

What's in the Crystal Ball for Corporate Governance?

Abstract

The Board of Directors plays a vital role in ensuring compliance and enabling their organization to outperform the competition.

This article investigates the drivers for changes that will occur in corporate governance that Board of Directors needs to be aware of. It provides an overview of the changes in corporate paradigm to manage risk in this electronic age from a viewpoint of current OHS legislation and the affects it has on people, commerce, industry, government and regulators. A strategy for corporations to gain the understanding of their OHS obligations that requires specification, one that the supply chain must provide in order for corporations to comply. Until now, these OHS legal obligations have largely remained "below the radar" and been ignored by corporations and inadvertently exploited by the supply chain. The article explores what is and what is not covered by the OHS guidelines and explains the gaps in Knowledge that place corporations at unacceptable levels of risk. The difficulties of overall compliance require urgent attention by Governments, Regulators, Commerce, Industry and Leaders in business. Knowledge Management and its Control are discussed as a simple solution to corporate governance fit for this electronic age.

Introduction

"Change is the law of life. And those who look only to the past or the present are certain to miss the future."
John F Kennedy. A profound statement, that was true in the 60's and more so in this 21st Century. There is an ongoing knowledge explosion in electronics and over the past 40 years corporations failed to keep up with this rate of change. Current organisational structures, policies and procedures inadvertently contain horizontal and vertical knowledge barriers. These obstacles make it difficult for executives to control continuous disclosure and achieve corporate cultures that are more transparent and, empower the right people throughout the organisation to achieve a corporate competitive management team, top down bottom up.

Current Changes in Corporate Governance – the tip of the iceberg

Regulations have changed from prescriptive to performance-based guidelines. Regulators recognised the knowledge explosion in electronic technology and they introduced guidelines into the Victorian Occupational Health and Safety Act 1985, Code of Practice for PLANT No. 19, 1 July 1995, in the form of an international standard I/C 1508 Functional Safety–Safety Related systems. The International

Electrotechnical Commission (IEC) and Standards Australia (AS) have published this standard as (IEC) AS 61508 Functional Safety of electrical, electronic and programmable electronic safety related systems. It is now the benchmark for overall management system performance. Companies must have a 'State of Knowledge' allowing them to establish a safe workplace, making the obligations universally applicable anywhere in this global market place.

What is good and bad about these guidelines?

This standard is an excellent blueprint that allows corporation to have corporate governance that is fit for this electronic age.

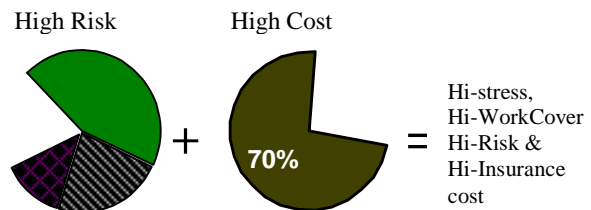
This guideline, like all other hardware software safety related standards anywhere in the world ^[1], provides little or no guidance that would assist corporations to **attain hardware/software integration** or to write a specification to achieve this.

Corporations need to integrate the 'integrated hardware/software' with high performing plant/infrastructure to meet the 'overall' risk management obligations prescribed in the guidelines.

There are many weakest links and at times the links are completely missing. Hardware/software integration is a missing link that is reflected in Safety Standards and recent industrial accidents and corporate collapses.

Failure statistics are the drivers for change

The Advisory Committee on Safety to the International Electrotechnical Commission (IEC) has quantified the risk of failure in each phase of the life cycle. Failure statistics of Instrument and Control systems expose the board of Board of Directors and shareholders to the risk of failure at 44% in the specification phase, 20% in the design/commissioning phase, 13% in the operations phase and a further 23% resulting from changes after commissioning ^[2].



Boards of Board of Directors, worldwide, accept accountability for 80% of failures with very little chance of success in case of accident or litigation. We have the figures that show these statistics are instrumental in cost escalation of 70% above budget ^[5].

These statistics will eventually lead to change, like the changes that are being introduced at present in the light of corporate collapses.

Pre-emptive change will prevent regulators from imposing rules that may inhibit corporate strategies from reaching their full potential. It's like the introduction of IEC 61508 (Functional Safety of electrical, electronic and programmable electronic safety related systems) corporations cannot comply. That is no one's fault; there is no better way of doing it. The missing link is 'business integration planning'.

The role of the Board of Directors in preventing failures

The role of the Board of Directors is to gather intelligence, including obligations below the radar, for the management of the functional safety of the whole infrastructure, its people, procedures and timeframes to enable people to predict future failures.

Once critical information is collated, Board of Directors must alert the Executive management, Audit Committee and other officers charged with responsibility for running the business,

Regulators, by nominating AS 61508 (Functional Safety of electrical, electronic and programmable electronic safety related systems) as a guideline establish new benchmarks for management performance. The standard provides the best guidelines available at present. However experts in the Industry write standards, they use industry jargon and inadvertently introduce knowledge gaps ^[1]. This makes it difficult for people to understand and implement compliant systems. The major difficulty is; people need to know what's missing in the guidelines in order to implement management systems to meet the needs of the guidelines. There are seven major issues that affect corporate governance.

1. The standard changes the paradigm from managing failure to one of proactively managing the consequence of failure – i.e. predicting and preventing. It requires evidence that the political/social, physical, environmental and legal consequences have been considered and how these will be managed. It requires evidence that this is in place for the whole life cycle of the infrastructure. The standard has an impact right across the organisation.
2. This standard changes the way we think about infrastructure. High performing plant/infrastructure, once fitted with an electrical, electronic or programmable control device becomes Equipment Under Control (EUC). It's no longer people, but hardware and software that 'manage' the high performing plant/infrastructure. Replacing people with hardware and software means a change in paradigm in managing those people that carry responsibility for the overall safety of the infrastructure. The standard requires corporations to have people that know how to

manage hardware and software and the new peopleware obligations.

3. The standard makes everyone involved in the decision making process responsible for his or her part in any decision that affect the functional safety of the overall facility. The standard prescribes the human factors that must be considered in the people selection process to prevent future failures.
4. This standard sets a new level of management performance. It prescribes that safety systems must function on demand, whenever that may occur, in the life of the infrastructure. This requires corporations to have 'systems' of management that will allow people to predict failures of high performing plant/infrastructure, hardware/software, people, business procedures and how they interact to ensure the functional safety, from concept to dismantling of an infrastructure.
5. The standard prescribes an independent audit of the functional safety of electrical, electronic and programmable electronic safety related systems be carried out and action taken to correct deficiencies by skilled people.
6. The standard prescribes documentation and record keeping of anything that may influence the functional safety of safety related systems from concept to dismantling and any additions, changes or modifications to the plant/infrastructure, hardware/software, people and procedures.
7. The standard provides guidance for Dependability of hardware and software. IEC 300/ISO 9000-4 (1993). Dependability is the collective term used to describe the availability performance and its influencing factors - reliability, maintainability and maintenance support. Dependability means many things to many, but the bottom line is value for money and meeting customer's expectations on demand.

The guidelines (AS 61508/IEC 300) require measurement of:

- Management system performance
- Combined dependability of hardware/software with the dependability of hi performing plant/infrastructure, people and procedures of a business.

Evidence that the political/social, physical, environmental and legal consequences have been considered and how these will be managed

The Board of Directors needs to address the requirements urgently because:

- **The standard leaves up to the Company's executives to determine how to integrate hardware and software ^[1]. This creates inherent risks in the ability to ensure effective & consistent application of the standards guidance.**

- **Current sophisticated risk assessment techniques fail to detect 67% of failures that remain hidden from operators until the failure occurs** ^[2].

There are huge knowledge gaps and barriers in organisational structures that prevent people from making informed decisions.

Board of Directors are not expected to understand the technical details required by the standard - but they need to know of its existence and its importance for their organisation and to ensure it is implemented.

What does hardware and software integration mean?

Victoria Stavridue ^[1] describes it as follows:

“Integration is a term often misused and misunderstood. The existence of integration as an activity in system development is undeniable. Its existence as a phase of the system lifecycle, which requires planning, and management is, however, **frequently ignored.**”

This omission is undesirable, particularly in critical systems where lack of integration planning may affect the system’s ability to meet its criticality objectives.

Systems integration is the practice of combining the functions of a set of subsystems, be it software, hardware or both, to produce a single, unified system that satisfies some need of an organisation.

Software integration is the practice of assembling a set of software components/subsystems to produce a single, unified software system that supports some need of an organisation.

Integration Testing is a set of procedures designed to verify whether a given assembly of components (be they systems, software or tools) does indeed satisfy the requirements of an organisation.

Not surprisingly, this confusion is reflected in many standards. How do the various critical systems standards deal with integration and, as a corollary, what standardisation activities are needed and **how can organisations relying on software intensive systems for critical functions approach this problem?**”

The IT/Plant management industries fail/cannot achieve this obligation for hardware, software integration.

So how can the Board of Directors approach this problem?

Raise the awareness of the Executive management team (managing electronic safety have moved beyond a single persons knowledge base) of the corollary between the integration of hardware/software and the integration of the high performing plant/infrastructure, people skills and procedures. As well as, the integration of performance measurement methods that can be applied to the overall business. Corporations need ‘integration planning’ as an activity to ensure a

safe workplace and corporate exposure to risk at an agreed as low as reasonably practical (ALARP) level and compliance.

Repeating Victoria’s words and replacing hardware and software with business systems “The existence of integration as an activity in business system development is undeniable. Its existence as a phase of the business system lifecycle, which requires planning, and management is, however, **frequently ignored.**”

To quote an important principle in law – ignorance is no excuse. Such ignorance is highly undesirable, particularly in business critical systems where the lack of integration planning does affect a corporation’s ability to meet its overall risk management objectives.

The purchase of any Custom off the Shelf (COTS) software, be it strategy or tools, perpetuates and reinforces these knowledge gaps which corporations must bridge in order to be competitive. The criticality of business integration planning is highlighted by the news reports about the Columbia Space shuttle disaster. NASA Space Corporation operates sophisticated ‘systems’ and not many are ‘integrated’ with each other. Almost everybody forgets the recording of events in time, because distortions in time have disastrous consequences on the validity of performance measurement/predicting failure. Distortions in time and availability of knowledge on time may well be the case in the Columbia Space Shuttle disaster.

In the mean time there is a dilemma for People, Corporations, Commerce, Industry, Government and Regulators. What should be the next step?

Business cannot stand still. The outside business environment drives the executive team and recent major corporate collapses and industrial accidents demand action, but what action?

Good Governance is critical but discovering good governance is not as simple as it seems ^[3].

The answers lie in Corporate Knowledge Management.

Experts in Knowledge Management ^[4] agree that current management technology is built **upside down**

- a) The IT industry developed information management technology without due consideration of people issues and their intellectual property.
- b) The IT industry **will not** enter into knowledge management until the people issues are resolved.

If that were true than it will never happen, people and technology go hand in glove in this hi-tech electronic age. Corporations have to solve the ‘integration’ problem to suit corporate governance needs. Cost benefits to the IT/PMS industry is a 70% cost escalation per project, making it highly undesirable for the electronics industry to solve the integration problem ^[5]. Corporations need to look for solutions outside the IT/PMS/Electronic industry.

They also agreed that corporations now place a high value on peoples combined knowledge, representing 70% of total corporate value ^[4].

To exploit this knowledge CEO's/Supervisors must know how to access it and how to utilise it.

Much of this knowledge is currently dormant, as is the value of the company.

Every threat presents an opportunity

Its simple: corporations need to solve the people problem, to enable them to make the supply chain deliver its products and services to meet the needs of good corporate governance, and implement management infrastructure that makes knowledge work happen - for the life of the infrastructure.

The 'integration' and 'performance measurement' issues are problems created by the divergence of knowledge in the industrial and electronic age.

Technologies ability to number crunch large volumes of data made it highly desirable to commerce and industry. But technology cannot sort out the people issues.

Leadership not "manager-ship" can sort out the people issue.

Corporations need to change the paradigm from the industrial age and align it with the paradigm of the electronic age.

Corporations need to implement two key elements:

- A language that aligns people with technology (knowing what, where and how to measure to maximise production for the life cycle)
- Business performance measurement architecture, (TIME based overall organisation memory) sensitive to electronic risk management, which aligns people with organisational goals and objectives.

This will enable corporations to 'make it happen' and have effective business knowledge management that achieves overall business risk and performance measurement.

The author identified the following fundamental people issues:

- Sources of information for technical workers:
 - 21% from consulting other people orally
 - 23% from catalogues
 - 29% from files and reports
 - 19% from books and Journals
 - 8% from memorySpend 35% of their time looking for information
- A single word can have multiple meanings therefore, leading to misinterpretation and electronic technology can turn this into a disaster
- Man cannot retain all pertinent information and valuable information can be lost

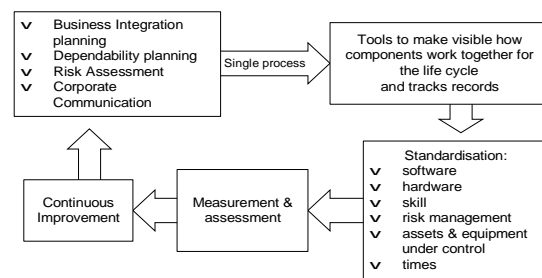
Standardisation of people and technology

To manage the people issues the key word is, 'standardisation'. In this case the language people use to teach technology. Standardisation ensures people can decide what to measure, how to record it and store any information so that it can be found by anyone needing it in real time and be transformed into decision

support material, making full use of the power of the computing technology. The standardised language (naming convention) must align people with technology and facilitate the overall business systems integration. It must also solve the hardware software integration problem of the electronics industry from a corporate perspective of performance measurement, corporate risk reporting and overall compliance. Because compulsory triple bottom-line reporting fails corporations in maintaining the value of its shares. The writer invented new terminology and called it "Business to Plant Reporting (BPR)".

People and their Business to Plant Reporting (BPR)

BPR is a single process that implements the 'Integration and Performance Measurement' obligations of the new guidelines (AS 61508 & IEC 300). It is the framework that allows people to make informed decisions and assess OHS issues in the concept/specification phase before the tender is placed for the design phase. A tool to ensure the supply chain performs as required and eliminates litigation resulting from imported knowledge gaps.



Standardisation is a key benefit of the standardised naming convention. It makes visible areas within the plant and the control systems that lead to a modular design and results in clear functional specifications for software and hardware. Standardisation is also the key in reducing costs in maintaining the overall OHS compliance. "BPR" is the corporate tool that allows people to ensure corporate risk management reporting for continuous disclosure are incorporated in specifications and reduce 'Integration Testing'.

The standardised naming convention is part of the toolkit corporations need to achieve effective knowledge management. To control knowledge, corporations need to realign the paradigm of the industrial age and match the paradigm of the electronic age. Corporations need to invest in or modify existing management infrastructure to facilitate the collection, storage, use and control of knowledge from within, the supply chain (including suppliers, customers specialist advisors, government and regulators) in the right time frame.

There is a need for a Knowledge Management Control System (KMCS). It must be an umbrella that integrates, enhances and safeguards the integrity of all current management systems. Commerce, Industry,

Governments and Regulators have spent significant amounts of money on these Systems. KMCS builds bridges so knowledge and communication can flow across organisational boundaries and human resources all the way up the supply chain and specialist companies. Governments, Regulators, CEO's, Managers and Employees need the assurance that current management systems will improve to meet the challenges of this electronic age.

A KMCS allow Commerce and Industry, Government and Regulators to leapfrog over these problems by making use of the collective memory of all human resources, whom literally hold tens of thousands of little items essential to the performance and dynamics of a particular commerce or industry. Collecting, storing and the availability of life cycle knowledge at the place of use, at the right time, has become essential to be competitive in this global market economy.

A Knowledge Management Control System (KMCS) can be used to forensically analyse installed infrastructure. Corporate Secretaries can quickly and easily establish the worth of a business at times of merger, acquisition, takeover, etc and also identify hidden risk that have not been identified using sophisticated risk assessment techniques.

The above is the tip of the iceberg of what KMCS can do for corporations. People, customer, and procedural risk management has equal importance in the overall risk management obligations required by current overall corporate governance, including the new OHS obligations.

There is an urgent need for governments and regulators to work with the business community and other stakeholders and visa versa. Non executive directors play a vital role in making this happen.

A Knowledge Management Control System = Management from the brain to the balance sheet.

References

- 1) Victoria Stavridou (1997) Integration Standards For Critical Software Intensive Systems, Department of Computer Science, Queen Mary and Westfield College, University of London, Mile End Road, London E1 4NS
E-mail: victoria@dcs.qmw.ac.uk
- 2) R Bell Health and Safety Executive UK / Chairman: IEC/SC65A Working Group 10, - IEC Workshop V, based on 34 incidents (IEC= International Electrotechnical Commission)
- 3) Washington Post, After High-Profile Corporate Busts, Governance Consulting Rooms 17/1/2003
- 4) Gerald W. Ash and Knowledge Management Luminaries, Fred Schoep formerly IBM, Jack Vinson Pharmacia soon Pfizer, Stephen Denning formerly World Bank, Will Hooper Xerox and others - Developing Quality systems in Knowledge Management - Paper presented at QSA Asia Pacific Forum October 2002

- 5) My team and I have worked on 5 of the largest infrastructure projects in Australia over the past 10 years. For three of these we have the facts for financial cost control of the Instrument and control system contracts. Each of these projects had cost escalations of 70% in the electronic systems and 50% of the overall project budget. Litigation caused ongoing dilemmas.