central to everything we do today whether as an individual or as an organisation. Some areas that demand it:-

- a. Corporate Governance;
- b. Legislation;
- c. Common Law/ Law of Tort;
- d. Triple bottom line (Social, Economic, Environmental Responsibility);
- e. Financing; and
- f. Business Continuity

It should apply in all business functional areas:-

- a. Business Development, Management;
- b. Marketing;
- c. Product/Service;
- d. Procurement;
- e. Asset Management and Maintenance;
- f. Human Resource Management;
- g. Information Technology;
- h. Administration; and
- i. Financial Management

**2. COMPLIANCE AND RISK MANAGEMENT - GENERAL**

**2.1 General**

Compliance and risk management is a critical component of managing and operating a business. It is sound Governance. It is the cornerstone of many pieces of legislation (especially Safety, Environmental and the proposed harmonised safety legislation) and is central to the quality (ISO 9001), safety (AS/NZS 4801) and environmental (ISO 14001) management system standards. It is important to understand the terminology and what is involved.

## 2.2. Due Diligence

Due diligence is when an organisation is able to demonstrate that the organisation had been duly diligent in meeting its obligations through developing, implementing and maintaining a management system. The following points are critical to proving this due diligence:

- Systems must be “effective” and not “paper”, “Legalistic” systems.
- Systems that emphasises results not process
- Systems are procedures that are in place and working procedures that outline what staff should do.

Essential ingredients of due diligence are:

- Real commitment to compliance
- Culture in the Business (a proactive culture that is not just about lip service)
- Consistent & effective enforcement – discipline, investigate, corrective / preventative action
- Full and effective reporting and actioning of reports
- Making sufficient resources available
- Satisfied system actually working – audits, monitor, inspect
- Identify and assess requirements as they impact your business
- Out sourcing / contractual obligations – You establish required standard and monitor
- Identify / analysis of risk exposure and manage / control
- Measure / assess level of compliance

These elements apply to any legislation and to the Australian Standards (ISO 9001, ISO 14001, AS/NZS 4801).

## 2.3. Compliance (Australian Standard AS3806)

### a. *Definitions*

Compliance means ensuring that the requirements of legislation, contracts, industry codes and organisational standards are met. From a quality perspective can include client requirements.

Includes Legal Compliance and System / Standard Compliance.

### b. *Common Elements*

The elements required under the compliance standard (AS3806) are applicable to the requirements for quality, safety, environmental, human resources. They are:

Commitment, policy, Management responsibility, resources, continuous improvement, identification of issues, operating procedures (systems), implementation, complaints handling, record keeping, identification and rectification, systematic and recurring problems, reporting, management supervision, education and training, visibility and communication, monitoring and assessment, review, liaison, accountability.

## 2.4. Legislation

### 2.4.1. General

Compliance and “Due Diligence” are central to ensure organisations meet their obligations under legislation. All businesses / organisations have a range of legislation (both Commonwealth & State) that impact their operation. The following are just a few that will have an impact:-

- Trade Practice, Environmental Protection, Workplace Health & Safety; and
- Compensation & Rehabilitation, Fair Work, Discrimination and Equal Opportunity;
- Corporation, Association Incorporation

All these have at their core – compliance / risk management and formal systems. You need to know and understand what is required, know your current level of compliance and what you need to do to improve.

Most legislation places an obligation on directors and senior managers to ensure the organisation complies with the requirements of the legislation.

### 2.4.2 Obligations

#### 2.4.2.1 General Obligations

##### Queensland Legislation

Only one piece of legislation actually places an obligation on the employer and persons in charge of a workplace to apply risk management. This is section 28 (Ensuring Health & Safety) Section 29 “Means of Ensuring Health & Safety” and 27A (Managing Exposure to Risks) of the workplace Health & Safety Act. It states the means to ensure workplace health and safety is following the risk management process. The Risk Management Code of Practice also sets out how to achieve the obligations.

Section 36 of the Environmental Protection Act is basically requiring employers and employees to apply the Risk Management process.

Other legislation also implies the application of the Risk Management Process.

The various pieces of legislation imply that for an organisation to achieve “Corporate Governance” and “due diligence” they need to identify and assess what obligations they have under legislation and what hazards/risks are directly or indirectly associated with their processes and product.

##### Other States Legislation

All other States have similar requirements to Qld WHS Act.

The Northern Territory has Section 55 which defines the “General Statutory Duties of Care” which includes Risk Management requirements. Section 58 requires a “Risk Management Plan” to be developed for hazardous activities.

### **Commonwealth Legislation**

The Occupational Health and Safety (Commonwealth Employment) Act 1991 doesn't have a specific section directly relating to Risk Management but in Division 1 "General Duties relating to Occupational Health & Safety" Section 16 "Duties of Employers" it requires employers to ensure the health and safety of employees and that they are free from risk to their health. The various parts of the supporting regulations also refer to risk management associated with specific risks such as a plant, hazardous substances, confined space etc.

Comcare / Work Safe have produced risk assessment checklists and general risk identification checklist for various specific risks such as manual handling. Comcare has also published an OH&S Risk Management Model/consisting of six (6) Principles. Principle 5 being "Risk Identification, risk assessment and risk control at the Workplace".

They require any practices or procedures produced to prevent and/or manage specific OH&S Risks must be integrated into existing operational practices and procedures.

### **Proposed Harmonised Federal "Safe Work Act" Due to be implemented late 2011**

Part 2 of this Act has four (4) key sections that are the foundation of the legislation and anchored on Risk Management. In Section 16 it defines the Principle of Risk Management and Section 18 defines the "Primary Duty of Care".

It is worth looking at these briefly:-

#### **Section 16 Principles of Risk Management**

"A duty imposed on a person to ensure Health & Safety requires a person:-

- a. To eliminate hazards and risks to health & safety, so far as is reasonably practicable; and
- b. If it is not reasonably practicable to eliminate hazards and risks, to minimise these hazards and risks so far as is reasonably practicable."

#### **Section 17 What is Reasonably Practicable?**

"Regard must be had and appropriate weight give to all relevant matters including:-

- a. Likelihood of the hazard or the risk concerned occurring;
- b. The degree of harm that might result from the hazard or risk;
- c. What the person concerned knows and ought reasonably to know about the hazard and risk and the ways to eliminate or minimising the hazard or the risk;
- d. The availability and suitability of ways to eliminate or minimise the hazard or the risk; and
- e. The cost of eliminating or minimising the hazard or risk."

## Section 18 Primary Duty of Care

“Persons or self employed person conducting a business or undertaking must ensure the health and safety of themselves, workers or any others who may be impacted by their activities by (without limiting the general duty) to ensure health and safety:-

- a. Provide/maintain safe and healthy work environment;
- b. Provide and maintain safe plant and structures;
- c. Provide and maintain safe systems of work;
- d. Ensure safe use, handling, storage and transport of plant, structures, substances;
- e. Provide adequate facilities for the welfare, at work, of workers;
- f. Provide any information, training, instructions or supervision that is necessary to protect all persons from risks to their health and safety arising from work carried out; and
- g. Ensure the health and safety of workers and the conditions at the workplace are monitored for the purpose of preventing illness or injury of workers arising from the conduct of the business or undertaking.”

### 2.4.2.2 Specific Obligations

Various Regulations and Advisory Standards under the Workplace Health & Safety Acts require organisations to undertake specific risk management processes. They require you to:-

- a. Identify the processes and sequence directly or indirectly involved in producing a product or service or undertaking a construction / building project;
- b. identify the steps in each process/activity
- c. identify and assess the hazards and associated risks
- d. Analyse each risk identified
- e. Establish controls for each risk
- f. Implement / monitor / review these controls
- g. Record each of the above

You are required to carry this out for:-

- a. Plant
- b. Manual Tasks
- c. Hazardous Substances
- d. High Risk Activities – Confined space, working at heights, working with high voltage
- e. Personal Protective equipment

If you look at the intent of the “general duties and obligations” it is inferring that organisations need to implement and maintain a Risk Management System at organisation, activity and project level. The new Australian and International Standard (AS/NZS ISO 31000) defines not only a process for identifying risks but also defines principles and framework for effective risk management, which if implemented effectively will enable organisation to meet their “General Duties” for ensuring Health & Safety.

## 2.5. Risk Management (Australian Standard AS/NZS ISO 31000:2009)

### 2.5.1. Definitions

- a. **Risk:**  
The effect of uncertainty on objectives. (an effect is a deviation from the expected – positive or negative. Often expressed in terms of a combination of the consequences of an event and the associated likelihood of the occurrence).
- b. **Risk Management:**  
Coordinated activities to direct and control an organisation with regard to risk.
- c. **Risk Management Framework:**  
Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
- d. **Risk Attitude**  
Organisation's approach to assess and eventually pursue, retain, take or turn away from risk.
- e. **Risk Management Plan**  
Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk.
- f. **Risk Owner**  
Person or entity with the accountability and authority to manage a risk.
- g. **Risk Management Process**  
Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk
- h. **Establishing the Context**  
Defining the external and internal parameters to be taken into account when managing risk, and setting the scope of risk criteria for the risk management policy.
- i. **Risk Source**  
Element which alone or in combination has the intrinsic potential to give rise to risk
- j. **Risk Profile**  
Description of any set of risks
- k. **Risk Criteria**  
Terms of reference against which the significance of a risk is evaluated.

### 2.5.2. Difference Between AS/NZS 4360 and AS/NZS ISO 31000

First of all the new Internal Standard evolved from the Australian Standard 4360. The risk management process defined in 4360 is exactly the same as the process defined in the new International Standard which is defined in Part 5 of the Standard.

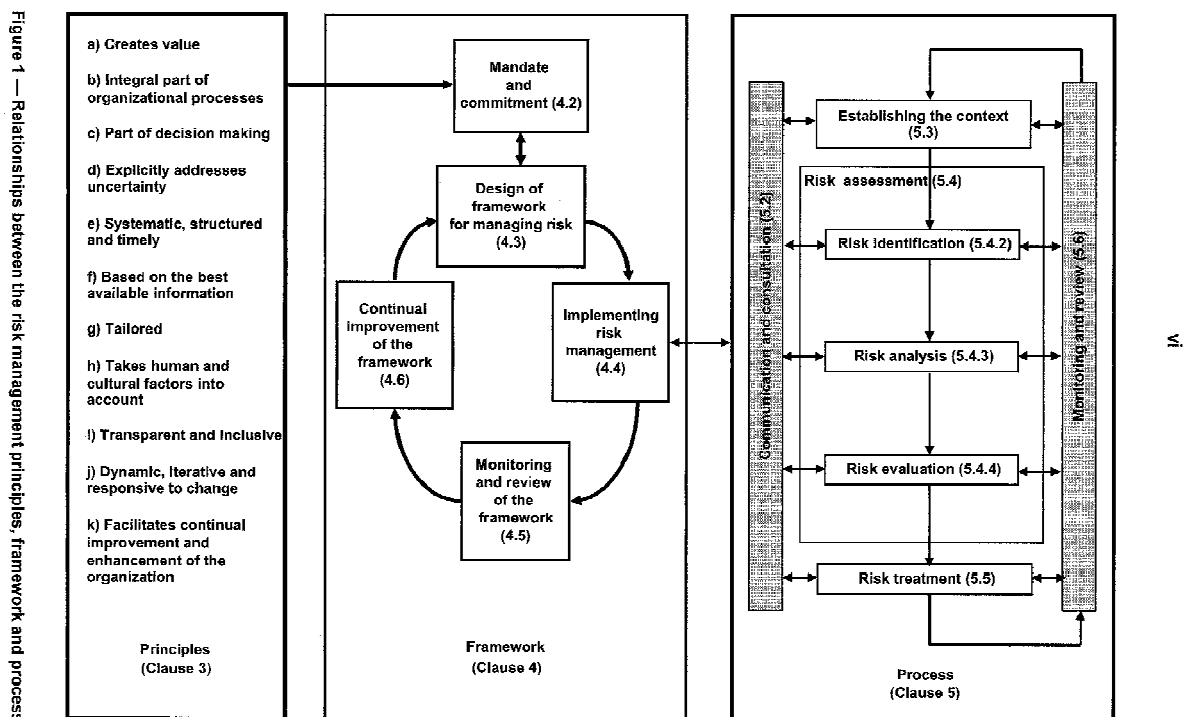
The difference is that 4360 only defined the risk management process and only partially covered the components of effective risk management where as the new Standard defines risk management being an integrated system of :-

- a. Principles;
- b. Framework; and
- c. Process

**NOTE:** The Standard is not a Standard that defines a Management System that can be audited to gain certification. It only provides principles and generic guidelines and risk management.

However if understood and applied in a formal way, will enable organisation to effectively manage risk and to meet their legislative, legal and other obligations.

The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in the Standard is shown in the following figure:-



### 2.5.3. The Principles

For risk management to be effective, an organisation should at all levels comply with the principles below:-

**a. Risk management creates and protects value.**

Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

**b. Risk management is an integral part of all organisational processes.**

Risk management is not a stand-alone activity that is separate from the main activities and processes of the organisation. Risk management is part of the responsibilities of management and an integral part of the organisational processes, including strategic planning and all project and change management processes.

**c. Risk management is part of decision making.**

Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

**d. Risk management explicitly addresses uncertainty.**

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

**e. Risk management is systematic, structured and timely.**

A systematic, timely and structures approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

**f. Risk management is based on the best available information.**

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

**g. Risk management is tailored.**

Risk management is aligned with the organisation's external and internal context and risk profile.

**h. Risk management takes human and cultural factors into account.**

Risk management recognises the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organisation's objectives.

**i. Risk management is transparent and inclusive.**

Appropriate and timely involvement of stakeholders and , in particular, decision makers at all levels of the organisation, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

**j. Risk management is dynamic, iterative and responsive to change.**

Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

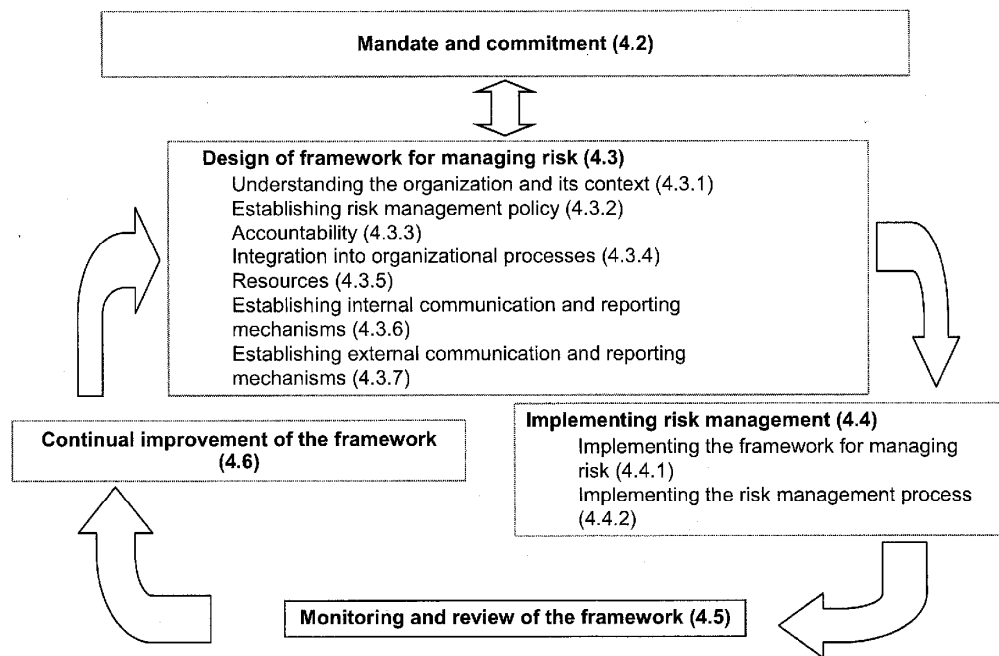
**k. Risk management facilitates continual improvement of organisation.**

Organisations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organisation.

**2.5.4. The Framework**

The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organisation at all levels. The framework assists in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of the organisation. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organisational levels.

This clause describes the necessary components of the framework for managing risk and the way in which they interrelate in an iterative manner, as shown in Figure 2.



**Figure 2 — Relationship between the components of the framework for managing risk**

### 2.5.5. Main Elements of the Risk Process

The main elements are:

- (i) **Communicate and Consult.**  
Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk process and concerning the process as a whole. You will note that this should occur at each step / stage of the process. From my experience this is usually not done or is not effectively done.
- (ii) **Establish the Context**  
Establish the external, internal and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined.  
  
This is critical to the process and is often not done at all or not done properly. It usually results in the process being faulty. It basically involves identifying external things that impact the organisation and internal things that may impact the required outcomes.
- (iii) **Identify Risks:**  
Identify where, when, why and how events could prevent, degrade, delay or enhance the achievement of the objectives.
- (iv) **Analyse Risks:**  
Identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk. This analysis should consider the range of potential consequences and how these could occur.
- (v) **Evaluate Risks**  
Compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.
- (vi) **Treat Risks**  
Develop and implement specific cost effective strategies and action plans for increasing potential benefits and reducing potential costs.
- (vii) **Monitor and Review**  
It is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement. Risks and the effectiveness of treatment measures need to be monitored to ensure changing circumstances do not alter priorities. It is also essential to ensure the treatments are working. This component should occur at each step / stage of the process. From my experience this is also not done well or not done at all.

**NOTE:** If you study the figure depicting the Rick Process you will see that each of the elements / components / steps are interrelated and it is an integrated process that is a closed loop process. It's effectiveness is that it is not linear with a start and finish but on going.

### 2.5.6. When to Apply

All organisations should ensure that all key personnel are trained in Risk Management and ensure that they apply it at Company and Project level. Employees should also be trained in the principles so that they can carry out a risk assessment before they undertake a job especially a high risk one or one that could cause a death or injury or short / long term health impact.

## 2.6. Using Legislation, Standards, Legal and Other Requirements as a Bench Mark / Guide

### 2.6.1. General

The Australian Standards (Management Systems, Compliance and Risk) and legislation are critical and an integral part of risk management for not only identifying requirements / obligations but for using as a guide or benchmark.

#### *a. Compliance*

- AS 3806-1998 Compliance Programs
- HB133-1999 Guide to AS 3806

#### *b. Risk Management*

- AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines
- HB 327:2010 Communicating and Consulting about Risks
- ISO Guide 73 Risk Management Vocabulary
- IEC/ISO 31010 Risk Management – Risk Assessment Techniques

#### *c. Management Systems*

##### Quality

- AS/NZS ISO 9001:2006 – Quality Management System
- AS/NZS ISO 9004:2009 Quality Management System – guide for performance improvement

##### Environment

- AS/NZS ISO 14001:2004 Environmental System
- AS/NZS ISO 14004:2004 General Guidelines on Principals, systems and supporting techniques.

##### Safety

- AS/NZS 4801:2001 Safety Management System
- AS/NZS 4804:2001 Guidelines for achieving Management Systems.

### 2.6.2. Legislation

As part of sound Corporate / Business Governance and Enterprise and Specific (Project / Activity) Risk Management it is critical that the organisation identifies all legislation that will impact their organisation overall and the specific ones that impact at operational / process / activity level. They need to identify the key obligations, how they impact, who owns these and how they will manage and achieve. This is a critical step in establishing strategy, direction and the risk process / framework. They need to develop a "Compliance Profile". They need to identify legislation (Act, Regulations, Code of Practice) from both the Federal and State level. They need to look at these from the following categories (not exhaustive):-

- a. Environmental;
- b. Personnel
  - i. Employment
  - ii. Health & Safety
  - iii. Compensation / Rehabilitation
  - iv. Harassment, Discrimination / Equality
  - v. Superannuation
- c. Specific to the Industry e.g. Building, Transport, Food, Health, Education / Training etc.
- d. General e.g. Trade Practice, Corporation, Finance / Taxation etc.

### 2.6.3. Legal and Other Requirements

This relates to such things as contractual, MOU's, certain insurance policy conditions, licences etc that impact the organisation, its operations or projects. Need to identify key requirements, how they impact, who they impact and the risks in not complying.

## 2.7. Level

As has been discussed before and as seen in the obligations, risks need to be considered at all levels:-

- a. Organisational
- b. Process / Activity
- c. Job
- d. Individual

In addition to these levels risk needs to be considered at specific levels (such as specific safety or environmental areas). These levels can be within the job, process and activity level. Risk Management takes the uncertainty out of the potential risk exposure, it allows for more effective planning and control at all levels.

## 2.8. Concept

The concept of risk has three elements:

- a. the perception that something could happen
- b. the likelihood of something happening; and
- c. the consequences if it happens.

Understanding these and applying them fully is the difference between a superficial risk assessment and a thorough assessment. The outcome of the risk process is directly related to the knowledge, skills and experience of the persons conducting the assessment.

## 2.9. Sources of Risk

### 2.9.1. Generic

The following are generic categories of risk at organisational level:

- a. commercial / legal relationships;
- b. socio-economic;
- c. political / legal;
- d. personnel/human behaviour;
- e. financial / market;
- f. management activities and controls;
- g. technology / technical;
- h. the activity itself / operational;
- i. business interruption;
- j. occupational health and safety;
- k. property / assets;
- l. security;
- m. natural events;
- n. public/professional/product liability; and
- o. custody of information including the duty to provide and to withhold access.

For ease of analysing and establishing controls for various risks the above generic categories can be categorised into four (4) key areas:-

- a. Property
- b. Income
- c. Liability
- d. Personnel

When carrying out the risk process for an organisation you need to identify all types of risk exposure in each of these categories.

### 2.9.2. Specific

Some disciplines categorise the above generic risks in other ways. They use terms like 'hazard or risk exposure'.

For example the scientific field or medical may have a category of "Diseases (affecting human, animals and plants). The safety profession uses hazard and risk. The Health & Safety Advisory Standard 2000 uses both by defining the hazard and the possible risk to a worker.

## 2.10. Treatment / Control of Risk

### 2.10.1. Control of Risk\_(Health and Safety Specific)

The hierarchy of control of risk in order of priority is:-

- a. Eliminate the hazard
- b. Prevent or minimise exposure to the risk by:-
  - (i) substitution – substance / material / process

- (ii) Redesign – equipment / method / layout / process
- (iii) Isolating the hazard
- c. Administrative Controls
  - (i) Job rotation
  - (ii) Restrict time exposure
  - (iii) Supervision
  - (iv) Procedures
  - (v) Signs
  - (vi) Preventative maintenance
  - (vii) Training
- d. Personal Protective Equipment (if safety related).

### 2.10.2. Treatment of Risk (General)

The Australian Standard defines this in detail. It uses different terms but they are similar to the ones used in the OH&S Advisory Standard.

Basically an organisation can:-

- a. Reduce the consequence or likelihood (or both) of the risk eventuating (this involves the above hierarchy of controls)
- b. Avoiding the risk (eliminating / alternative)
- c. Acceptance (do nothing)
- d. Transfer (get another organisation to do)
- e. Exploit (take advantage of the risk)

## 2.11. Documentation Required

In both the compliance and risk management process it is critical to document the identification and assessment process. In fact it is a legislative requirement, especially the OH&S Act.

For a small process this step may be documented by a simple tabulation where as more complex documentation may be required for a larger process.

The following is the minimum required:-

- a. list each risk, identify its source and consequences (for safety include hazards);
- b. classify risks under functional groups if appropriate;
- c. identify each control process and how the risk is to be treated;
- d. identify areas of research if appropriate;
- e. who was involved in the process;
- f. when was the risk assessment process conducted.
- g. Any assumptions made

## 2.12. Requirements

Effective risk management requires:-

- a. Rigorous thinking: (logical and systematic process – a means to an end not an end in itself)
- b. Forward thinking: (identifying and being prepared for what might happen – threat or opportunity.)
- c. Proactive rather than reactive management
- d. Responsible Thinking: (identifying and taking opportunities to improve as well avoid or reduce possible loss/harm)

- e. Accountability in decision making: (decision making and acting in ways that are consistent with statutory requirements and corporate values / ethics)
- f. Balanced thinking: (deciding what level of risk is acceptable – balancing cost with benefit)
- g. Understanding: (thorough understanding of business operations, hazards/ risk associated with)
- h. Research : (thorough gathering of information)
- i. Involvement / Consultation: (it requires involvement of all concerned (especially employees) expert assistance maybe)
- j. Documentation / Records (Documenting process and outcomes)

### 2.13. Key Questions in Identifying Risks

Whether you are conducting the risk process at the organisational level or whether at the specific level the following questions are critical to the outcome of the process and the thoroughness of the process:

- a. When, where, why, how are the risks likely to occur, and who might be involved?
- b. What is the source of each risk?
- c. What are the consequences of each risk?
- d. What is the potential cost in time, money and disruption to clients of each risk?
- e. What controls presently exist to mitigate this risk?
- f. What are the accountability mechanisms – internal and external?
- g. What is the need for research into specific risks?
- h. What is the scope of this research?
- i. What resources are needed to carry out the research?
- j. What is the reliability of the information?
- k. What are the stake holders expectations of the organisations performance?

### 2.14. Possible Method of Identifying Risks

As indicated before the process of identifying risks is the most critical. It requires detailed knowledge of and an understanding of the Organisations policy, processes and activities being reviewed. It should be, where possible, conducted by more than one person. It should involve personnel working in the activity. You should also consider having experts give advice/guidance.

The following are methods that should be considered when identifying risks and analysing risks.

- a. Interview / focus group discussion;
- b. Personal experience or past organisational experience;
- c. Audits or physical inspections;
- d. Brainstorming;
- e. Survey, questionnaire;
- f. Examination of local or overseas experience (internet / worksafe / visits)
- g. Judgmental – consensus, speculative / conjectural, intuitive;
- h. History, failure analysis;
- i. Scenario analysis;
- j. Decision trees;
- k. Strengths, weaknesses, opportunities and threats (SWOT) analysis;
- l. Flow charting, system design review, systems analysis, systems engineering techniques, e.g. hazard and operability (HAZOP) studies;
- m. Work breakdown structure analysis; and
- n. Operational modelling.

### 3. ACHIEVING INTEGRATION INTO YOUR ORGANISATION

#### 3.1. Process Starting Point Analysis:

The following is the starting point for the compliance / risk management process and for any other specific analysis such as skills / training analysis, work methods etc.

- a. Conduct a business / organisation analysis:-
  - i. Your product / industry
  - ii. Your strategic direction, business / operational plans
  - iii. Business strategies / objectives / standard required
  - iv. Existing management system and information / communication technology
  - v. Compliance requirements
  - vi. Existing resources etc
  - vii. Organisational structure
- b. Identify the processes and activities (develop a process map/flowchart)
- c. Identify the following for each activity / steps within each process;
  - i. Hazards
  - ii. Risks
  - iii. Flow / layout
  - iv. Work method
  - v. Skills, competencies required
  - vi. Materials / substances
  - vii. Equipment / tools / work aids
  - viii. Existing controls
  - ix. Quality issues
  - x. Environmental issues
- d. Identify your existing Assurance and Continuity activities and assess how effective they are
- e. Assess current competency of staff to perform their job to standard required

Many organisations carry out step 'c.' separately, when in actual fact they would achieve better results if they were completed together.

#### 3.2. Establish Direction

Once you have conducted your business / organisation analysis you need to establish the following:-

- a. Governance Directives / Policy / Objectives / Standard Required / KPI's
- b. Formal Integrated Management System;
- c. Organisational Structure including responsibilities, authority and accountability
- d. Adequate resources – facilities, people, equipment, money etc
- e. Integrated Assurance Program – inspections, audits, reviews etc.
- f. Compliance / Risk Profile
- g. Organisational Continuity should the risk eventuate