MESSAGE

To: consult/SFC@SFC CEOO Ext :
cc: "Naomi Burley" <Naomi.Burley@compliance.org.au> Ext :

From: "Martin Tolar" <Martin.Tolar@compliance.org.au>
Date: 24/12/2009 08:40 AM

Subject: ACI Submission

Please find attached a copy of the ACI submission.

Please note that due to copyright issues we have included one of the attachments to our submission as an attachment to this email rather than an attachment within the submission itself. It should be read in conjunction with our submission.

Regards,

Martin Tolar
Chief Executive Officer
Australasian Compliance Institute
ACI – Supporting you, your organisation, your profession
Australasian Compliance Institute Inc. ABN 42 862 119 377 I www.compliance.org.au
Level 1, 50 Clarence Street, Sydney NSW 2000 I GPO Box 4117, Sydney NSW 2001 I **Ph 02 9290 1788 I Fax** 02 9262 3311
ACI is proud of the support of our Principal Members: Westpac, PricewaterhouseCoopers, Ernst & Young, National Australia Bank, AMP, ANZ, IAG, Commonwealth Bank

Proposals to Enhance Protection for the Investing PublicV3 (2).pdf ACI3806-2006.pdf

Australasian
Compliance
Institute

24 December 2009

Principal Members

Westpac

PricewaterhouseCoopers

Ernst & Young
Quality In Everything We Do

nab

ANZ

AMP

CommonwealthBank

Securities and Futures Commission
8th Floor
Charter House
8 Connaught Rd
Central
Hong Kong

Via email: consult@sfc.hk

Proposals to Enhance Protection of the Investing Public

The Australasian Compliance Institute (ACI) would like to take the opportunity to thank the Securities and Futures Commission (SFC) for providing an opportunity for ACI to make a submission and comment upon its Proposals to Enhance Protection of the Investing Public.

ACI is the peak industry body for the practice of compliance in Australasia. Our members are compliance, risk and governance professionals actively engaged in the private, professional services and Government sectors within Australia, New Zealand, Hong Kong Singapore, Thailand and Indonesia.

ACI is supportive of the approach proposed by the SFE to help enhance consumer protection while also shoring up investor confidence in Hong Kong's investment markets and securities products. ACI would like to provide this submission to contribute to the measures the SFE will be putting place. There are a few points of clarification ACI would seek from the SFE as well as comments it would like to make in respect to the proposals put forward by the SFE.

ACI understand the value of Principles based regulation, especially in a market where there are international participants and organisations of various sizes. However, as there has not been a long history of this approach in Hong Kong, compared to rules based legislation, we would suggest that the market will need a number of support measures in order to assist them to meet the expectations of the regulator. Even in a market that is familiar with a principals based approach, the majority of regulators find it necessary to use of such devices as Regulatory Guides (RGs) or soft law on specific parts of the new requirements that need clarification by industry. These help establish the expectations of the regulator clearly, can provide examples of the approach to compliance desired by the regulator and allow stronger wording

around specific requirements that can be easily updated by the regulator as the market evolves. This gives certainty to organisations; assists the regulator in achieving its objectives and gives confidence to investors as well as quite specific protections where required.

In addition, ACI would recommend that the new regulatory reforms be accompanied with an extensive education campaign to ensure that industry are fully informed and understand the SFE's requirements in terms of compliance, reporting and breach management and how the SFE intends to enforce the new regime. ACI also believes that there may be benefit in the SFE giving consideration now as to how they intend the compliance frameworks that will be created in response to the new regulations to be reviewed for effectiveness. It is on this basis that we attach a copy of our review protocols to this submission.

We have also included references in this submission to an existing Standard for Compliance. It is currently and Australian/New Zealand Standard, however work is underway to have it adopted as an ISO. This standard (NZS/AS 3806) (attached to email) has a proven performance record in this region as a tool to assist organisations in creating organisation wide compliance programs that are flexible and responsive and is similarly principles based to enable use by all industries and sized organisations. We would encourage the SFE to have a closer look at the benefits this standard could provide to the organisations it regulates and would recommend that the SFE promote its use as a baseline Standard. This would clearly establish the regulator's expectations as well as provide a reference for reviews the regulator may undertake of an organisation's program.

In addition we would also suggest either guidance within the legislation or a supplementary regulatory guide around the regulator's expectations for self reporting of breaches by organisations. Australian regulators have found this a useful method to reduce the burden on the regulator for investigating and reviewing every organisation it regulates; pre-empts consumer and investor complaints; provides an alert and data collecting method to provide intelligence on market and behaviour trends and can also give clues to the regulators about the entities that aren't reporting and the status of their compliance programs.

ACI would also recommend that the SFE look at establishing a time period to allow for transitional arrangements to occur, that way ensuring industry has time to adjust their operations to the new regulatory regime without falling foul of the legislation.

Part III Intermediaries Conduct

ACI would like to address the following General Principles (GP) in the proposed Code of Conduct.

Code of Conduct – General Principles

GP3. Capabilities

ACI is supportive if this concept however we believe more detail needs to be provided, either within the Code of Conduct or supporting regulatory guides.

Given the circumstances that gave rise to the need for the SFC to introduce these proposals, ACI would have expected that there would have been an increased focus upon the compliance and risk management activities that will be undertaken by licensed or registered persons. In particular, we believe that specific reference needs to be made for licensed or registered persons to have access to compliance and risk management systems that are appropriate for the size and complexity of their business. ACI accepts that for smaller firms or sole operators, that this function can be outsourced, however we note that while the function maybe outsourced the responsibility remains with the licensed or registered person.

By way of example, the Australian Securities and Investments Commission (ASIC) has issued a Regulatory Guide (RG 104) that addresses this specific issue. This guidance note is for license holders and in part states:

> RG 104.49 We expect that you will allocate to a director or senior manager responsibility for:
>
> (a) overseeing your compliance measures; and
>
> (b) reporting to the governing body (including having ready access to the governing body).
>
> RG 104.50 You need to ensure that the area responsible for compliance:
>
> (a) is independent enough to do its job properly;
>
> (b) has adequate staff, resources and systems; and
>
> (c) has access to relevant records.
>
> RG 104.51 It may be appropriate for you to have a separate compliance function (which might be outsourced to a third party). This is likely to be the case for larger, more complex businesses (including a corporate group), but not for licensees whose business is small or whose main business is not the provision of financial services.

ACI also notes that the Office of the Commissioner of Insurance has already issued a guidance note (Guidance Note 10) which is similar to RG104. GN10 states:

> "An authorised insurer is encouraged to appoint a compliance officer to oversee the compliance by it and its staff with the relevant laws, regulations, guidance notes and industry standards and codes of practice. The compliance officer shall also report to the Board at regular intervals."

GP6. Conflicts of Interest

While ACI fully supports the notion that clients should be treated fairly if a licensed or registered person is unable to avoid a conflict of interest, we believe the client should also be informed if the conflict exists. This allows them to make a fully informed investment decision and should the client still proceed with the investment knowing that a conflict exists and what it is, then they can determine if they believe that the adviser has treated them fairly. Without client knowledge as to what the conflict is, then it is up to the adviser's 'moral compass' to assess if the client is being treated fairly and as such there will be a lack of transparency and accountability from both a regulatory perspective as well as a management perspective.

GP7. Compliance

Once again whilst being supportive of this principle, ACI believes more guidance is required to ensure this objective is achieved. We refer to our comments above around GP3, as the issuance of a regulatory guide similar to RG 104 would assist industry in meetings it regulatory obligations.

In addition, ACI believes there is benefit for both industry and the SFC in defining what skill sets a compliance officer must have to be entitled to the title and to be employed by a licensed organisation as the person responsible for regulatory compliance.

ACI has produced a White Paper on this very issue and in short, the attached table to the submission outlines the competencies ACI has found over the past 14 years demonstrate that a person has the skills and knowledge required to be successful in the role as well as ensuring their organisation meets their compliance obligations. We would support the introduction of this criteria by the SFC in determining if an employee with the position title of compliance manager/officer is suitable to hold the role.

Additionally, as previously mentioned, either a supporting regulatory guide or this section itself could refer organisations to the Standard for Compliance (NZS/AS 3806) to assist them in establishing a robust program organisation wide. This will assist the regulator in achieving the objectives of the legislation, establish some consistent criteria across industry and provide a benchmark/reference for the regulator when reviewing behaviours and programs in industry.

Part IV Post Sale Arrangements – Cooling Off Period

While ACI is generally supportive of the concept of a cooling off period so that additional protection is provided to investors under circumstances where aggressive sales techniques have been used, there are some issues we believe need to be addressed before the cooling off provisions should be introduced.

First, ACI notes that the cooling off period would only apply for products that were either long term or illiquid in nature. In respect to the long term nature of an investment product, we believe the SFC need to provide guidance or explicitly define what a long term investment product is. Not only will this create certainty for investors, it will also create certainty for the industry thus assisting in reducing compliance costs. Also, with a clear definition in place, this will prevent unscrupulous advisors from changing the definition of a long term product to suit their means and avoid having to adhere to the provisions of providing a cooling off period.

Secondly ACI agrees that any fees, charges, lost commissions or capital losses should be borne by the investor should they wish to withdraw from the product. However, we believe that this needs to be declared upfront prior to any investment decision being made and again should the investor enquire about exercising their right to leave the product within the timeframe established under the cooling off provisions.

Finally and most importantly, ACI believes that the existence of cooling off provisions can provide the SFE with valuable market data. In most circumstances, an investor will withdraw from a product if they feel a high level of anxiety or buyer's remorse. In most instances, this remorse can be attributed to buying as a consequence of high pressure

or aggressive selling practices. If the SFE collected data on the number of times cooling off provisions were exercised, they would soon gain a valuable insight into the selling techniques of the industry and of particular organisations. If the SFE was then to take a risk based approach to enforcement, it could target those organisations for more frequent inspections/audits if they repeatedly had higher than average industry rates of investors exercising their cooling off options. It would also allow the SFE over time to see if sales practices within the industry were improving or declining.

Once again ACI would like to thank the SFE for providing an opportunity for ACI to make a submission on its proposals to enhance protection of the investing public. Should you require any additional information or seek clarification on the comments that appear in this submission please do not hesitate to contact ACI on +612 9290 1788.

Yours sincerely,

Martin Tolar
Chief Executive Officer

Table 1: Compliance Professional Capabilities

		Pre-Management	Management	Senior Management
1.1	**Generic Skills**			
1.2	Skill Transfer Training	✓	✓	✓
1.3	Communication Programs	✓	✓	✓
1.4	Assertiveness	✓	✓	✓
1.5	Leadership and Team Building	✓	✓	✓
1.6	Negotiation, Influencing, Facilitation and Mediation		✓	✓
1.7	Creative Problem Solving		✓	✓
1.8				
1.9	**Business Process**			
1.10	Change Leadership & Organisational Behavior	✓	✓	✓
1.11	Project Management	✓	✓	✓
1.12	Performance Management & Analysis	✓	✓	✓
1.13	Investigatory: Forensic Review & Monitoring	✓	✓	✓
1.14	Quality Processes and Systems		✓	✓
1.15	Information Management Systems & Reporting		✓	✓
1.16	Internal auditing and general monitoring		✓	✓
1.17	Business Planning, Budgeting and Reporting		✓	✓
1.18				
1.19	**Generic Compliance**			
1.20	Compliance Framework, Planning & Implementation	✓	✓	✓
1.21	Risk Management Frameworks including fraud	✓	✓	✓
1.22	Corporate Governance Frameworks	✓	✓	✓
1.23	Ethics and Social Responsibility	✓	✓	✓
1.24	Breach Identification Management & Escalation Processes		✓	✓
1.25	Complaints Handling Processes		✓	✓
1.26	Compliance Policy Development & Regulatory Relationships			✓
1.27	Due Diligence Processes			✓
1.28	Whistleblower Systems			✓
1.29	Compliance Training Programs			✓
1.30				
1.31	**Legal Compliance**			
1.32	Law for Non Lawyers	✓	✓	✓
1.33	Privacy, Anti-Trust, Consumer Protection, Corporations Act.		✓	✓
1.34	Criminal Code, Anti-Money Laundering			✓

Australian
Compliance
Institute

CPR Protocols

Protocols for Reviewing and Assessing the Adequacy, Effectiveness and Efficiency of Compliance Programs

Foundation Members

Australia's First Bank

PricewaterhouseCoopers

GWF
George Weston Foods Limited

RIO TINTO

Ernst & Young

ZURICH

National

ANZ

Blake Dawson Waldron

IAG

May 2005

building integrity and trust

Australian Compliance Institute Inc. ABN 42 862 119 377 | www.compliance.org.au
Level 2, 341 George Street, Sydney NSW 2000 | GPO Box 4117, Sydney NSW 2001 | Ph 02 9290 1788 | Fax 02 9262 3311

Australian
Compliance
Institute

Disclaimer

This document is not legal advice. Users should seek legal opinion as to the applicability of these protocols to their individual situation.

Document Control Information	
Document Name	Compliance Program Review Protocols
Status	Version 1.0
Release Date	26th May 2005
Version Control	CEO of ACI
Copyright	Australian Compliance Institute

Australian
Compliance
Institute

Contents

1 INTRODUCTORY INFORMATION

1.1 Purpose of these protocols

The purpose of these protocols is to enable organisations and regulators to confidently rely on reports that are produced as a result of a compliance review. The aim of the protocols is to benchmark the quality, consistency, transparency and effectiveness of both the compliance review process as well as the resultant report.

The protocols have been specifically developed to enable organisations to:

- Better understand what is required of them when they are subject to a mandated compliance review as part of a regulator's enforcement outcome.
- Obtain more value from compliance reviews by being able to negotiate more effectively with external reviewers.
- More effectively plan and undertake internal reviews.

The aim of the protocols is also to provide regulators with:

- A set of procedures that can be incorporated or referred to in enforcement and surveillance activities.
- A response to concerns about the quality and consistency of compliance review reports.

The protocols have also been developed to enable the compliance industry to:

- Have a minimum standard for compliance programme reviews and reporting that will enable realistic comparison and benchmarking across organisations as to the effectiveness of compliance measures.
- Set competency benchmarks for persons undertaking reviews in order that compliance professionals can further develop the compliance profession's certification structure.

1.2 What is a compliance review?

A compliance review in these protocols means the undertaking of a process to assess the adequacy, effectiveness and efficiency of an organisation's compliance culture as well as its arrangements and measures to meet its regulatory requirements.

The process may assess the presence of these elements for the past, current and /or future. The scale and depth of a review will vary depending on its purpose. At the broadest level, a compliance review will apply compliance methodology and standards against the overall regulatory framework of an organisation, its business structures, culture, resource management, business and decision making processes, supervision, monitoring and reporting procedures and strategic direction.

A compliance review report is a document that contains detail of the scope and review process, analysis undertaken, levels of assurance, findings, opinions, recommendations as well as any qualifications.

Where a review is requested as a result of a known or suspected regulatory breach, the review may also investigate the cause of the breach and what other compliance issues such a failure may indicate. The subsequent report would contain recommended measures to reduce the risk of the breach occurring again and how those measures may do this.

1.3 Application of protocols

The protocols may be applied to the full range of compliance reviews however they have been drafted in contemplation of setting a minimum standard for compliance reviews and reports that are required from time to time by regulators in relation to enforcement actions.

The standard required by regulators is necessarily high because the report is often requested as part of enforcement activity. These reports are obtained to provide a level of assurance about the effectiveness of compliance arrangements in place and the ability of the organisation to comply with regulatory obligations going forward.

For other reviews whether conducted internally or by external parties the protocols should be seen as best practice for a broad compliance review. Accordingly for many reviews not all considerations in relation to each protocol will be relevant.

In particular it is acknowledged that many considerations will not be relevant for small organisations (less than 20 people).

In recognition of the potential different users, PART 2, " THE PROTOCOLS", is a stand alone section which allows the user to determine what is relevant to meet each protocol.

The protocols may be applied to any scale or type of review. Examples of the types of reviews where they may be applied include:

- Compliance with AS3806 "Compliance Programs";
- Compliance with specific regulatory obligations;
- Compliance with an industry Code of Practice; and
- Compliance with internal policies.

The scale of a review can range from the review of a single issue to a range of issues, or from an in-depth, to a high level review and may include the following:

- An organisation's commitment to compliance (cultural review);
- Existence of a broad compliance framework (high level program review);
- The effectiveness of a compliance framework to an agreed level of assurance (assurance or regulatory review); and/or
- The assessment of individual measures to determine ability to comply with specific obligations (specific obligation review).

The protocols may also be useful for organisations for use in conjunction with other internal monitoring processes, or for a compliance review of third parties under outsourcing or other contractual arrangements.

> **Caution**
>
> These protocols are aimed at the process of carrying out a compliance review and drafting a compliance review report. It is envisaged that compliance with the protocols may be used by an organisation or a regulator as a way to determine the adequacy of the review process. It is *not* envisaged that they be relied upon to determine whether any findings contained in a compliance review report are accurate. By following the protocols, the content and findings in the report should be able to be verified in some way. The quality and accuracy of the findings depend, amongst other things, on the skills of the reviewer and the level of cooperation from the organisation.

1.4 Why a review and not an audit?

The term "audit" has deliberately not been used in the protocols, even though it is acknowledged that the term "compliance audit" is often used to describe a compliance review process. A review process may use recognised audit procedures and principals, but the review process is intended to denote a different process to audits contemplated under the Corporations Act 2001. Audits of this nature are performed by registered auditors and are subject to the auditing standards and guidelines issued by the Australian Auditing and Assurance Standards Board.

There are key differences between an audit and a compliance review:

1. A compliance review often requires legal and other non-accounting skills to be applied. These skills may include the ability to:
   - analyse and understand a broad cross-section of legal obligations;
   - understand what frameworks, processes, and behaviour need to be in place for the organisation to comply with its obligations; and
   - assess whether the processes in place will enable compliance in the future.
2. An audit is usually intended to:
   - cover past events;
   - express a high level of assurance through a positive expression of opinion; and
   - determine a position over a specified period or at a point in time.
3. A review process may also cover an audit outcome but may also provide a view as to:
   - whether there are measures in place to enable compliance in the future;

- nature of an organisation's compliance culture; and
- the quality and effectiveness of an organisation's compliance programme and frameworks in light of its risk management frameworks and corporate governance processes.

Caution

The term "review" in these protocols does not necessarily have the same negative assurance meaning as used in Auditing Standards prepared by the Auditing and Assurance Standards Board.

1.5 How to use these protocols

This document is divided into 4 main parts:

Part 1 *Introductory Information* - provides background and explanation about the protocols.

Part 2 *The Protocols*- 12 outcomes that should be met

Part 3 *Considerations for each Protocol* – what to consider and helpful tips

Part 4 *Guidance for Reviewers* - contains specific guidance for reviewers.

The protocols are designed to help parties draft a review planning document and subsequent compliance report.

Each protocol describes an outcome that must be either incorporated in the review process and/or in the review report. Each protocol is then followed by guidance as well as a number of considerations that should take into account when addressing the protocol.

As each protocol is linked to the other protocols they should be read and applied as a whole however, to assist users, there is duplication in some guidance to enable each protocol to be as stand alone as possible. The protocols have not been designed as a "how to", rather they have been designed to help parties ask the right questions so that they can align expectations upfront and achieve a high quality outcome.

The protocols are not intended to provide guidance on how to analyse the information obtained during the review or detail what conclusions can be drawn from the existence of certain measures or certain structures or certain gaps. Analysis depends amongst other things on the skills, experience and knowledge of the reviewer.

1.6 Updating the protocols

The protocols will be updated and reviewed by the Australian Compliance Institute as needed, but as a minimum within 3 years. Any review will be based upon feedback of users to ensure the protocols remain relevant and facilitate the outcomes being sort.

Feedback should be sent to: CRP@compliance.org.au

2 THE TWELVE PROTOCOLS

First Protocol Scope

The review plan must state the reason for the review and clearly define its scope, including, what will and will not be reviewed and why, the type or level of review, the period to be covered, and what will happen if scope creep occurs.

It must also explain the reviewer's reporting obligation in the event they come across any issue or breach which is not part of the scope.

Finally, it must specify any limitations that apply to the circulation of the report to third parties.

Second Protocol Reliance

The review plan must state who will be relying on the compliance review report and for what purpose or purposes.

Third Protocol Assurance

The review plan must state the level of assurance that will be provided and any standard disclaimers that may appear in the compliance review report.

Fourth Protocol The Process Plan

The review plan must clearly describe the process that will be followed in relation to the management and administration of the review. Including who will be responsible, progress reporting, timing, and resources. The review plan must also state at what stage draft or interim reports will be provided to the organisation and how feedback on these reports will be recorded.

Fifth Protocol Limitations

The review plan must set out any limitations to conducting the review and the compliance review report must set out any limitations in preparing the report.

Sixth Protocol Information

The review plan must set out as far as possible what information will be reviewed and collected to form the factual basis of the compliance review report. The review report must describe in detail what information was actually reviewed, collected and relied upon to form the basis of the findings and/or recommendations.

Seventh Protocol Methodology

The review plan must outline the methodologies that will used to review and collect the information that will form the basis of the compliance report. The review report must confirm use of the methodologies and disclose any variance from the methodology detailed in the review plan.

Eighth Protocol Who Performs the Review

The compliance report must disclose all persons who performed the review including what part of the review they performed and what qualifications and experience enabled them to carry out that work.

Ninth Protocol Basis

The compliance report must detail the basis of why the information reviewed caused the reviewer to make the findings, opinions or recommendations. This analysis must be complete and transparent.

Tenth Protocol Level of Assistance

The review report must detail the level of assistance received by the reviewer from the organisation when conducting the review, including the level of assistance, from whom as well as any hindrance. The report must also detail any complaints or feedback received by the reviewer about the reviewer's methodology or approach.

Eleventh Protocol Risks Going Forward

The review report must explain within the context of the review the risks to the ability of the organisation to comply going forward. The final report may also contain a response by the reviewee as to how each risk will be managed.

Twelfth Protocol Present the Findings

The review report must contain findings, opinions and recommendations in a clear and easy to read format or table. The report (if agreed in the review plan) must also contain a plan for implementation of the recommendations.

3 CONSIDERATIONS FOR EACH PROTOCOL

First Protocol Scope

The review plan must state the reason for the review and clearly define its scope, including, what will and will not be reviewed and why, the type or level of review, the period to be covered, and what will happen if scope creep occurs.

It must also explain the reviewer's reporting obligation in the event they come across any issue or breach which is not part of the scope.

Finally, it must specify any limitations that apply to the circulation of the report to third parties.

Considerations

How does the reason for the review impact on its scope?

Background information which highlights why the review has been requested will help to limit the scope. The level of detail of background information will depend on the level of awareness of the review circumstances that the expected end-users of the report will have.

For example each of the following reasons for the review will have a different impact:

- Board/management request
- Regulatory requirement
- Regulatory enforcement (license conditions, enforceable undertakings, other)
- Takeover due diligence
- Parent company requirement
- Contractual requirement, eg as part of a loan or outsourcing agreement

What is the level of the review?

- High-level review of the compliance framework against AS 3806, including the existence of relevant documentation.
- Review of the elements of a compliance programme in place, including resources, positive compliance culture and high level reporting, review and monitoring. Are they in place and are they working, what are the issues and what are the gaps in reducing beaches?
- Review of detailed compliance measures to meet specific regulatory obligations. Are the compliance measures in place able to meet compliance obligations, now and in the future and why?

- Review of past compliance issues. What happened in the past and why?
- Is the review going to assess effectiveness as well as efficiency? Are the compliance measures effective going forward as well as efficient?
- Review of potential internal and external environmental impacts on the organisation's compliance measures. In looking at effectiveness, what potential changes will be taken into account in the future and is there a limitation on this period?
- An assessment of the, competency, understanding and behaviour required at board and management to meet obligations (eg managing conflicts of interest).

What is the period to be reviewed?

- Are existing compliance measures being reviewed only?
- Are measures in place over a certain period or past date being reviewed?

What other points should be considered?

- What is in and what is out of the review? For example, the review will cover monitoring and supervision procedures over outsourced service providers; though it will exclude procedures performed by the outsourced service provider.
- What will happen in the event of scope creep?
- How broad is the review? Eg, compliance by the whole entity with the Trade Practices Act from board level to call centre operators; or compliance of a regional cold storage operation with HACCP. That is, the scope should detail what aspects of operations and the business units of the entity that are to be reviewed.
- What does each stake holder expect from the review? Each may have a different expectation. What do they expect to know at the end of the review?
- What are the consequences if a review is not conducted?
- What assurance will be required about the effectiveness, as well as the efficiency, of the compliance measures and how will this impact on scope. A level of comfort may be able to be provided that the entity has measures in place that enable compliance, but are they so inefficient that compliance will be difficult to sustain?
- Is the assessment of internal and external impacts part of the review?
- If the review is to assess breaches, will the review cover why the breach occurred? What has been done to fix it, or can be done to fix it.
- Will the review look at, training, induction and human resource processes?

Does the review provide an opportunity to raise issues or breaches outside the scope?

- What is the responsibility of the reviewer in this event
- Should observations be contained in a separate document to be provided to the organisation being reviewed only?

What if the reviewer has some serious concerns while conducting the review?

- An independent board member may be the most appropriate person in this regard but in some instances disclosures must be reported in accord with State and Commonwealth corruption and whistleblower protection laws. Informing a business owner or board member may breach these laws.
- Procedures for handling information concerning fraud, corruption or other acts of a criminal nature uncovered by or reported to a reviewer must be prepared prior to the project commencing. The procedure must recognise the obligations under the State and Commonwealth laws relevant to the organisation being reviewed.

What third parties may review the report?

- Will it be viewed by auditors at some time in the future?
- Which regulators may have access to it?

Second Protocol Reliance

The review plan must state who will be relying on the compliance review report and for what purpose or purposes.

Considerations

Who is the report being prepared for?

- Identify all parties, both internal and external, who are likely to read and place reliance on the report. Understanding who will use the report and for what purpose will guide considerations on materiality and level of detail required.
- Who will be provided copies (boards, auditors)?

What are the potential liabilities to the reviewer as a result of this reliance?

- If a third party relies on the report is there any indemnification for the reviewer?
- How will the report be relied upon and what impact does this have for the liability of the reviewer?
- What indemnity for the reviewer may be appropriate?

Is there a way of limiting the reviewer liability?

- Determine what the consequences would be if the reviewer gets it wrong. Will the parties relying on the report require compensation? It may be appropriate to enter a "pre-nuptial" agreement with the reviewer to limit compensation, eg set a maximum of 10 times the fee for the review.
- Will professional indemnity insurance be required and if so how much? Will a copy of the policy be provided?

For example, where an organisation has agreed to obtain a compliance review as part of a regulatory action, then parties may agree that:

- the report is to be prepared for the organisation and will be provided to the organisation by the reviewer;
- the organisation will be responsible for providing the report to the regulator;
- the reviewer will only be liable to the organisation for any negligence in preparing the report;
- the reviewer will be under no obligation to disclose to the regulator any issues arising outside the scope of the review plan; and
- the regulated entity will be responsible for negotiating with the regulator the level of assurance to be provided in the report.

Third Protocol Assurance

The review plan must state the level of assurance that will be provided and any standard disclaimers that may appear in the compliance review report.

Guidance

This protocol is closely related to the previous protocol, as the level of assurance provided relates to how much reliance, or the type of reliance, parties will have in relation to the report.

Examples of assurance wordings that will accompany findings in the report should be provided in the review plan in order to avoid surprises later. Assurances may relate to, opinions as to whether compliance has occurred in the past and /or whether compliance measures in place will enable compliance in the future.

The more in-depth the review, the greater the level of assurance that can be provided. Where a review is high level it may be agreed that the report will not contain any assurances as to compliance, but merely recommendations.

Considerations

- How much responsibility is the reviewer prepared to take?
- What type of comfort is the organisation seeking in relation to their ability to comply in the future?
- Should different levels of assurance be provided in relation to different aspects of the review?
- Will it be negative assurance?
- Will it be positive assurance?
- Will it be a guarantee?
- Is an agreed upon procedures report more appropriate?

For some regulators the level of assurance in relation to compliance is not the issue, rather they rely more on the quality and transparency of the review process. The greater the review process is understood, the easier it is for the regulator to form their own view as to compliance issues. Accordingly, a level of assurance as to the ability to comply going forward may not be required, but rather an assurance that all agreed procedures in relation to the review were carried out and that certain compliance measures are in place may be more appropriate.

Helpful Hints

In order to minimise the expectation gap, prepare a draft wording similar to what is intended to be included in the report, and have the principal users of the report and the reviewer agree on the wording before the review commences.

Fourth Protocol The Process Plan

The review plan must clearly describe the process that will be followed in relation to the management and administration of the review. Including who will be responsible, progress reporting, timing, and resources. The review plan must also state at what stage draft or interim reports will be provided to the organisation and how feedback on these reports will be recorded.

Guidance

The level of planning for the review will depend on its type and scale. An in-depth far reaching review may have a large impact an organisations day to day activities. To manage this issue the review plan should be signed off by all parties before any work commences. The plan must be detailed enough in order that the organisation clearly understands the level of commitment it will need to provide throughout the review process.

Many reviews fail due to lack of assistance from within the organisation as well as poor planning by the reviewer. For this reason it is important that assistance be guaranteed through board and senior management support by their sign off of the review plan. It should also include a contact plan or meeting schedule in order that the reviewer can take into account commitments and feedback from staff within the organisation throughout the review process.

Considerations

In developing the process consider which of the following may be relevant:

The plan – high level:

- How will the project plan for the review be documented?
- Will the reviewer use a recognised project planning methodology?
- Who will sign off the review plan?
- Besides the decisions on scope, assurance, etc, what else will the plan contain?
- Who within the entity will sponsor or champion the review?
- How will access to relevant documents/records/staff be negotiated

Plan detail – resources:

- What resources, including specialists, will be needed? (include internal and external, eg IT specialist, industry analyst, administration, legal, accounting, etc)
- What will be impact of the review on the organisation? – When will it happen, how and what will be the cost in money, time and resources?
- How will the plan be communicated to the organisation's staff and management and how often will updates occur?
- Who will be the main contact throughout the review within the organisation?
- What information will be provided to the board and senior management about progress?
- Who will be accountable if the review is not completed within the timeframe?
- What site safety, inductions, procedures and security must the reviewer be aware of before entering the premises

Helpful Hints

A project leader should be appointed to "own" the project. This person should be responsible for drafting the review plan and be the main point of contact for all parties associated with the review. It is likely the project leader will be a senior member of the organisation being reviewed. Whether the project leader works within the operation under review or not will depend on the type of review and level of independence required.

The plan should contain milestones, action plans (if relevant), the names of persons that will need to be involved, risks, limitations, costs, timing, impacts and measures for success as well as a communication plan.

The draft or interim report:

- Will a draft or interim report be provided and if so, to whom and at what stage in the review? Will they have an opportunity to comment and if so on what?
- It is sometimes not appropriate for the organisation to be given an opportunity to review draft findings in the report as there may be the opportunity for the report to be sanitised before release, or at least create a perception the report may have been sanitised.
- However in most cases it is appropriate (even desirable) for the organisation to be provided with an opportunity to provide feedback on the factual basis contained in the report so that the accuracy of information can be checked before the report is finalised.
- Will a log of any amendments to the draft report be detailed in the final report?

Helpful Hint

If there are a number of drafts of the report, consider including a commentary explaining the basis for the changes from the previous draft so that all parties are comfortable with the amendments and have opportunity for comment.

The final report:

- What will the final report look like?
- Will it contain findings as well as recommendations on how to address issues?
- Will it contain a rectification plan detailing timing and areas or people responsible?
- Will the issues be rated in order of priority or risk?
- What methodology will be used to identify and categorise the risk of a compliance issue?
- Will the report be delivered to all parties at the same time or in an agreed order?
- How will the report be provided – hard copy, soft copy or both? Will it be numbered so that all copies are able to be identified.
- Will the reviewer be required to present the report verbally and be subject to questioning? If so, by whom – board, regulator or others?

Helpful Hint

It may be appropriate to release a report in two stages. The first report can cover the big issues so that all interested parties can make a start on any corrective action required while the detailed report is being finalised.

Fifth Protocol Limitations

The review plan must set out any limitations to conducting the review and the compliance review report must set out any limitations in preparing the report.

Guidance

Limitations may include limitations of scope due to unavailable staff and/or records, conflicts of interest, remuneration or time allowed. Limitations on scope may be unavoidable due to the timing and urgency of the report. These limitations should be identified by discussions between all parties when developing the review plan.

Considerations

The area of limitations can be quite complex. For example, it may be necessary to explain why the scope of the review limits the assurance or opinions that can be formed.

- Were there any limitations in preparing the report or in carrying out the review?
- Was there enough time?
- Were the right people available?
- Did the scope change?
- Was there enough board and management support?
- Was there enough access to systems and records?

Helpful Hints

Often it is helpful to explain what the review will not provide to the organisation. For example, it is unlikely that a review will be able to confirm for the board of an organisation that it is currently complying with all regulatory obligations continuously. Full, practical disclosure (not hidden behind legal or auditing jargon) about the limitations of the report is encouraged.

Sixth Protocol Information

The review plan must set out as far as possible what information will be reviewed and collected to form the factual basis of the compliance review report. The review report must describe in detail what information was actually reviewed, collected and relied upon to form the basis of the findings and/or recommendations.

Guidance

The quality, depth and accuracy of the information obtained are a vital part of any review. The quality of the information has a direct bearing on the ability of the reviewer to undertake an analysis to form a view. The report should disclose the processes, systems and documents reviewed, personnel interviewed, which reviewer performed the work, whether they were on-site and how long they were there performing this work.

This information will allow the reader to form a view as to whether the results of the review met the original objectives and identify any gaps in the review that may require further attention.

Liability issues should also be easier to deal with if the working papers clearly set out what work was done and why and how the results support the wording in the report.

Considerations

What information needs to be collected to make findings, form opinions or make recommendations?

What depth of information will allow them to assess for example the:

- Effectiveness of the compliance programme – what benchmark or standards?
- Presence of the necessary elements of the programme
- Level of the compliance culture
- Effective communication of the compliance policy
- Adequacy of compliance resources
- Quality of compliance of operational processes
- Adequacy of supervision & monitoring
- Effectiveness and truth of reporting

What was the source of the documentation and who provided it:

- What was the character of the document?
- Where did it come from?
- Who else has a copy?

How will the information be collected, recorded and stored:

- How will documents be managed, identified, recorded and stored? The collection of documents and recording of information must be able to stand up to close scrutiny. The time, date, method of delivery and source of any document must be recorded. Documents must be collected in such a way that they are easily identified. Where documents are reviewed ensure that there is a full description of the document.
- How will systems be described for ease of reference?
- How will answers to questions be documented?
- How will information provided during an interview be recorded? Will the conversations themselves be recorded or will another method be used.

Who will have access to the working papers?

Helpful Hints

It is suggested that the reviewer be provided with a secure area on the premises of the entity in order that all documents and files can be safely secured during the review process.

Seventh Protocol Methodology

The review plan must outline the methodologies that will used to review and collect the information that will form the basis of the compliance report. The review report must confirm use of the methodologies and disclose any variance from the methodology detailed in the review plan.

Guidance

Agreeing on the methodologies of how information will be collected is necessary as it supports the level of assurance that may be required. It also provides clear guidance to the reviewer by determining how the information will be collected, and from where, to allow the reviewer to obtain sufficient information to draft the report and formulate conclusions?

Considerations

Has the methodology been disclosed?

For example, have details of the following been provided where applicable:

- use of self assessment
- types of testing performed
- collecting and identifying data – how was this done?
- sampling basis, i.e. use of an appropriate statistical basis and method for selecting items for testing. The reviewer should record the reasons why the sample is representative of the population of items selected from. The basis of selection should reflect the purpose of the testing, eg if the issue that gave rise to the review only arises in transactions of a value less than $10,000, then the sample would be restricted to the population of transactions in this category.
- use of experts
- use of walk throughs
- observation of processes over a period of time
- scenario testing
- questionnaires or surveys
- substantive testing, i.e. vouch items directly to supporting evidence
- controls testing i.e. satisfy yourself the system of controls is adequate and is/has been operating effectively over the review period and will continue to do so. The objective is to be able to rely on the system of controls to pick up any errors in the operation under review and, on that basis, be satisfied the output from the operations is correct.

- industry quality controls, eg Hazard Analysis Critical Control Point (HACCP) systems.
- document review – what was read and what was sighted. Was the use of the document by the entity tested in practice?
- system review, eg use of dummy data, reliance on previous third party reports, use of experts.
- process review, eg walk through tests, review of procedures manuals, etc.
- recording information – in what style?
- methods of verification of information.

Choosing a Methodology

The reviewer should research the area of operations to be reviewed to provide them with sufficient knowledge of the business that will allow an effective and efficient review methodology to be developed.

The most appropriate methodology will depend on a number of factors, including:

- type of operations being reviewed, eg highly automated, technically complex, labour intensive, high volume of transactions, etc;
- level of assurance provided. A higher level of assurance will require more detailed work to provide more certainty that the results of the review accurately reflect the organisation's state of operations.
- scope of review, eg is it a high level review of a large operation, or a detailed review of a specific area of the entity's operations? Does it cover effectiveness and efficiency?
- time available to perform the review. If there is a short timeframe the methodology agreed up front may have to be based on less intensive testing, eg: analytical review, self assessment questionnaires, etc
- availability of entity staff. If key staff are not available alternative procedures may be required;
- records available;
- circumstances that gave rise to a requirement for a review.

If one of the reasons for the review was the reliability of certain records, the methodology may need to be developed to use other data to ascertain the organisation's true circumstances.

Quality of Evidence

The quality of evidence obtained from the review will be a direct result of the methodology used and will depend on the circumstances of the review.

An example of good quality evidence is confirmation obtained from independent third parties directly by the reviewer. Moving down the scale, independent confirmation obtained by the organisation would be of lower quality, while verbal representations by staff would usually be considered lower again.

This may not however be the case when considering issues such as corporate culture. In such a case it may be appropriate to use surveys or knowledge testing questionnaires to test the level of compliance knowledge throughout the organisation.

Helpful Hints

Consider obtaining information from the parties who initiated the review. They may have relevant information from previous investigations that gave rise to the review being requested. This could save significant time and cost for all parties involved, though is likely to require a release from the regulated entity that they do not have an issue with the reviewer discussing confidential matters with the regulator.

Eighth Protocol Who Performs the Review

The compliance report must disclose all persons who performed the review including what part of the review they performed and what qualifications and experience enabled them to carry out that work.

Guidance

It is imperative that independent, suitably qualified and experienced reviewers design and carry out a review to be able to correctly analyse and interpret the review of information. In some instances specialist skills may be required, for example specialist industry knowledge, IT skills and administration skills.

Considerations

Reviewer capability and appropriateness

- why were they chosen?
- why are their skills, knowledge and experience relevant to the review?
- do they have the necessary independence?

Appointment of a Reviewer

- What process will be or was undertaken to appoint the reviewer?
- Was the review put out to tender?
- Who assessed the tender proposals?
- Has the independence of the reviewer been independently verified? Is it necessary to obtain references?
- Has the appointment process been transparent?

Where the approval of a reviewer must be approved by a third party or regulator that approval process must also be transparent.

Proper submissions should be made outlining all the relevant factors relating to the appointment of the reviewer in order to avoid personal preferences dictating who is appointed.

What skills, experience and knowledge are required?

The skills, knowledge and experience required needs to be determined once the scope has been agreed.

How relevant are the following?

- Level of understanding of the relevant law and how it applies to the entity,
- Level of understanding of the industry and its compliance frameworks,
- Level of understanding of administrative processes,
- Level of understanding of IT systems,
- Level of legal, actuarial, accounting, auditing skills,
- Any implications from the reviewer being part of the same industry,
- Compliance skills and knowledge,
- Level of practical knowledge and experience,
- Number of previous reviews conducted,
- Independence, conflicts of interest and details of any other services the reviewer has performed for the regulated entity and payment received,
- Where it is an internal review, how much control and input the reviewer had in the implementation of the compliance framework previously,
- Level of professional insurance required,
- Capacity to provide services and backup.

Some of the above will have little importance, while others will be crucial. It sometimes helps to rate the importance using a scale of one to ten in order that there is more of a chance to have a choice of qualified reviewers.

In certain circumstances it may be appropriate and more efficient to appoint a reviewer who is an employee of the organisation to make use of their knowledge and experience of the organisation's business. If additional comfort is required to satisfy any concerns about a perceived conflict of interest, a third party could be engaged to assess the review process that was followed.

Is there a power of veto in relation to the appointment of the reviewer?

This is an issue that must be discussed, particularly if a review is requested by a regulator. The question arises who should choose the reviewer. With set criteria this would seem simple enough, but sadly often preconceived views and personalities have an impact. The appointment of a reviewer should be an objective transparent process. Where the appointment of a reviewer is objected to, or one reviewer is chosen over another, the reasons must be documented. This will reduce the risk of bias by both the organisation and third parties including regulators.

Who is in the Review Team?

It is important to record all persons who took part in carrying out the review particularly where special expertise has been utilised. It must be made clear what the role of each reviewer was and what they actually did as part of the review. For example, there may be an instance where a reviewer has been contracted but in reality they only performed a project management or strategic role. In this instance it will be important to identify who actually carried out the review and what they did.

Independence and conflicts of interest

The key aspect to independence is the potential for a conflict of interest. Lack of independence is seen as an issue that may compromise any report. What it means to be independent will be different for different reviews. The level of independence will need to be agreed upfront and full disclosure made of any relationships or other potential conflicts. The higher the level of assurance required the more independent the reviewer must be.
The review plan should set out how conflicts of interest are to be disclosed by each party to the review and if any further due diligence is required. The plan should also cover processes to determine if any changes to the process plan or appointment of reviewer are required to address the conflict.
What it means to be independent or without conflict will be different for each review. The key is to define independence and potential conflicts in the context of the review up front. Where a review is being conducted as part of regulatory enforcement, the following may be considered to be *minimum requirements:*

The reviewer

- did not put the measures in place that they are reviewing.
- will not be the person given the responsibility of implementing recommendations in the report.
- has no prior informal association with the entity or any of the management.
- has no current or past professional relationship with the entity or its management at least in relation to matters related to the review.
- is not being remunerated by the entity in any other capacity.

Ninth Protocol Basis

The compliance report must detail the basis of why the information reviewed caused the reviewer to make the findings, opinions or recommendations. This analysis must be complete and transparent.

Guidance

The basis of the review is the reasons why findings were made, and opinions and recommendations provided. This is the key skill of any reviewer as it represents the analysis of the information obtained.

There are two processes to form the basis of a compliance report:

- the review of the information; and
- the analytical assessment of that information.

The reviewer must be able to show that all processes have been followed in forming the basis of the findings. The process may be contained in working documents which are kept by the reviewer.

A reviewer should be able to show why the presence of certain factors was relevant to the final findings. In this regard it is sometimes necessary to split the findings into those that are independently verifiable and those that are an opinion only.

Considerations

- Were there limitations in the information that would impact on the analysis?
- Were there any timing issues with the provision of the information?
- How has the examination of historical information been impacted by changes made by the organisation?
- How far can the information be relied upon?
- What qualifications need to be provided about the basis?

Recording the results

In order for the review to be independently verifiable and for the readers of the report to understand how the reviewer formed their views the reviewer must record the procedures performed in detail. This follows on from the Seventh Protocol "Methodology" and includes recording:

- sampling methodology used;
- documents reviewed;
- results of any testing;

- positions of people spoken to;
- which operations were visited and when;
- if work was completed on-site or remotely;
- how long the reviewer spent on-site and which review team members were involved; and
- questions asked in interviews and the answers received.

The above list is not exhaustive and the reviewer will need to use professional judgement as to the level of detail that is appropriate to the circumstances.

Helpful Hints

Depending on the type of the review and parties involved it may be useful at the start of the review for the reviewer to prepare a scoping paper setting out how the review is to be performed.

This may be essential if, once the review has commenced, the reviewer realises that it is not possible to complete the review in accordance with the process plan and needs to amend the approach. This should avoid disappointment from the amended approach not meeting the report users' requirements

Tenth Protocol Level of Assistance

The review report must detail the level of assistance received by the reviewer from the organisation when conducting the review, including the level of assistance, from whom as well as any hindrance. The report must also detail any complaints or feedback received by the reviewer about the reviewer's methodology or approach.

Considerations

What do you need?

Provide the organisation with a clear message of:

- what levels of personnel in the organisation are needed to help,
- how much of their time you estimate you will need; and
- when access is required.

What did you receive?

Disclose in the report how much assistance you received and who from.

- Was it helpful, was there any hindrance?
- If the reviewers were hindered was there a material impact on the review?

  This has implications on the scope and integrity of the report hence is very significant information for the end-user of the report.
- How will you rate the level of assistance?

  It will be important to define how levels of assistance will be defined or rated. Will it be a number out of 5 or words such as helpful to obstructive?

Some things to consider include:

- Access to documents – how quickly were they able to be retrieved?
- Access to managers and other key staff time – did they avoid the commitment or did they have other priorities?
- Free access to systems and files
- Access to administration or other relevant areas
- Openness of staff – were they concerned they might get into trouble?
- Availability of staff
- Access to records, including board records.
- How will you record and report obstructions?

If the level of assistance was poor it may indicate a number of factors including:

- a cultural problem;
- a lack of resources;
- an organisation in crisis;
- fear of retribution if seen co-operating with the reviewer;
- poor communication by the reviewer ; or
- the reviewer not following the agreed plan.

Any one of the above may assist in determining findings and may help support any negative conclusions in the report.

The difficulty in this area is gut reaction. What if the reviewer suspects they are being lied to and they know this will hamper them materially in performing the review?

To address this it is suggested that for each review the organisation provides not only a business owner but also a person that the reviewer can report any real obstructions to. An independent board member is often the most appropriate person in this regard however where the obstruction is very serious the reviewer must consider whistle blowing obligations under State and Commonwealth laws relevant to the organisation.

Ceasing the Review

There may be some instances where the reviewer must cease the review because of lack of support. This may be because the entity as lost confidence in the reviewer or they are concerned that the review will highlight issues that they would rather not be highlighted at the time.

Accordingly each review must have a defined and agreed exit strategy.

Eleventh Protocol Risks Going Forward

The review report must explain within the context of the review the risks to the ability of the organisation to comply going forward. The final report may also contain a response by the reviewee as to how each risk will be managed.

Considerations

- Explain the nature of the risk
- What is its likely impact of the risk?
- How serious is the risk?
- How can it be addressed?

Have you considered risks such as:

- a lack of compliance resources
- poor systems
- need for training
- a lack of compliance culture
- a lack of business ownership
- inflexibility of processes
- regulatory change
- uncertainty of regulatory approach
- lack of a link of compliance measures to risk management
- poor corporate governance
- conflicting or poorly drafted legislation

The report should include the reviewer's observations in respect of potential impacts on the compliance framework going forward. The report should explain:

- if the reviewer believes that the organisation has in place systems, resources, etc that enable them to comply with the law;
- if corporate culture is an issue; and
- what comfort there is that the organisation's management know what they are doing and that they want to improve?

All of the above factors will influence views on the risks to the organisation's ability to operate effectively and in compliance with the law on an ongoing basis.

The difficulty will arise where it is apparent that there is little chance of the entity being able to address risk going forward. For example, a lack of:

- financial capability; or
- board and CEO capacity.

There may also be significant issues identified by the reviewer as risks to the compliance framework that may not be a current issue but will need to be addressed in the near future. Examples include:

- future planned changes to the organisation's activities;
- impending changes to external factors such as legislation or major customers; and
- over-reliance on key staff.

When explaining the risk in a report it is particularly important to explain the basis for the comment as this will have an impact as assessing the likelihood of the risk occurring .

Twelfth Protocol Present the Findings

The review report must contain findings, opinions and recommendations in a clear and easy to read format or table. The report (if agreed in the review plan) must also contain a plan for implementation of the recommendations.

Considerations

Consider reporting using headings such as:

- findings
- weaknesses identified
- what the findings mean for the organisation
- response by the organisation /business heads to the report
- opportunities
- the way forward
- recommended actions
- as well as the subjects and issues contained in previous protocols and or specific requirements by regulators.

Who is the audience?

It is likely that the reviewer's report will be read by people who are unfamiliar with the background to the issues that gave rise to the review and the entity's activities and structure. This needs to be taken into account when deciding the level of detail required in the report.

Avoid padding and remember the document is a key communication document. Link the findings to the scope and group the findings if possible. Use of an index, contents page, executive summary and glossary are always helpful, as is numbering the paragraphs.

Is it going to a regulator?

Where the report is being presented to a regulator and the organisation is only permitted to see the final report, prepare the report in such a format that allows the organisation to provide specific comments on each part of the report (remember the process for issuing interim reports must be in the process plan).

Communicating recommendations

One of the more difficult issues is how to address the recommendations or suggestions for improvement. Placing theses recommendations in the same table as the findings may not always be the best approach as the recommendations may apply to a number of findings. In some instances it may be appropriate to place the recommendations on how to address issues or rectify them in a separate document, which becomes a planning document for the entity.

Separating compliance issues?

Some reports may require a separate section on limitations to addressing the compliance issues or rectifying them. This separate section may have limited circulation, for example the view may be that, in order to improve overall compliance the CEO will need to be removed, or the compliance manager is not up to the task. These comments clearly should not be in a widely circulated document.

Helpful Hints

Ensure that numbers of copies are recorded and who they are held by (you may want to number each copy). It may be necessary to recall all copies at a later date. Where a soft copy is provided, convert it into a secure PDF document if possible to avoid it being tampered with.

Ensure the cover page clearly states who it is addressed to, that it is private and confidential and that it cannot be copied or distributed unless agreed.

4 SPECIAL GUIDANCE FOR REVIEWERS

(Please note the following is not legal advice and is not intended to be relied on as such)

When a review is being conducted by an external party the issue of liability arises. As with any professional service there is contemplation that the service will be performed to a certain standard and, if that standard is not met, legal action may follow. The issue around liability becomes more complicated where more than one party will be relying on the compliance review report. Each situation will be different and will ultimately depend on the scope of the review and the relationship between the parties.

In determining the extent of a reviewer's lability the following may be considered:

- Who is the reviewer liable to (or to whom do they have a duty)?
- To what extent are they liable (for what actions or non action can they be liable)?
- How much responsibility are they willing to accept including professional indemnity coverage?

In considering who the reviewer may be liable to, there may be an assumption that the only liability is to the person or organisation being reviewed. Where a review is part of a regulator's enforcement action, and as such the regulator may be relying on the report, there is a risk that the reviewer's liability may also extend to the regulator. This may be the case even where the organisation takes responsibility for providing the compliance report to the regulator.

Analogous issues have arisen where duties have been found to be owed to parties other than the client. In that regard, the reviewer needs to bear this potential expansion of liability to third parties in mind when framing the engagement and performing the review.

When considering the extent of potential liability, the following factors may be considered:

- scope of the review,
- who the report is being produced for?
- who will be relying on the report and for what purpose?
- level of assurance required, and
- what disclaimers or qualifications may be relied upon or acceptable?

Ultimately it is a matter to be determined in relation to each review. In some circumstances it may be appropriate to limit lability to the quality of the conduct of the review and not to the accuracy or reliability of the findings or assurances. However in the event that liability must be accepted for any findings and/or for assurances that the organisation will comply going forward, it may be appropriate, particularly where third parties will be relying on the report, for the reviewer to obtain some form of indemnity from the reviewed organisation.

4.1 Identifying and Managing Risks and Determining Costs

Each reviewer may need to consider what responsibility they are willing to accept in performing a review and how best they can limit their risks. In particular, the responsibly that may continue after a review is completed will need to be considered.

The level and extent of responsibility and risks may have a direct bearing on the amount to be charged.

In managing this risk a reviewer may consider the following:

- The extent of cover under their professional indemnity insurance (will it cover litigation costs?).
- The breadth of any indemnity they may need from the organisation reviewed. This may include indemnity for costs in answering subpoenas or producing working papers in litigation.
- What confidentiality agreements will need to be entered into?
- What approvals may be required from the entity to speak with its lawyers, auditors, service providers or the regulator? Further, what obligations arise for the reviewer to share these conversations with the entity?
- The extent to which the reviewer will need to arrange for potential compensation or reimbursement for costs associated with involvement in litigation or investigations after the review.
- How will working papers be stored and for how long. It is usual to ensure the records are kept for a minimum of seven years. This availability may be made known in the final report. The cost of this storage may also need to be considered.

4.2 Conflicts and Whistle Blowing

The identification, disclosure and management of conflicts must be considered before, during and after each review.

There will be instances where the conflicts are such that the reviewer is unable to conduct the review, particularly where independence is an issue.

Conflicts may also arise during a review which may necessitate some action by the reviewer. In particular, a reviewer may be placed in a conflict situation where pressure is placed upon the reviewer to delay, change or provide early warning of findings. This may conflict with the interests of other parties relying on the compliance report.

Often the motivation behind this pressure is a desire to start the rectification process before the report is delivered to other parties including regulators. Reviewers will need to address the potential for these conflicts in the review plan as well as detail what action they will take. There is a clear expectation by regulators that, where a review is undertaken as part of an enforcement action, the reviewer will report any such pressure to it.

Reviewers must also consider what action they would take in the event that they become aware of a serious breach or potential breach which is outside the scope of the review. In some circumstances the potential conflict arises between the interest of the client and the public interest.

While unlikely to be a common event it is a matter that may cause the following considerations as to the actions to be taken:

- Not reporting the breach may be a breach of the law by the reviewer.
- It is likely in most cases the reviewer may think there is a breach though will not have enough evidence to prove it. Finding further evidence may be outside the scope of the review.
- Reporting a breach may compromise the review process, as staff of the regulated entity may become less helpful, as they will try to protect themselves and colleagues.
- If the reviewer reports the matter to management of the reviewed entity for their attention/action, is that enough to discharge the reviewer's obligation?
- Should the possibility of such a finding and the reporting of it be covered in the engagement letter and/or review plan?
- Should a benchmark such as "in the public interest" be used as the overriding principal to advise a regulator directly?
- Should issues like the awareness of the entity of the breach or the deliberate hiding of the breach be factors that should be added?

GLOSSARY

Existence

Framework is documented, compliance responsibility is clear, operational procedures are recorded and accessible, monitoring and supervision of procedures is identified and recorded, there is evidence of reporting and breach management.

Quality

The framework being reviewed is both efficient and effective. That is as at a current point in time the reviewer can confirm that at a certain agreed level the framework is achieving compliance, was able to achieve compliance or will be able to in the future in relation to the scope of the obligations being reviewed.

Current Point in Time

The compliance framework within the existing organisational structure, current personnel, current products and services and existing regulatory regime. There may be a little bit of movement but it will depend on the effectiveness of the framework to stand up to changes.

Ongoing Compliance

The ability of the framework to enable compliance in the future at agreed levels and within agreed changes to the environment.

Past Compliance

A review of whether the framework was able to ensure compliance to an agreed level over an agreed period.

5 ACI Resources

5.1 Accreditation

ACI offers a multi level accreditation program for Compliance Professionals. This rigorous program sets high standards against which all applicants are judged. The program is unique in its recognition of the extensive range of skills needed to effectively manage compliance.

5.2 Education

ACI provides training at several levels on 27 subject areas including risk management, compliance framework and policy development and change leadership. An extensive range of on-line material is also being organised.

ACI has a fully integrated learning centre which can be accessed at learning.compliance.org.au

5.3 Events & Activities

ACI will run over 60 events in 6 cities over the next 12 months. Members and non-members are welcome

One of the major programs is the benchmarking of organisations which is an ongoing program.

5.3.1 National Conference

The National Conference is held each year in September. The program is designed to push the frontier of thinking on compliance practices.

5.3.2 Regulators' Conference

This unique event is designed to improve the relationship between regulator and regulated and to explore better practice in regulator operations.

5.4 Library

ACI has an extensive on-line library of articles that have been written on compliance over the last 9 years. These are available free to members from the web site at www.compliance.org.au

5.5 Membership

ACI has members from all sectors of the economy including members from many regulatory agencies. Our philosophy is one of engagement and dialogue. You can join on-line at www.compliance.org.au or call the office on 02 9290 1788.

ACI: building integrity and trust