Governance, Compliance, Risk, Assurance, Continuity and Health, Safety and Welfare (HSW)

Graham Caddies
Owner / Principal
Advance Profitplan

1. INTRODUCTION

Where do we take Health, Safety & Welfare (HSW) next within organisations? Whether your organisation is Government, Semi Government or private sector, large or small, profit or not profit I want to suggest we need to change our focus, widen our scope and look outside the "norm", "the square".

We need to seriously start engaging not only at the shop floor level but at all levels – Board, Senior Management, Middle and Front Line Management and Workforce. We also need to start engaging within the organisation at the following levels:-

a. Shop Floor level;
b. Organisational level;
c. Supplier / Contract level;
d. Design / Planning level; and
e. Resourcing level

The other change of focus is to seriously address and understand the whole person (mental, physical and social being) and their interaction with work environments, work aids and work systems / practices.

The last change of focus is practical integration of HSW into every aspect of how an organisation is managed and operated and their business / operational of systems.

If we as professionals (internal or external) want to impact the short and long term HSW of individuals and to change the culture we need to understand each of the areas above, we need to talk the language at each level and we need to be competent in business and management and not just HSW.

In the time I have I can not cover all of the above so I want to put some light on what is Governance, Compliance, Risk, Assurance and Continuity and how HSW relates to these.

I want to briefly look at terminology, principals and process in each of these and how they are integrated. I acknowledge that many organisations do not understand or apply these very well but they are finding they have to get better at these if they are to meet their legislative and legal obligations and remain viable.

I want to suggest that we need to start with Directors duties and obligations and how these lead to those areas. I want to look at some practical ways to achieve this and I want to generate a debate on how we in the safety and risk profession can influence this necessary change. I want to look briefly at the following:-

a. Summarise the components of the levels mentioned above;
b. The critical components of an enterprise / business / organisation;
c. Terminology and guidance documents relating to some of these components;
d. Duties / obligations / compliance;
e. Practical Implementation.

2. SUMMARY OF COMPONENTS OF HSW LEVELS

To assist with linking all the levels together I believe the following are some of the critical components:-

a. Shop Floor Level
    i. Empowering workers to make changes and apply HSW;
    ii. Empowering front line management / supervision to ensure HSW;
    iii. Improving understanding of hazards and potential risks;
    iv. Effective consultation, cooperation and partnership;
    v. Provision of information, instruction, training and supervision to ensure HSW;
    vi. Providing and maintaining safe work environment and work practices;
    vii. Addressing complacency;
    viii. Ensuring competency to perform task / job;
    ix. Enforcement and assurance;
    x. Ensure specific to organisation and its work areas and not generic.

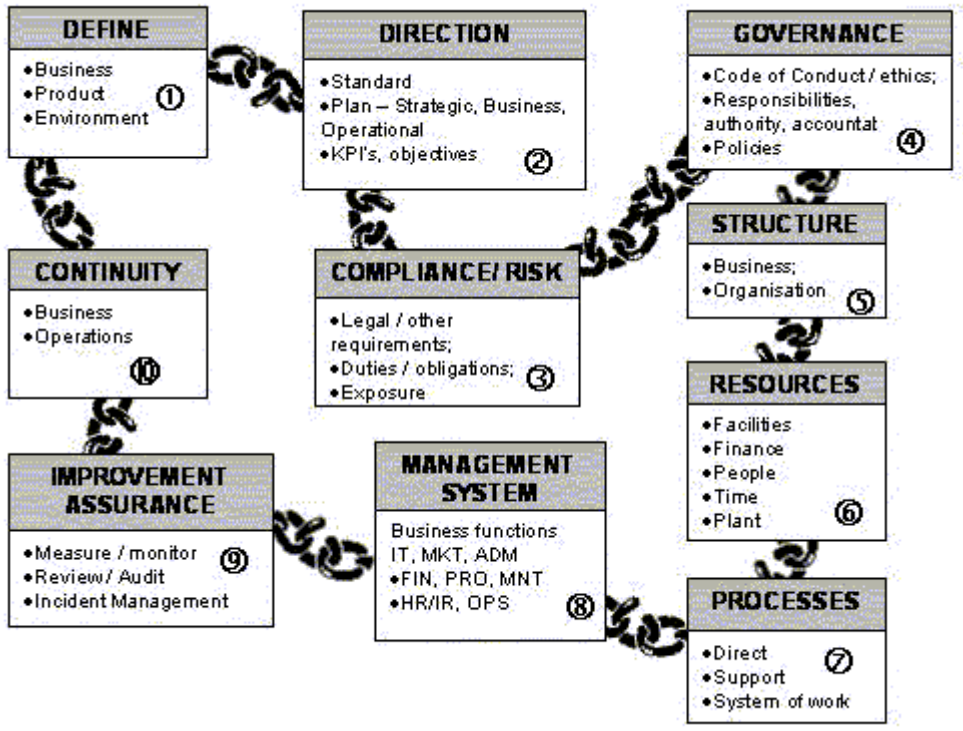
b. Organisational level
    i. Integrate Governance, Compliance, Risk, Assurance, Continuity with HSW being an Integral component;
    ii. Performance, accountability, responsibilities;
    iii. Formalised integrated management systems to achieve nominated standard and consistency;
    iv. Reporting – Corporate Social Responsibility (CSR) and Triple Bottom Line (Social, Economic Environment).
c. Supplier / Contractor Level
    i. Establishing systems and standards;
    ii. Establish a partnership;
d. Design / Planning (Internal)
    i. Design facilities, work layout, work practices, work process, plant and material to meet obligations and ensure compliance;
    ii. Establishing clear, achievable, measurable direction through effective planning at strategic, business, operational, project, resource and day to day level.
e. Resourcing Level
    i. Providing and maintaining all resources to achieve the required standard and outcome. Fit for purpose and sufficient.

To be effective in ensuring HSW we need to carry out all of the above as an integrated process. With the time available I am going to concentrate on one level and one component within that level.

3. COMPONENTS OF AN ENTERPRISE / ORGANISATION

If you were to analyse every organisation (profit, not for profit, government), the following components interact to enable the organisation to provide / produce its product(s) or deliver its service(s). The degree of application is directly linked to the type of organisation e.g. a company operating under the Corporations Act (shareholders / Directors) and the complexity, size and risk exposure of the organisation. They also depend on the degree of impact of both internal and external influences.

Interrelated Business Components



There are probably some additional boxes or links you could add, but I am not debating what are the components but rather I want to debate and show what is involved with and what is meant by ERM (Enterprise Risk Management) and how the health, safety, welfare (HSW) fits into each of these components. Even though I have shown compliance / risk as a separate box, I want to suggest this is integral to the total process and drives each of the other boxes.

We need to look at some of these boxes and what is involved and the associated terminology before I can focus on the subject of this paper – "Governance, Compliance, Risk, Assurance, Continuity and HSW". To fully address this specific subject we also need to briefly look at the duties of Directors and obligations of Directors, Management, Supervisors and workers.

4. TERMINOLOGY / GUIDANCE DOCUMENTS

To achieve the change of focus and integration it is critical that management, (Directors to Leading Hands), and safety professionals have a common understanding of the concepts, principles and terminology involved. Having a common understanding improves the chances of practical application across the Enterprise and each of its business functional areas. I will only highlight key points.

4.1. Corporate Governance

Corporate Governance is the system by which entities are directed, managed and controlled. It is about accountability, performance and relationships.

Corporate Governance generally refers to the processes by which organisations are directed, controlled and held to account. It encompasses authority, accountability, stewardship, leadership, direction and control exercised in the organisation.

Governance addresses the issues arising from the inter-relationships between Directors, Senior Management and relationships with owners, and other interested parties, including employees, regulators, auditors, creditors, financiers, analysts, suppliers etc.

Corporate (organisational) Governance is not a single activity or function but an umbrella term for incorporating a wide range of long practiced Board and Management activities that collectively assist in directing and controlling an organisation. These are:-

a. Strategic planning
b. Risk Management
c. Performance assessment
d. Board Composition
e. Remuneration and reward
f. CEO / Executive appointment
g. Shareholder / stakeholder reporting
h. Values and ethics

Of the ten (10) Principles of the ASX Good Governance Principles, four (4) directly relate to the subject and intent of this paper:-

a. Principle 1 – lay solid foundations for management and oversight
b. Principle 3 – Promote ethical and responsible decision making
c. Principle 7 – Recognise and manage risk
d. Principle 8 – Encourage enhanced performance

The Australian Standards AS 8000 series outlines the requirements for Corporate Governance:-

a. AS 8000 – Good Governance Principles
b. AS 8001 – Fraud & Corruption Control
c. AS 8002 – Organisational Codes of Conduct
d. AS 8003 – Corporate Social Responsibility
e. AS 8004 – Whistle blower Protection Program

These standards outline a range of things for governance but I want to highlight three (3) Board responsibilities that directly relate to the subject of this paper:-

a. Ensure compliance to applicable laws;
b. Ensure that risks facing the entity have been identified, assessed and that the risks are being properly managed;
c. Ensure policies on key issues are in place, appropriate and reviewed for compliance (see AS 3806 for compliance programs).

Isn't this what compliance, risk, assurance and business continuity is about and isn't this where they should be centred and started. Isn't this directly related to HSW?

There are a range of documents giving guidance for applying Governance, the following are just a few:-

a. ASX Corporate Governance Council – The ASX Principles;
b. OECD Principles of Corporate Governance;
c. Australian Standards:
   (i) AS 8000:2003 Series (8000-8003) Principles, Codes of Conduct, Corporate Social Responsibility (CSR);
   (ii) AS 3806:2006 Compliance Programs;
   (iii) AS/NZS 4360:2004 Risk Management.

The main documents giving guidance to integrating Governance, risk management is Australian Standard Hand Book HB254:2005 Guide to Controls Assurance and Risk Management and HB158:2006 Delivering Assurance based on AS/NZS 4360.

4.2. Compliance

Compliance is adhering to the requirements of laws, industry and organisational standards and codes, principles of good governance and accepted community and ethical standards. Compliance is based on twelve principles which are grouped under four (4) headings:-

a. Commitment;
b. Implementation;
c. Monitoring and measuring;
d. Continued Improvement.

The document giving guidance to implementing and achieving compliance is Australian Standard AS 3806:2006 Compliance Programs.

4.3. Risk Management

Risk is the chance of something happening that will have an impact on objectives. These can be positive or negative. Risk Management is the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.

The Company Directors Manual defines Risk Management *"is about assisting businesses to achieve their objectives, through performing their activities in a manner where they understand and expose themselves to the level of risk they are prepared to accept and are capable of bearing"*.

There are seven (7) elements of the risk process:-

a. Element 1 – Communicate and Consult (throughout)
b. Element 2 – Establish Context (critical)
c. Element 3 – Identify risks (all)
d. Element 4 – Analyse risks
e. Element 5 – Evaluate risks
f. Element 6 – Treat Risks
g. Element 7 – Monitor / Review (assurance)

The words in bracket are my words. Elements 1, 2 and 7 are not well understood and not well applied. The risk process requires the involvement of more than one person. It can not be carried out in isolation. It is critical as a management tool, a HSW tool and decision making tool.

The documents giving guidance to achieving this are Australian Standards:-

a. AS/NZS 4360:2004 Risk Management;
b. HB 436:2004 Risk Management Guidelines.

4.4. Assurance

Assurance is a process that provides confidence that planned objectives will be achieved within an acceptable degree of residual risk.

Assurance is based on planned controls to manage risk exposure and includes adequacy and effectiveness of controls. Adequacy of risk management, control and governance processes is present if management has planned and designed them in a manner that provides reasonable assurance that the organisations objectives and goals will be achieved efficiently and economically. HSW is integral to the process.

The assurance process consists of the following:-

a. developing an assurance strategy
b. planning an assurance engagement
c. reporting the assurance program; and
d. designing controls.

The assurance process and program can be sourced and carried out internally or externally. At shop floor level assurance includes planned inspections and at organisation level includes audits and management reviews and reporting.

The main document is Australian Standard HB158:2006 "Delivering Assurance based on AS/NZS 4360" which builds on and is a companion to HB254:2005. Other standards that give guidance are:-

a. AS/NZS ISO 9001 Quality Management System
b. AS/NZS ISO 14001 Environmental Management System
c. AS/NZS 4801 Safety Management Systems

4.5. Business Continuity

Business Continuity is 'the uninterrupted availability of all key resources supporting essential business functions." **Business Continuity Management** provides for the availability of processes and resources in order to ensure the continued achievement of critical objectives. **Business Continuity Plans** are a collection of procedures and information that is developed, complied and maintained in readiness for use in the event of an emergency or disaster.

The main guidance document for Business Continuity is Australian Standard Handbook HB 221:2004 Business Continuity Management.

Business Continuity Management – An Integral Part of Risk Management

Current thinking on business continuity recognises the importance of business continuity planning (BCP) and disaster recover, but now places it as an essential aspect of sound risk management, corporate governance and quality management. Understanding of business continuity has evolved substantially from the historically narrow concepts of BCP in specialised areas, such as information technology, disaster recovery and crisis management, to a more holistic approach embracing all aspects of strategic and operational areas of an organisation.

Business continuity management (BCM) now includes the concepts of business resilience and long term performance. The outcomes of BCM today, and into the future, need to contribute a substantial benefit to the continuity of an organisation before a major disruption, as well as following the disruption.

BCM can assist organisations, regardless of size, to sustain good corporate governance; maintain their customer base, market share, reputation and public image; and assist market growth.

The key elements of BCM include:-

- Understanding the overall context within which the organisation operates.
- Understanding what the organisation absolutely must achieve (the critical objectives);
- Understanding what barriers or interruptions may be faced in trying to achieve these critical objectives;
- Understanding the probable outcome of controls and other mitigation strategies (remaining residual risk);
- Understanding how the organisation can continue to achieve these objectives should interruptions occur;
- Understanding the criteria or triggers for implementing crisis and emergency response, continuity response and recovery response procedures;
- Ensuring that all staff understand their roles and responsibilities when a major disruption occurs;
- Ensuring that there is a clear understanding throughout the organisation of what accountabilities and responsibilities are in place when emergency, continuity and recovery response are in effect, and that currency is maintained;
- Building consensus and commitment to the requirements, implementation and deployment of business continuity integrated as part of the routine way 'we do business';

The terms 'corporate governance', 'risk management', and 'business continuity management' are, by their very nature, broad concepts.

The principles of good corporate governance require that an organisation undertakes appropriate risk management practices including effective business continuity management. In turn, the establishment of effective business continuity management requires the use of well founded risk management processes. At the same time, effective risk management and business continuity management at the strategic level will dictate the establishment of an appropriate corporate governance framework.

The key outcome of any BCM process should be to identify what is the minimum level of acceptable performance of the organisation and what infrastructure and resources are required to achieve and sustain it. Obviously a major benefit of a well conducted BCM approach should be to place the organisation in a more resilient position than previously.

"The above is extracted from the Australian Standards handbook HB221."

Before looking at practical applications, we need to briefly look at duties and obligations under legislative, legal and other requirements.

5. DUTIES / OBLIGATIONS

5.1. General

To address the issue of Corporate Governance, compliance, risk and Business Continuity we firstly need to briefly look at the role and responsibilities of the Board and individual Directors in general terms. This section is based on the 'Company Director Manual' as put out by the Australian Institute of Company Directors.

5.2. General Duties

The Common Law principle of the duties of Directors is to act honestly, to exercise reasonable care and skill, to be diligent and to be aware of and understand the fiduciary duties of a Director.

Fiduciary (one who holds a thing in trust – that is the business on behalf of the shareholder). A wide range of duties imposed on Directors and others who engage in management. These duties are stricter and involve greater potential liabilities than is the case for employees.

Directors have the following individual duties (Not all are covered):-

a. Fiduciary Duties (owned by each Director):-
    (i) Act bonafide in the best interests of the company as a whole (act in good faith);
    (ii) Exercise care, skill and diligence;
    (iii) Retain their discretionary powers;
    (iv) Exercise the powers for the purpose for which they were conferred;
    (v) Avoid conflict of interest.
b. Statutory Duties:-
    (i) Duty to act in good faith (overall common law duty);
    (ii) Duty to shareholders;
    (iii) Duty to creditors;
    (iv) Duty of care, skill & diligence;
    (v) Duty to exercise power for there proper purpose;
    (vi) Duty to prevent insolvent trading.
c. Duties in relation to Fraud;
d. Duties in relation to Corporation Act;
e. Duties in relation to CLERP 9 (Corporate Law Economic Reform Program Act);
f. Duties in relation to Taxation and revenue laws;
g. Duties in relation to other laws & codes:
    (i) Trade Practice;
    (ii) Consumer credit;
    (iii) Employment law:-
        - equal opportunity
        - harassment;
        - OH&S;
        - Industrial Agreements;
        - Superannuation.
    (iv) Criminal law;
    (v) Environmental laws.
h. General Duty of Care and diligence.

Directors act on behalf of the shareholders and are entrusted with the resources of the Company (Fiduciary Relationship) to act in shareholders interests (these days they have to also consider other stakeholders). As a group Directors are to oversee the affairs of the Company and are responsible for:-

a. Over all governance of the Company; and
b. Monitoring of management and risks.

The legislation recognises that Directors have to delegate how an organisation is managed and operated to the organisations management. Directors need to show they have exercised "Reasonable Care" in establishing direction and applying accountability to ensure the organisation is compliant.

5.3. Role Of Board

The Board has the overall responsibility for Corporate Governance. It sets the strategic direction of the company and the goals for Management. Day to day operations and the administration are delegated by the Board to the Managing Director and his/her Management Team.

The Board reviews the plans of Management, and monitors the performance of Management against those plans in achieving the established goals.

To maintain industry leadership, to grow the Company and to win work with governments, and national and multinational companies, organisations need to demonstrate they have effective systems in place to manage and operate their business and to control the risks within and external to the organisation. They need to demonstrate triple bottom line reporting – social, economic and environmental responsibility.

5.4. Specific Duties / Obligations

Various legislation requires the Chief Executive (that is Directors and anyone who takes part in or has an interest in the management of the organisation) to ensure the organisation is complying with the requirements of the legislation.

For example in Queensland under the Workplace Health & Safety Act the following sections apply:-

a. Section 167 – Ensure Compliance (each individual has obligations).
b. Section 22 – Health & safety has been ensured if individuals are free from the risk of death, injury or illness from the organisations activities.

In New South Wales, the Occupational Health & Safety Act has similar requirements. Section 8 requires the Employer to ensure the health & safety and welfare at work of all their employees as well as ensuring others are not exposed to risk to their health & safety because of the employers undertaking. Section 28 states that if a corporation contravenes, whether by act or omission, any provision of this Act or regulation, each Director and each person concerned in the management of the corporation has contravened the same provision.

In Victoria, the Occupational Health & Safety Act has similar requirements. Part 3 'General Duties', Section 21., requires the employer, in so far as it is reasonable, practicable, to provide and maintain for employees a working environment that is safe and without risks to health. It goes on to spell out in more detail what this involves.

Other states have similar obligations.

5.5. Other Legal Requirements

In assessing the above requirements, many organisations over look other requirements placed on Directors and Management from documents such as:-

a. Contracts;
b. Licences (eg. environmental licence);
c. Insurance policies etc.

5.6. Ensuring Compliance

There are a range of things Directors need to do to ensure compliance and achieve Corporate Governance, however in summary Directors need to:-

a. Establish goals and direction;
b. Understand legal and other requirements;
c. Establish and resource an organisational structure to manage and operate the business;
d. Establish clear responsibilities, authorities and accountabilities;
e. Establish an effective reporting, review, monitoring, audit program (assurance program).

6. PRACTICAL IMPLEMENTATION

6.1. General

When applying compliance, risk, assurance and business continuity, it is critical that it applies to the following areas:-

a. Business, Enterprise, Organisational wide;
b. Each business function:-
   (i) Information Technology;
   (ii) Marketing, business development;
   (iii) Administration & Financial;
   (iv) Human Resources / Personnel;
   (v) Other resources – facilities, plant, material;
   (vi) Operations;
   (vii) Procurement.

c. Each level of the Organisation Structure – Directors, Senior Managers, middle Managers, front line Supervisors, workers;
d. Other stakeholders – Suppliers, Contractors, Government Agencies, Financiers, community etc.

Also need to consider both internal and external sources / influences.

6.2. Planning

The starting point for any business / organisation is establishing direction and purpose of the business. This includes clearly defining goals, objectives, strategies and performance indicators. It involves establishing standards for how the organisation is managed and operated and providing a structure and resources to achieve, maintain and improve. This involves clearly defining, communicating, reviewing and reporting achievement:-

a. Strategic Plan (3 – 5 – 10 yrs forward direction);
b. Business Plan (achieving strategic plan next 1 – 2 yrs);
c. Operational Plan, Resource Plan, Financial Plan etc. (supporting business plan).
d. Objectives, policies and required standard.

The next step is identifying and assessing compliance, risk, assurance and continuity which are directly linked to and are an extension of these plans. These processes address what will stop the organisation achieving these plans.

6.3. Compliance

The second step involves assessing compliance requirements. This involves identifying and assessing all key requirements coming from the organisation, community, Owner, customer, legislation, legal (contracts etc.), insurance policies, Suppliers, Contractors, employee and other requirements directly or indirectly impacting the business.

As part of this process of identifying key requirements from the above areas, the organisation needs to clearly define:-

a. At what level the requirement applies – enterprise wide, Directors, management etc.;
b. How these may or may not impact the business and it's operation;
c. How to manage, achieve requirements and react when requirements are not or potentially not being achieved.

This involves applying the principles and processes defined in AS 3806.

This requires the development of a formal "Compliance Profile / Matrix / Register"

6.4. Risk

The third step following establishing direction and compliance requirements is identifying all existing or potential risks that may impact the business positively or negatively. This involves the identification, assessment, and establishing controls to eliminate / manage / minimise / treat the risks. This involves applying the principles and processes defined in AS/NZS 4360.

This should result in the formal development of a Risk Profile / Matrix for the Organisation and its various arms / sections.

The compliance and risk profiles can be one document or two separate documents, but they must be integrated and linked to and an extension of the Strategic and Business Plan.

6.5 Assurance

The fourth step involves the board establishing an assurance program so that management can give them assurance their plans, objectives, policies are being achieved. This also includes external assurance where required or necessary.

Use HB254 and HB158 as guides for achieving.

6.6 Continuity

The fifth step is ensuring the continuity of the organisation and its resources should the required standard fall.
This step is an extension of the fifth step in the Risk Management Process – Treat Risks. This involves carrying out a Business Impact Analysis (BIA) which identifies and assesses the impact of losing company resources. This involves nine (9) steps (as defined in Australian Standard Handbook HB221:2004)

This should result in the development of a formal Business Continuity Plans and Communication strategy.

6.7 Systems, Resources and Continuous Improvement

The final step is critical and an area that is usually not well carried out or implemented.

a. Development and implementation of Management System, procedures etc. at enterprise, functional and specific areas (AS/NZS ISO 9001, 14001 and AS/NZS 4801 as guides);
b. Provision of resources to achieve required outcome – time, people, material;
c. Establish responsibilities, authority, accountability and reporting;
d. Establish Continuous Improvement through monitoring, review, audit etc.

6.8 Critical Components Throughout

All of the above is under pinned by:-

a. Consultation, communication, involvement, ownership;
b. Systems, processes, project approach;
c. Training, education, competency, information;
d. Flexibility, change, culture.

In addition to the above components being integral to the steps outlined above it is critical that each step is seen as part of a whole and not just stand alone. They all relate to each other. HSW is a critical component of each of the steps outlined.

7 CONCLUSION

To achieve Enterprise Risk Management (ERM), we as professionals need to start talking to Directors, Senior Managers, middles Managers and Frontline Supervisors about establishing a common understanding of the Principles and concepts of the individual components and applying these to achieve an integrated approach rather than separate pieces. Effective risk management is more than financial risks and disaster risks. It is integral to effective planning, governance, compliance, risk and continuity. Risk and compliance are integral in everything an enterprise does. It allows informed decision making and a willingness to take sensible commercial risks. These should be integral to the way an organisation is managed and operated. The resources and business management system should flow from these and the achievement of these should be regularly reviewed and reported on. Health, Safety and Welfare is an integral part of this and we need to start to build it in and applying at this level as well as at the grass roots, design / planning and supplier levels.