



Working together to achieve maximum results

COMPLIANCE MANAGEMENT & RISK MANAGEMENT

THE FOUNDATION

PRESENTER: **MR GRAHAM CADDIES** CPRM, FSIA, FRMIA, FAIM

Vice President SIA QLD Div.

Advance Profitplan; Townsville

email: enquiry@advanceprofitplan.com.au

COMPLIANCE & RISK - OVERVIEW

CONTENT

- Misconception.
- Due Diligence / Compliance / Legislation
- The New Standard
- Key Questions
- Achieving Integration in your Organisation.

COMPLIANCE & RISK - OVERVIEW

It will only work if:

- the focus is right
- applied for the right reason
- the process is understood and followed
- it becomes the culture – individual, section, organisation.

COMPLIANCE & RISK - OVERVIEW

MISCONCEPTION / MISAPPLICATION:

- Not seeing it as a Management System
- Not following process.
- Reactive not proactive.
- Only apply at task level.
- Focus on risk assessment tools.
- Only as good as level of experience.
- 4360 doesn't address hazards.
- Got to separate and define hazard and risk.
- Turning into robotic application.
- Forced on individual.
- One person carries out.
- Miss vital steps.
- Only relates to insurance/finance.

COMPLIANCE & RISK - OVERVIEW

It is integral to everything we do:

- Corporate Governance
- Legislation
- Triple bottom line reporting
- Financing
- Business Continuity Planning

Integrate into everything, a culture change:

- Planning
- Business Functions
- Resourcing
- Facilities

COMPLIANCE / RISK MANAGEMENT INTRODUCTION

Compliance / Risk Management:

- Critical aspect of Managing/Operating a Business/Organisation;
- Corner stone of most legislation;
- Sound Governance and critical to Due Diligence;
- Integral part of quality, safety and environmental management system standards.

COMPLIANCE / RISK MANAGEMENT INTRODUCTION

Due Diligence:

Is when an organisation is able to demonstrate that the organisation has been duly diligent in meeting its obligations through developing, implementing and maintaining a management system.

COMPLIANCE / RISK MANAGEMENT INTRODUCTION

COMPLIANCE

“means ensuring that the requirements of legislation, contracts, industry codes and organisational standards are met.”

COMPLIANCE / RISK MANAGEMENT INTRODUCTION

- Existing Federal and State legislation requires the application of Risk Management to ensure Health & Safety of workers and others who may be impacted by the activities of the workplace
- The harmonisation legislation – Safe Work Act requires the same.

LEGISLATIVE SPECIFIC OBLIGATIONS

To meet legislative requirements need to:

- Identify processes and sequence of work
- Identify the steps in each process/activity
- Identify and assess the hazards and associated risks
- Analyse each risk identified
- Establish controls for each risk
- Implement / monitor / review these controls
- Record each of the above.

LEGISLATIVE SPECIFIC AREAS

- Plant;
- Manual Tasks;
- Hazardous Substances;
- High Risk Activities – Confined space, working at heights, working with high voltage;
- Personal Protective Equipment;
- Electrical – High Voltage;
- Environmental Harm;
- All work undertaken.

DEFINITIONS

RISK

The effect of uncertainty on objectives. (one 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).

DEFINITIONS

Risk Management

Coordinated activities to direct and control an organisation with regard to risk.

DEFINITIONS

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.

DEFINITIONS

Risk Attitude

Organisation's approach to assess and eventually pursue, retain, take or turn away from risk.

DEFINITIONS

Risk Management Plan

Scheme within the risk management framework specifying the approach, the management component and resource to be applied to the management of risk.

DEFINITIONS

Risk Owner

Person or entity with the accountability and authority to manage a risk.

DEFINITIONS

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.

DEFINITIONS

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.

DEFINITIONS

Risk Source

Element which alone or in combination has the intrinsic potential to give rise to risk

Risk Profile

Description of any set of risks

Risk Criteria

Terms of reference against which the significance of a risk is evaluated.

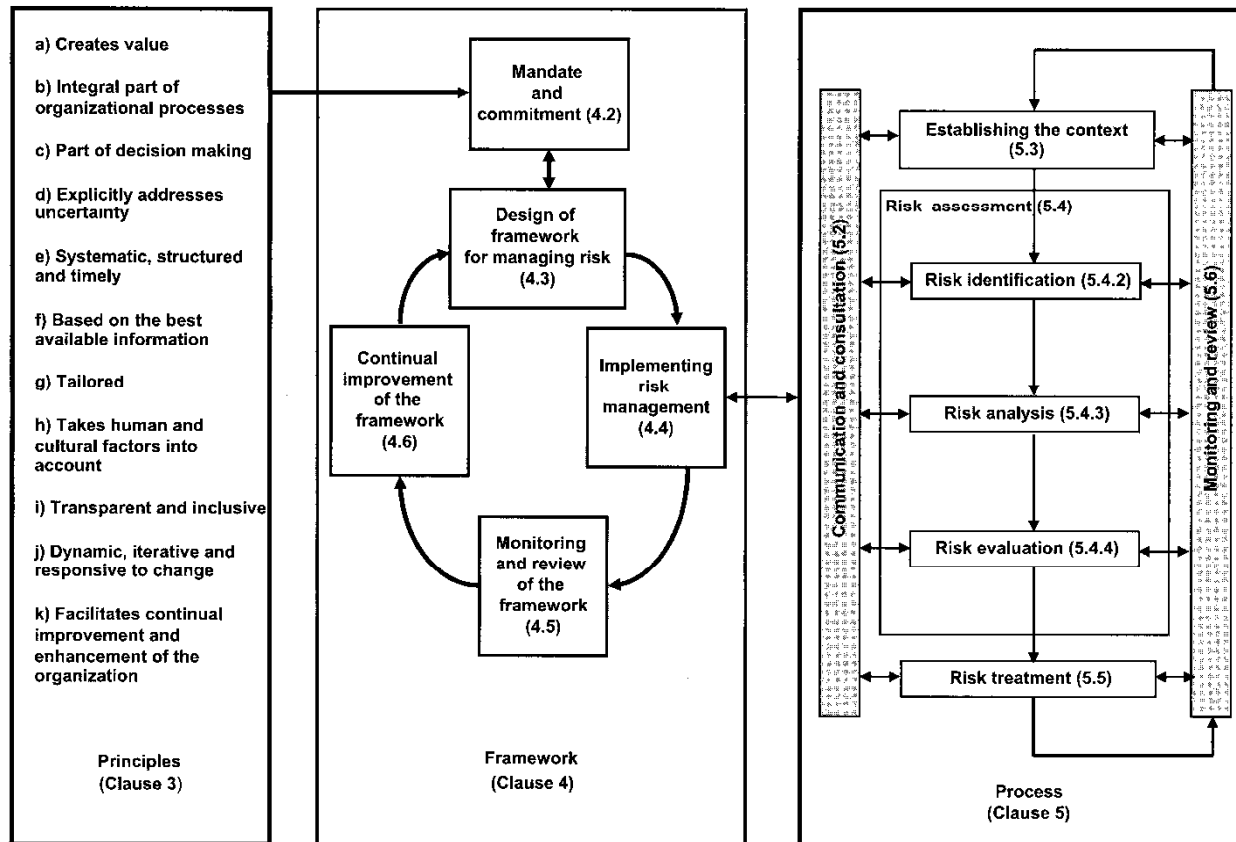
RISK MANAGEMENT

Difference between AS/NZS 4360 and AS/NZS ISO 31000

- 4360 defined a risk process
- 31000 defines
 - Risk Principles
 - Risk Framework
 - Risk Process

RISK MANAGEMENT

Figure 1 — Relationships between the risk management principles, framework and process

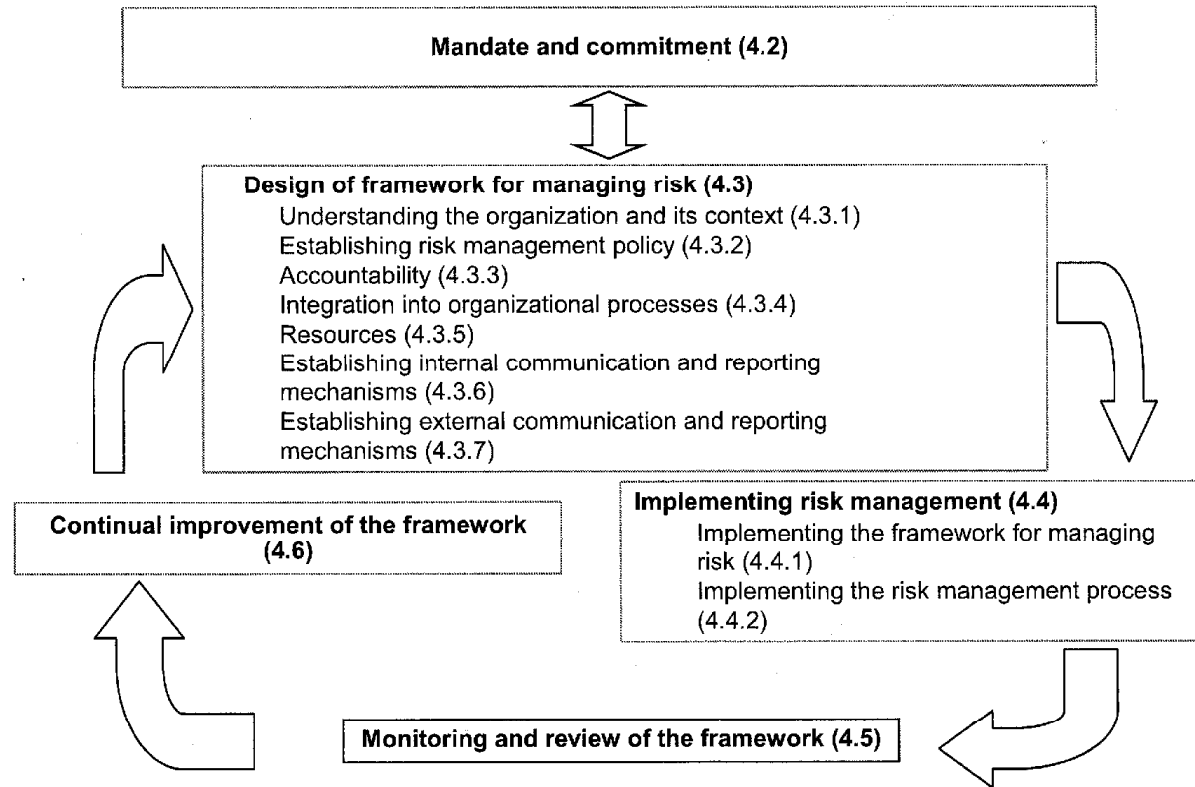


RISK MANAGEMENT PRINCIPLES

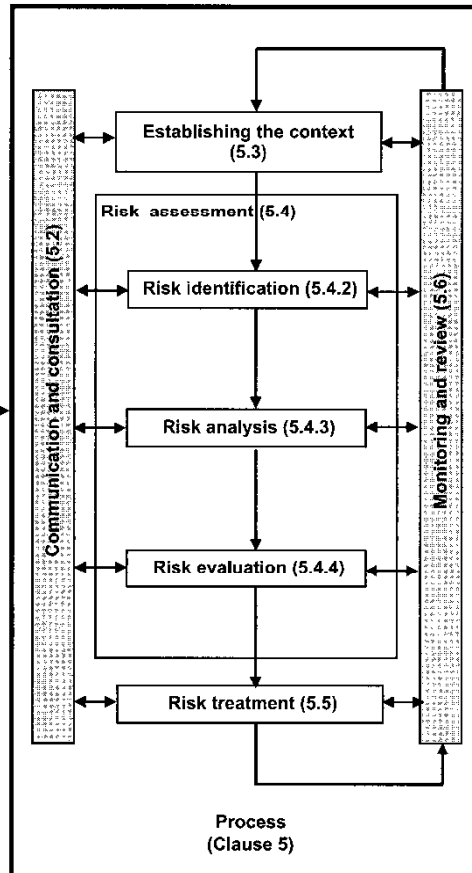
- a) Creates value
- b) Integral part of organizational processes
- c) Part of decision making
- d) Explicitly addresses uncertainty
- e) Systematic, structured and timely
- f) Based on the best available information
- g) Tailored
- h) Takes human and cultural factors into account
- i) Transparent and inclusive
- j) Dynamic, iterative and responsive to change
- k) Facilitates continual improvement and enhancement of the organization

Principles
(Clause 3)

RISK MANAGEMENT FRAMEWORK



RISK MANAGEMENT PROCESS



BENCHMARK / GUIDANCE

- Management System Standards
 - ISO 9001, ISO 14001, AS/NZS 4801
- Compliance (AS 3806)
- Risk Management (AS/NZS ISO 31000, HB327)
- Legislation
- Legal and other requirements

GENERAL LEVELS

Risk process applies at all levels.

- **Organisational**
- **Project**
- **Process / Activity / Job**
- **Individual**

RISK MANAGEMENT

- Takes uncertainty out of potential risk exposure;
- Allows for effective planning and control at all levels.

ELEMENTS OF CONCEPT OF RISK

- Perception something could happen
- Likelihood something could happen
- Consequence of it happening

POSSIBLE SOURCES OF RISK (GENERIC)

- Commercial / legal relationships;
- Socio-economic;
- Political / legal
- Personnel / human behaviour;
- Financial / market;
- Management activities and controls;
- Technology / technical;
- The activity itself / operational;
- Business interruption;
- Occupational health & safety;
- Property / assets;
- Security;
- Natural events;
- Public / professional / product liability; and
- Custody of information

GENERAL CATEGORIES

- Property
- Income
- Liability
- Personnel

SPECIFIC CATEGORIES

- **Health & Safety (Hazard / Risk)**
- **Environmental (Aspects / Impact)**

HIERARCHY OF CONTROL OF RISK

- **Eliminate the hazard;**
- **Prevent or minimise exposure to the risk by:-**
 - Substitution – substance / material / process;
 - Redesign – equipment / method / layout / process;
 - Isolating the hazard.
- **Administrative Controls**
 - Job rotation;
 - Restrict time exposure;
 - Supervision;
 - Procedures;
 - Signs;
 - Preventative maintenance;
 - Training.
- **Personal Protective Equipment (if safety related)**

Treatment of Risk

- Reduce consequence / likelihood
- Avoid the risk (eliminate / alternative)
- Accept
- Transfer
- Exploit

DOCUMENTATION REQUIRED

- **List each risk, source, consequence;**
- **Classify risks;**
- **Identify control process and how the risk is to be treated;**
- **Identify areas of research;**
- **Who was involved;**
- **When was the risk assessment process conducted;**
- **Any Assumptions made.**

REQUIREMENTS

- Rigorous thinking;
- Forward thinking;
- Proactive rather than reactive;
- Responsible thinking;
- Accountability in decision making;
- Balanced thinking;
- Understanding;
- Research;
- Involvement / Consultation;
- Documentation / Records;

KEY QUESTIONS IN IDENTIFYING RISKS

- **When, where, why, how the risks are likely to occur?**
- **Who might be involved?**
- **Source of each risk?**
- **Consequences of each risk?**
- **Potential cost?**
- **Disruption to clients of each risk?**
- **What controls presently exist?**
- **Accountability mechanisms?**
- **Need for research into specific risks?**
- **Scope of this research?**
- **Resources needed to carry out the research?**
- **Reliability of the information?**
- **Stakeholders expectations?**

PROCESS STARTING POINT- BUSINESS ANALYSIS

- **Industry / Product;**
- **Strategic / Business / Operational Plans**
- **Objectives / Standards / KPI's**
- **Management System;**
- **Information Technology**
- **Compliance Requirement**
- **Resources**
- **Organisational Structure**

PROCESS STARTING POINT- INTEGRATION

- **Identify the processes and activities;**
- **Identify the following for each activity within each process:-**
 - Hazards;
 - Risks;
 - Flow / Layout
 - Work method
 - Skills, competencies required
 - Equipment / tools / work aids
 - Existing controls
 - Quality issues
 - Environmental issues
- **Identify existing Assurance / Continuity Plans**
- **Assess current competency of staff**

PROCESS DIRECTION ESTABLISH

- **Governance / Policy / Standard**
- **Integrated Management System**
- **Organisational Structure**
- **Adequate Resources**
- **Integrated Assurance Program**
- **Compliance / Risk Profile**
- **Business Continuity**