

Effective Direction of Compliance from the Board—A Director’s Survival Guide

Peter D Whyntie

abstract

This article was developed as a short guide for directors to optimise boards’ effectiveness in providing direction in the increasingly complex compliance environment. Whilst the literature devoted to practical compliance management at the compliance and operational management levels is voluminous, there has been relatively little practical advice aimed specifically at directors. However, the experience of the author, both as compliance professional and a director, is that unless directors take a strong leadership role and develop appropriate expertise, the compliance culture in a company is unlikely to be effective.

This paper will provide some practical guidance on how boards can establish the structure and methodologies to better discharge their compliance governance duties and to promote a strong and effective compliance culture. Whilst this article will not deal specifically with operational risk management, it is acknowledged that compliance is increasingly being seen as an element of risk management. Indeed, many companies now include compliance as a risk category. Readers are therefore asked to consider, as they progress through this article, how their company might ensure that the related disciplines of compliance and risk management are coordinated to maximise the synergies between the two.

The screws for directors are tightening

Through changes to law and decisions of the courts the focus of directors over recent years has increasingly been directed towards compliance. Parker and Conolly (2002, p 276) found an increasing shift, both in explicit law and through the courts, towards directors being expected to exercise their duties in respect of effective compliance: ‘In Australia, after the AWA appeal and CLERP reforms to duties of delegation and the business judgement rule, directors arguably have a basic duty to monitor both business performance and compliance with law and corporate policy.’

In the financial services industry there have been legal requirements for responsible entities (REs) of managed

investment schemes and Australian Financial Services licensees (AFSLs) to have documented compliance plans. REs are required to either have a majority of independent external directors to take responsibility for compliance or to appoint an external compliance committee. AFSLs are required to notify the Australian Securities and Investments Commission (ASIC) of any significant breach or potential breach of a relevant financial services law within five business days of its discovery.

The move by various state governments to introduce criminal sanctions for deaths and serious injuries in the workplace also highlights the increasing focus on directors’ duties in respect of compliance.

A recent update from Mallesons Stephen Jaques (Bednall, 2006) looked at the recent examples of non-executive directors stepping in when crises overcame the CEOs of James Hardie and Amcor, and also a number of other prominent corporate crises involving allegations of unlawful behaviour. The update makes the general point that a key message from these examples is ‘that legal compliance, as part of the oversight of risk management generally, is the remit of the board rather than management’. In reviewing the ASIC case against the One.Tel Chairman, it goes on to note that ‘...directors should now assume that they have an obligation to establish and monitor the compliance system, and ensure that it is operating effectively on a regular basis’.

Compliance duties may even arise from seemingly obscure directions. A Freehills' update (McEniery, McCullagh and Fernon, 2002) explores the potential for the court to apply the duty to exercise care and diligence to a director that failed to take reasonable steps to ensure that reasonable e-security policies and practices are in place in a corporation operating in an online environment. It finds that directors '...may be in breach of their duties in any of the [various situations arising from breaches of e-commerce provisions] if the company does not have proper IT security'.

Some help at hand—AS3806–2006

The Australian Standard for Compliance Programs AS3806–2006 (the Standard) is emerging as the standard by which a number of regulators are measuring whether companies they regulate have effective compliance frameworks. The ACCC pioneered the concept of making the implementation of a compliance program subject to an enforceable undertaking. The Standard was developed partly at the instigation of the ACCC, which was seeking to have greater consistency in compliance programs. The 2006 version, which replaced the 1998 version, has addressed shortcomings perceived in the earlier version, especially in respect of measurable outcomes.

The new version places greater emphasis on controls to manage identified compliance obligations and on monitoring, measurement and reporting of performance of the compliance program than did its predecessor.

Both ASIC and the Australian Competition and Consumer Commission have been public supporters of the Standard. ASIC makes reference to the Standard in its licensing guidelines to Australian Financial Services (AFS) Licensees. The ACCC has developed standard trade practices compliance program templates for their enforceable undertakings that closely follow the principles set out in the Standard.

The Standard is a document with which any director, charged with the responsibilities of overseeing the corporation's compliance, should be encouraged to become familiar. The Standard makes several references to the function of the board, which it terms 'governing body' (given that the Standard is for use widely not merely by companies).

A board should be encouraged to formally adopt the Standard. That would send a clear message to top management that compliance is not only important but that it will be subject to clearly specified and measurable requirements.

The Standard is built on twelve Compliance Principles grouped under four headings: commitment, implementation, monitoring and measurement, and continual improvement. The board is the primary body

responsible for Principle 1: commitment. On that issue, the Standard states '[T]he governing body, chief executive and all levels of management actively demonstrate commitment to designing, developing, implementing, maintaining and improving an effective compliance program.' (p 8)

Under Principle 6 (p 12) (which clearly articulates and assigns responsibility for compliant outcomes), it states that '[F]or a compliance program to be effective the governing body and top management need to lead by example, both by adhering to and actively supporting compliance and by being seen to adhere to and actively support, the compliance program.'

Under Principle 10 (p 21) (performance of the compliance program is monitored, measured and reported), it states that '[T]he governing body, top management and the compliance manager should ensure that they are adequately informed on all relevant compliance failures and actively promote the principle that the organisation encourages and supports a culture of full and frank reporting.'

The strategically placed references to the 'governing body' in the Standard place emphasis upon the role of directors at the points where they can maximise their position in the organisation. It is also important to note that at each point of reference to the governing body, the word 'actively' appears. This is no accident. Unless the directors are active in exercising their oversight of compliance it is less likely that top management, and in turn middle management and employees, will view it as a matter of primary importance to the company.

Role of the board and some practical governance structures

The optimal structure that a board adopts to oversee compliance will be dependent upon a number of considerations. These will include the complexity of the legal environment in which it operates, the size of the board and the number of available directors, the model provided by other similar sized companies in its particular industry or market sector, the relative maturity of its governance functions, and its compliance history.

Generally companies will follow one of three models. They are that the board will discharge its compliance oversight role directly, it will delegate to a board committee, or it will appoint an independent compliance committee.

Direct oversight

A board may decide to address compliance directly without resort to a committee. The reality is that in very small entities with limited governance resources and small numbers of directors, the creation of board committees may not be practicable.

It is important for directors in that situation to ensure that the board is able to properly address compliance matters and be able to demonstrate that material issues are given appropriate consideration. The level of expertise that directors need to fully understand and address compliance should be a consideration in selecting directors. The meeting agendas should allow for sufficient time for compliance to be considered, and the level of formal reporting on compliance matters should be commensurate with the significance of the compliance risk to the company and its operations.

Board committee

In today's complex regulatory environment even many small private companies are moving to adopt a formal governance structure involving board committees.

Where a board chooses to delegate compliance oversight to a board committee, it can be to the audit committee or to a special committee established for the purpose. In the financial services industry, that tends to be either a dedicated compliance committee or a risk and compliance committee. Outside of financial services the norm is still for the audit committee to oversee risk management and compliance, although there is a trend emerging of establishment of risk management committees that also oversee compliance.

There is nothing intrinsically wrong with making the audit committee responsible for overseeing compliance. However, the important consideration should be whether the focus of an audit committee might be so directed to the financial risk management of the entity that it is a less effective forum for reviewing the often diverse and complex issues raised in the compliance context. Increasingly boards are looking for some specific compliance skills and experience to be represented on the board. These might be better deployed on a committee that can focus on reviewing compliance (and perhaps also operational risk management) issues rather than one that also addresses audit and financial risk management.

Where compliance is to be the responsibility of the audit committee, boards would be well advised to ensure two aspects are addressed. The first is to ensure there is an appropriate level of compliance skill and experience within the mix of directors on the committee. With the increased complexity of compliance management that might be a director with specific experience in managing or consulting on compliance and risk management.

The second is to ensure that the audit committee agenda

gives sufficient time to the serious consideration of compliance matters. That should not be restricted to the receipt of a compliance report, but should extend to wider considerations such as regular presentations from industry specialists, updates on legislative and regulatory matters and attendance by management with operational responsibility for implementing compliant systems and processes.

The advantage of utilising a compliance, or a risk and compliance, committee is that it is relatively easier to keep the focus directed on the compliance function. Even where the actual committee membership is identical or substantially in common with that of the audit committee, anecdotal evidence suggests that the quality of consideration of compliance matters can be higher and more focused when the committee is not distracted by non-compliance matters.

... 'that legal compliance, as part of the oversight of risk management generally, is the remit of the board rather than management'.

Independent compliance committee

The independent compliance committee model was developed specifically for REs operating managed investment schemes. REs operating in the highly prescriptive financial services sector have to satisfy very stringent independence rules in respect to directors performing compliance functions and members of the statutory independent compliance committee. However it is a model that has had some attraction for financial services companies other than REs. This has been the case for a number of financial adviser and dealer groups where the boards have not had sufficient non-executive directors and/or the relevant compliance expertise among the directors to appropriately address the volume and complexity of matters requiring their attention.

In these instances, the companies have appointed a compliance committee of external compliance specialists (usually drawn from a legal or compliance consulting practice) or created a committee of directors and external or management compliance specialists. It should be noted in this model that the committee is not a committee of the board, and its role is to review the management of compliance, to review compliance issues, and to report and make recommendations to the board.

The responsibility for compliance remains with the board. It is important to note that the board still needs to give

visible attention to addressing the independent compliance committee's report, including consideration of its recommendations and assessing its performance. It would be dangerous for the directors to assume that the independent compliance committee is responsible and to merely 'rubber stamp' its reports. The board would be well advised to have compliance as a standing agenda item, address the independent compliance committee reports, and to invite the Chairman of the independent compliance committee, if not already a director present, to attend board meetings to discuss the report. The board should also hold regular discussions with the Compliance Officer.

Clear charter

The Charter, whether for the board or a committee, is a key component of the governance structure for effective compliance. A scan of charters made publicly available by a range of companies shows significant variations. Arguably many are too brief to provide sufficient guidance as to what directors are expected to be responsible for. It is difficult to see how these boards could claim an effective due diligence defence in the event of a serious compliance breach being examined by a court.

An example from one SME is two paragraphs that effectively state that the Audit, Compliance and Corporate Governance Committee reviews the Company's policies and procedures for compliance with [a range of obligations] and ensures the independence of the external auditors. It also monitors corporate risk management, internal control and compliance.

It is difficult to see how these boards could claim an effective due diligence defence in the event of a serious compliance breach being examined by a court.

Another, this time from a substantial public company that professes in the Charter's introduction to '... actively pursue[s] best practice governance to remain amongst the top Australian companies in applied corporate governance', is totally silent on compliance other than a brief reference to trade practices and environmental acts under a section titled 'The Role of Individual Directors', and a line '[P]olicies relating to the corporate code of conduct as well as procedural compliance' under the section 'Human Resource and Workplace Health and Safety'.

A very good example is that of the HCF Life Compliance Committee Charter (2005). That clearly outlines the Committee membership and the independence requirements for its members, including that the Chair may not be the Chairman of the Board nor the Chairman of the Audit Committee. The purpose is clear and includes the Committee's powers to investigate many matters brought to its attention, full access to 'all books, records, facilities, and personnel of the company' and powers to engage independent counsel and advisers. It retains the responsibility for appointing the Compliance Officer. It details the frequency and purpose of meetings, being to:

1. Review and note the Compliance Officer's report;
2. monitor the effectiveness of the company's compliance program including staff training;
3. confirm whether any significant compliance breaches have occurred and ensure those identified, if any, are promptly rectified;
4. identify new or changed regulatory obligations;
5. allocate appropriate resources to ensure compliance obligations are consistently met;
6. review and note complaints made to the Life Insurance Complaints Service; and
7. evaluate the composition and effectiveness of the Committee.

The Charter provides for the Committee to meet in private session at least once a year to evaluate the Compliance Officer's effectiveness. It then goes on to detail its duties and responsibilities including oversight, appointment of the Compliance Officer and communications with stakeholders.

The Zurich Financial Services Australia Limited Risk & Compliance Committee Charter (2006), in addition to being broadly consistent with that of HCF Life, details specific management reports required and includes the following statement providing for independent reporting to it by certain key appointments:

The persons with the position of General Counsel, Head of Internal Audit and Head of Risk Management and Compliance (or equivalent functional positions) shall have direct, unfettered and confidential access to the Committee to raise issues of a corporate governance, compliance, risk management or internal audit nature.

The Committee has authority, within the scope of its responsibilities, to seek any information it requires from any employee or external party.

It is also important that the Charter is clear about any limitations on the scope of its compliance responsibilities. It may be that the board wishes to limit the compliance scope to certain areas. It is not uncommon for the independent compliance committees of managed investments schemes REs to be limited to only financial services laws. However, if a committee is to be limited in its scope, it is important the board is cognisant of the fact that it has responsibility for every law that may impact the entity. Many boards would be surprised to discover how long that list of laws can be. If it has limited the charter of a committee, it needs to ensure that it has a board charter to cover all the other laws that are outside the scope of its specialist compliance committee.

Agenda

The agenda should reflect the Charter. The Chairman is well advised to establish with the Company Secretary what the agenda should incorporate. Whether compliance is considered as part of an overall business agenda, or as a specific meeting, it should allow for matters arising from previous meetings (with updates provided by responsible management), appropriate reports including the Compliance Officer's Report, reports on compliance aspects of complaints management, emerging issues and legislative changes that will impact the entity, and any other matters that the board considers to be relevant.

One company has found it useful to split its meetings into alternate General Reporting Meetings and Special Matters Meetings. It allows the General Reporting Meeting to focus on the formal reporting that the Compliance Committee requires to provide proper governance oversight. The Special Matters Meeting then can be limited to a small number of items such as presentations from line managers on how they implement compliance in their area of operational accountability, presentations from internal or external specialists on matters of interest (for example, research reports, emerging issues, new legislation, etc.), and any other matters outside of the normal formal reporting agenda. The directors of this company have found that allows them to devote time to broad thinking and consideration of wide ranging issues that would be difficult in the more cramped agenda of the formal reporting meeting.

Where compliance is to be considered in the normal board agenda, or at the audit committee, it is important that the agenda still reflect sufficient time and weight of thought to the compliance function. For instance it may not be sensible to always place compliance at the end of the agenda, where it will more than likely either be deferred or be rushed through with insufficient time to

give full and proper consideration to the matters tabled. With regard to the Standard, it is unlikely that the board could be seen to be fulfilling its obligations in such circumstances.

Compliance report

It has been the author's experience that boards often are uncertain as to what the Compliance Officer should be reporting. In turn, Compliance Officers are seeking a lead from their board as to what directors view as important to enable them to provide proper oversight and guidance to management and the Compliance Officer.

There is no one size fits all solution to this. One practical piece of advice is that the board and its Compliance Officer develop an open dialogue that will allow both to freely exchange ideas that can lead to the Report evolving over time. The author ensured that he frequently invited his boards/compliance committees to comment on the structure and content of his reports and sought their ideas to improve it.

It is important to have an appropriate mix of information that both informs the board of the current state of health of the company and forecasts operational, legislative and environmental changes that will need to be managed. Ideally the report will include dashboard equivalent reporting of compliance incidents and breaches, complaints management, training, and other lead and lag indicators.

An experienced Compliance Officer will seek the board's approval of a breach reporting policy and procedure that would include a risk based breach evaluation and reporting table that will ensure a structured escalation process. The board might want to receive statistical information on all incidents/breaches (risk rated low, medium and high) whilst only receiving the details of high risk incidents/breaches.

Other standard report items might include regulator actions involving the company, regulator actions in the industry with relevance to the company's field of operations, projected regulatory changes that will impact on the company, summary of subsidiaries' compliance reports, compliance involvement in significant business projects, results of compliance reviews conducted, compliance with relevant industry codes/standards, compliance matters arising from internal or external audit reports, etc.

Business planning

If compliance is to be seen to be important, to be an integral part of the business, and to have credible implementation, it is important that the board impose the same disciplines upon compliance management as it would on any other part of the business.

The Compliance Officer should be required to develop a rigorous compliance business plan, with budget, clearly stated and measurable deliverables, timelines, and allocated responsibilities. The plan should detail how and when the plan will be reported on to the board, and include the agreed key performance indicators (KPIs) by which its effectiveness is to be measured.

The benefits of such an approach to the Compliance Officer will be to increase his/her credibility with the senior management team. It will assist the Compliance Officer in obtaining the appropriate resourcing, and enable the compliance function to receive proper recognition for the delivery of an effective compliance culture.

The board can also assist the Compliance Officer in the goal of fully embedding compliance if it insists that management's business proposals put to the board include statements of compliance risk and of how management will deal with them.

Independent reviews/audits of the compliance framework

The board should seek independent evaluation of the effectiveness of the compliance framework and culture from time to time. The Compliance Officer is naturally conflicted in carrying out such an assessment him/herself. That is not to say that there is not useful compliance self diagnosis that the compliance function can conduct. However an appropriate level of independent review is an important governance requirement. This is also being mandated by an increasing number of laws and regulator standards.

Formal audits can be conducted by both internal and external auditors. Increasingly, boards are seeking independent reviews to be conducted by the specialist compliance advice services offered both by the larger firms and niche specialists. They might be on a targeted basis on a regular schedule, say annually. If the Compliance Officer has a program of regular self diagnosis that utilises objective methodology it may be sufficient to seek an independent review on a less frequent basis, say every three years.

Times of significant corporate change, such as major restructuring, mergers/acquisitions, or entry into new business areas, can also be useful triggers for the conduct of an independent review.

These reviews should be seen as a validation of the Compliance Officer's efforts and an opportunity to benefit from a fresh set of eyes rather than as a threat to their perceived credibility or effectiveness. It is important that the board is actively engaged in the selection and appointment of the reviewer, the agreement of the

scope, and the consideration of the output, especially where it is to be a comprehensive exercise.

Conclusion

Directors are facing increasing demands in respect of time, personal liability, experience and knowledge. The obligations for compliance oversight are expanding and becoming more and more complex. The risks of failure are serious and far reaching.

Equally the rewards to a company and its stakeholders of putting in place and maintaining a best practice compliance framework and culture are substantial. They include satisfied customers and suppliers through quality of output, certainty and transparency in client and supplier relations, confident dealings with regulators, protection of the bottom line through reduction of costly breaches, and higher employee morale.

To take a company to that plane of compliance excellence requires first and foremost that the board has a highly visible commitment and provides strong leadership. When management knows that the board places primary importance on an effective and fully embedded compliance culture, and equally appreciates that the board is driven to assist that happening in as practical and unobtrusive way as possible, there is likely to be strong and positive cooperation between both parties.

This guide will assist directors in setting the board agenda, considering the appropriate governance structure, providing guidance to the Compliance Officer, ensuring the appropriate level of resourcing, and giving leadership to management in implementing a strong culture of compliance.❖

References

- Bednall T, 2006, 'Managing Reputational Risk: Are NEDs the Gatekeepers?', Mallesons Stephen Jaques update (April).
- McEnery M, McCullagh A & Fernon M, 2002, 'Board Responsibility for Protecting Information Assets', Freehills update (September).
- Parker C Conolly O, 2002, 'Is there a Duty to Implement a Corporate Compliance System in Australian Law?', *Australian Business Law Review*, vol 30.
- The Hospitals Contribution Fund of Australia Limited, 2005, 'HCF Life Compliance Committee Charter' (February).
- Zurich Financial Services Australia Limited, 2006, 'Risk & Compliance Committee Charter' (October).