

Proposing the role of

“Governance Director” or “Chief Governance Officer” (CGO)

A white paper by Gary Hinson, CEO of IsecT Ltd.

January 2005

Introduction

In the context of corporate governance, I propose the role of “Governance Director” or “Chief Governance Officer” (CGO) at senior executive level to act as a focal point for issues relating to corporate management control, risk management and ethics. Through this paper explaining the rationale for my position, I intend to stimulate further discussion and development of the concept.

What is “corporate governance”?

In essence, corporate governance is a modern buzzword for old-fashioned management controls. The core aspects of governance include:

- Appropriate management structures i.e. organizational design, including the roles of executive and non-executive directors
- Management control frameworks with clear accountability and responsibility (such as financial and other limits on “delegated authority”)
- Ethics in the business context, and social responsibilities
- Risk management - risks in general including operational, financial, market and IT risks
- Management oversight and independent review - making sure that managers and staff comply with internal and external rules, regulations and laws (e.g. compliance and audit functions)
- Transparency *i.e.* open and honest communications by management to stakeholders about the true internal state and future prospects of the organization

Corporate governance committees

During the past decade or so, reports such as Cadbury, Turnbull, Hampel, Combined Code, Greenbury and Higgs in the UK have stimulated widespread discussion on the subject of corporate governance. The studies were stimulated by major British corporate problems that were thought to be symptomatic of failures in the overall systems of management control.

The reports were written by senior quasi-governmental committees, taking input from a range of commercial, governmental and academic groups in a form of cross-industry benchmarking. Interested groups (such as the professional bodies for auditing and accountancy) were invited to discuss their perspectives on recent management control failures and propose generic improvements. Each study also built on the last.

The committees’ findings primarily relate to large publicly listed limited companies although the underlying principles, if not the full details, are more generally applicable. The recommendations are not formally enshrined in British law but organizations are well advised to comply. This is a similar situation to the London Stock Exchange Listing Rules with which limited companies must comply in order to be listed. Listed companies that break the rules may be de-listed, and any which bend the rules are likely to have problems finding professional advisors such as auditors.

In the United States, the Enron and WorldCom scandals further reinforced the need for widespread governance improvements. America responded by implementing legislation such as Sarbanes-Oxley and Gramm-Leach-Bliley, imposing new legal obligations on corporate management. Directors who fail to uphold the principles of good corporate governance now face imprisonment. Suddenly, corporate governance is on the agenda, big time.

Other guidance on corporate governance

The corporate governance debate is far from over. Every time there is a major accounting or banking scandal, governance goes straight back on the corporate agenda. Governmental bodies and industry regulators are constantly re-working the reporting rules (e.g. a Department of Trade and Industry proposal to mandate the inclusion of Operating and Financial Reviews in annual company reports in order to improve transparency, is currently open for public comment). Various academics and accounting and audit professional bodies are actively researching, developing and issuing governance guidelines and standards.

COSO (The Committee of the Sponsoring Organizations of the Treadway Commission) was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent American private sector initiative. The commission was sponsored by five major financial professional associations in the United States: the American Accounting Association, the American Institute of Certified Public Accountants, the Financial Executives Institute, the Institute of Internal Auditors and the National Association of Accountants (now the Institute of Management Accountants). COSO's 200-page Enterprise Risk Management Framework, now available in draft, is due for publication shortly. It includes recommendations for corporations, regulatory bodies and the education system. The initial chapter on fraudulent financial reporting is an excellent introduction to the problem underlying this paper.

Who *should* be responsible for governance?

It could be argued that governance is 'everyone's responsibility' but in practice governance is a crucial part of the role of certain corporate support functions including internal audit, physical site security, information security, risk management, compliance, health and safety and legal. Governance characterises and unifies these functions whilst differentiating them from other corporate support functions such as IT, finance, marketing and human resources for whom governance is merely a side issue.

The governance functions have common interests in corporate policies and compliance, and benefit from being independent of the routine operational functions. They are also functions that, in my experience, rarely find a happy home elsewhere in the conventional organization/management structure. Some would consider them the perennial corporate misfits, although personally I prefer the term 'internal consultants'!

I firmly believe there is a strong case for a new executive management role of "Governance Director" or "CGO", supplementing and enhancing the non-executive and executive directors and senior managers with the greatest influence on corporate governance.

In my personal view, the single step of establishing the role of Governance Director/CGO would solve common organizational design problems such as:

- To whom should [semi-]independent internal control and review functions report?
- How can discrete governance activities be aligned across the organization?
- Who should take the lead on the subject of ethics?
- How should the executive and non-executive directors interact?
- [Last but not least] Who should be held accountable for corporate governance?

A major advantage of aligning these functions under a governance directorate or department is that, in effect, you create a centre of excellence for governance-related skills and competencies.

Forming a critical mass of people whose primary focus is governance leads to interesting opportunities for cooperation on research and development of governance concepts. With appropriate senior management direction, they will become governance evangelists, spreading the good word about the beneficial value of sound management controls throughout the business at large.

I therefore propose the following role description:

Governance Director/CGO role

The Governance Director/CGO is an executive board position with overall accountability for the organization's corporate governance activities. This role does not release other directors, managers and staff from their individual governance responsibilities but acts as a co-ordination, alignment and strategic leadership function.

The Governance Director/CGO's primary responsibilities are as follows:

- Proactive leadership and strategic direction for all matters relating to corporate governance, including related policies, implementation or improvement plans and measurement
- High-level co-ordination of governance, risk management and related control activities throughout the organization, including systematic governance improvements as necessary
- Promoting the value-enhancing aspects of sound corporate governance as well as compliance with the policies, rules, regulations and laws
- Line responsibility for the primary governance functions such as internal audit, physical site security, information security, risk management, compliance, health and safety, legal and so forth
- Liaison with non-executive directors (via the Senior Independent Director or equivalent)
- Secondary responsibilities include:
 - Being the focal point to lead discussion and make corporate decisions on serious ethical issues, governance-related policies and other governance matters
 - Offering advice to other directors and senior managers on governance and management control matters
 - "Dotted line" responsibilities for managers in charge of important governance and control activities such as annual financial reporting, due diligence etc.
 - Liaison with external regulators *etc.* on governance and control matters
 - Creation of a "whistleblowers' charter" and the corresponding mechanism for confidential internal reporting of frauds, impropriety, internal control failures and similar governance breaches

Governance in relation to IT

Some commentators focus on the governance role of information security. The US National Cyber Security Partnership's paper "Information Security Governance - a Call for Action" for instance states that "Although information security is often viewed as a technical issue, it is also a governance challenge that involves risk management, reporting and accountability. As such, it requires the active engagement of executive management." The paper takes a bottom-up approach linking information security to corporate governance.

I personally prefer to consider governance in a broader top-down sense as an all-encompassing framework of management and technical controls for an organisation. Thinking specifically in terms of IT, for example, governance includes but extends well beyond management of the IT department. IT is a major function in many organizations with a significant budget. IT is used and has impacts throughout the organization and indeed through business relationships to suppliers, partners and customers. IT governance is therefore both a business and a technology issue. Given the penetration of IT into the business, IT governance is also a major part of overall corporate governance in most modern organisations.

I am surely not the only one who thinks this way. In a letter published in September 2003's issue of Director, the Institute of Director's journal, Julian Brackley of Niku Corporation UK said that "The updated Combined Code on corporate governance will force thousands of businesses to undertake a review of the way IT is managed ... Companies will have to apply a similar level of governance to IT as they would to the finance function."

Here are five key aspects of IT governance that I believe would be of direct interest to a Governance Director/CGO:

1. **Conventional management control within the IT department** - the Governance Director/CGO would not have a hands-on executive role (that's the IT manager's job) but would be responsible for sharing best management practices amongst all departmental managers e.g. budgeting and forecasting and expenditure tracking; HR management; supply and demand management (capacity planning, service levels etc.).
2. **Project management** - technology projects are notoriously risky yet the established principles of good practice in project management are seldom fully applied. For instance, we were horrified but not entirely surprised to find that less than half of IT projects surveyed by Computer Weekly even have a documented business case.
3. **Change management** - most new or changed IT systems and services are presumably implemented to improve the organization in some way, yet conventional change management concepts are usually notable by their absence. As a simple example, project communications, if they are managed at all, are typically internally-focused within the project team and/or IT: rarely have we seen truly customer-focused project teams that communicate effectively with the rest of the organization and make any real effort to smooth the implementation, except perhaps for a token effort to "train the users". Is it any surprise, then, that system implementations are often resented and sometimes rejected by the very users whose lives were supposed to be improved by the new systems?! Users don't behave like performing dogs!
4. **Information security management** - whilst traditional IT security functions have tended to focus on technical security controls within the systems and networks, the remit of modern information security extends throughout the organization and beyond. Proactive management of information security risks and controls requires someone to integrate general user and management activities with those inside IT, and to help coordinate HR, physical security, IT/network operations, marketing and procurement functions.
5. **IT risk management** - we have already touched on the need to improve management of risks in projects and information security, but risk management techniques have broader application. Effective contingency planning, for example, requires coordinated effort across the organization.

Benefits of Board-level representation

It is often said that the most critical success factor for major strategies, projects and initiatives is solid senior management support, and with very good reason. The management hierarchy of a typical organisation invests a great deal of power and influence in senior management, just as a football team looks to its captain and coach for leadership direction, motivation and support. Something proposed and/or strongly championed from the top has an uncanny way of coming to fruition. Conversely, if senior managers do not actively support something, or worse still if they oppose it, they have many ways to influence the outcome negatively through what is known colloquially as 'company politics'.

I feel strongly that the same is true of corporate governance. Senior management support for governance is an essential component of success. This is the key reason that I am proposing a Board-level management focus for governance, but not the only one. Here are some others:

- Of course I believe in the strength of the cost-benefit case for governance of control frameworks as a whole. Strong controls increase alignment of the organisation's various parts with its central strategic objectives, and reduce risks relating to noncompliance with all sorts of policies, rules, regulations and laws. This is essentially an argument for quality assurance in relation to management processes. Solid governance controls allow the organisation to go into risky situations with greater confidence;
- Ethical standards of the top team influence the entire organisation. Their tacit or explicit acceptance of unethical policies and working practices can easily lead junior managers and staff astray. Another way to express this is 'cultural leadership';
- Governance has become a more complex issue of late. Sarbanes-Oxley, for example, includes specific, narrowly defined legal requirements that could easily be missed or misinterpreted through ignorance, yet precious few senior managers have the time or inclination really to get to grips with their governance responsibilities. The Institute of Directors, for one, has consistently bemoaned the lack of management qualifications or training to support senior managers as they step up to the Board;
- With a clear focal point driving from the top, governance is more likely to be defined and applied consistently across the corporation. Distributed piecemeal governance initiatives are unlikely to be as effective, especially in the face of competing demands for limited resources;
- There are tangible costs involved in designing and operating a sound governance framework, albeit offset by rather intangible business benefits. In a typical corporate environment, these costs must be justified relative to other investments in order to secure sufficient budget;
- Other managers and staff who become aware of governance failures in the organisation will have more confidence in reporting the matter internally to a senior person for whom governance is their entire *raison d'être*;
- Board-level appointments are publicised as a matter of course, presenting an ideal opportunity to nail the corporation's colours to the mast. Appointing a Governance Director/CGO sends a clear message to the outside world as well as to the organisation itself about the importance attached to governance. This is a positive sign for corporate stakeholders who are increasingly concerned about governance of their investments, in other words it should theoretically improve the share price.

Conclusion

In summary, I believe there is more than enough governance-related work to be done in any large organization to justify the full-time leadership position of Governance Director/CGO (or perhaps "The Governor"!), especially with today's increased focus on this issue. At least one organisation (Sympatico, the consumer Internet services division of Bell Canada) has appointed a CGO. How about yours?

References

This small selection of governance-related references is presented in reverse chronological sequence. The European Corporate Governance Institute (ecgi) website gives access to scanned or uploaded copies of most of these plus other related reports. They are also hyperlinked from the online version of this paper at <http://www.isect.com/html/governance.html>:

COSO Enterprise Risk Management Framework Latest draft publication from the Treadway Commission, due for final publication in Summer 2004.

Information Security Governance - a Call for Action Paper by the National Cyber Security Partnership. April 2004.

Revised Combined Code Updated to reflect Higgs, Smith *etc.* July 2003.

Tyson report Recruitment and Development of Non-Executive Directors. At the invitation of the UK Department of Trade and Industry, Laura D'Andrea Tyson (Dean of the London Business School) led this study. June 2003.

Higgs report Review of the role and effectiveness of non-executive directors. Committee chaired by Derek Higgs. Department of Trade and Industry (DTI). January 2003.

Smith report on Audit committees - Combined Code guidance. Committee chaired by Sir Robert Smith. Financial Reporting Council (FRC). January 2003. The committee report is included within the Revised Combined Code.

The Combined Code Principles of good governance and code of best practice. Derived by the Committee on Corporate Governance from the Committee's Final Report and from the Cadbury and Greenbury Reports. May 2000. (Updated in 2003 - see above)

Turnbull report Internal control; guidance for directors on the Combined Code. Committee chaired by Nigel Turnbull. Institute of Chartered Accountants in England and Wales (ICAEW). September 1999.

Hampel report Final report of a committee on corporate governance chaired by Ronnie Hampel. January 1998.

Greenbury report Study group on directors' remuneration set up by the Confederation of British Industry (CBI). July 1995.

Cadbury report Committee on the financial aspects of corporate governance, chaired by Adrian Cadbury. December 1992.

Appendix: Isect Ltd's consultancy services relating to governance

Our interest in governance stems from our practical experience of information security controls coupled with an enduring interest in management.

Every modern organization depends critically on high-quality and reliable information, with virtually all using IT systems to collect, process and disseminate information. Managers receive huge amounts of information from, and issue reams of decisions and instructions to, the workforce using computers and various communication systems. Securing (i.e. ensuring confidentiality, integrity and availability of) those information systems and data is extremely important, but so too is the design of appropriate information flows and systems. In many ways, modern management is as much about systems engineering as it is about traditional direction and control.

Our consultancy services all fall within the scope of governance with a particular focus on governance within IT. At a broader level, we can also help clients review and improve governance as a whole, and ensure that governance within the IT context blends seamlessly with and supports overall corporate governance.

For more information on the issues raised this paper, or for advice on our IT governance consultancy services, please visit www.isect.com or contact Gary Hinson by emailing gary@isect.com or telephoning +44 1428 727 900.