28-April-2008

To: The Board
Audit & Risk Committee

Through: Chief Executive Officer

From: Dushy Visvanathan

Compliance Plan and the Framework

Background
A compliance management framework has been in existence for some time. The framework is part of an overall Governance framework of the Institute.

Purpose
The objective of this report is to analyse the existing governance framework and recommend improvements to proactively manage the compliance risks associated with the Institute's business. This memo accompanies a report that comprehensively analyses compliance issues incorporating a plan. I believe the expansion of the framework is very much necessary to meet the dynamic nature of the compliance obligations.

ACI's compliance program is discussed in detail in terms of each of the principles of AS-3806 standard for compliance program.

Conclusion
ACI has a robust governance framework in place. This ensures the good governance of the Institute involving a risk management and compliance frameworks. ACI's constitution requires specific committees to be formed with delegated authority to manage its business activities.

It has been established that the framework does cover a depth of policies but lacks a robust monitoring mechanism

Recommendation
- Appoint a dedicated Compliance Officer with appropriate seniority who should have independence and access to Audit & Risk Committee.
- Direct the Chief Compliance Officer (CCO) to review the plan for appropriateness including sufficient controls.
- Ensure adequate monitoring mechanisms in place, including Key Risk and Control Indicators are developed.
- Direct the CCO to provide regular reports on the performance of the compliance plans.
- Direct the CCO to review and enhance the controls on a regular basis.

Australasian Compliance Institute

Compliance Management Framework

Auatralasian Compliance Institute

Australasian Compliance Institute (ACI) is a non-profit member based organisation which was established in October 1996. The Institute is the peak body for the development and practice of compliance and the integration of compliance, ethics, governance and risk into the fabric of organisations. The work of the Institute with a volunteer board and its approximately 1500 members has helped develop a dynamic, robust and compliant culture in the Australasian.

The Mission

ACI's vision is to provide relevant services that support members professionally and enable them to add value to their organisations through the delivery of an Accreditation and Education program that is accessible, affordable, credible, widely recognised and portable by engaging with external stakeholders to give members a voice to influence the environment in which they operate. ACI's values are Leadership, Courage, Integrity, Excellence and Teamwork, which make possible meeting the objectives.

Overview

ACI's vision is to be the peak body that develops a dynamic, robust and compliant culture in the Australasian region. Effective compliance and risk management framework is key to achieving this goal.

Compliance is defined as ensuring that activities undertaken agree with both the letter and the spirit of the standards, laws and/or regulations that govern a business or activity and the internal policies and procedures set down by that business for its own activities. (Gordano Knowledge Base).

Compliance Management Framework

Compliance management framework has been developed to guide ACI in meeting its compliance obligations, in addition to internal standards, policies and procedures. The framework operates within the core risk values and principles and inline with the AS 3806-2006 of Standards Australia for compliance.

ACI's compliance status is discussed below in terms of the 12 AS-3806 principles;

Commitment by governing body and top management

Effective commitment from the top management, including the board, governing body, chief executive and all levels of management to develop an effective compliance program. The top management's responsibility is to ensure the commitment is fully realised with clear and consistent message regarding the commitments to fulfil the compliance obligations by developing comprehensive policies, procedures and processes addressing not only the than the legal requirements but also for any other codes and agreements. The program has to be regularly reviewed and continuously improved. The commitment includes appointing a compliance officer with appropriate seniority and ensuring adequate compliance resources are in place. The top management also ensures accountability across all relevant management levels across the organisation.

ACI's constitution provides for a board elected by the members and is responsible for the governance. There are four specific committees formed with charters approved by the board to ensure the effective governance of ACI. Audit & Risk Committee is tasked with establishing and monitoring an effective compliance management framework that promotes a strong compliance culture. There is no dedicated Chief Compliance Officer but the CEO has responsibility as the Chief Compliance Officer and has direct access to the Board and Audit & Risk Committee. ACI's board commits to meet all the requirements of laws, regulations, industry codes and organisational standards and best practice by strictly adhering to the principles of Efficiency & Honesty, Competence, Management & Control and Financial Prudence. The Audit & Risk Committee ensures that the CEO, supported by the National Manager has the accountability to monitor, assess the compliance program and its continuous improvement. This involves review and approve the framework, monitor the performance of compliance risks and controls, ensure adequate processes are in place to manage regulatory change. Ethics committee oversees the complaints management and whistleblower systems. An independent audit function to review the design and operational effectiveness of the business activities and reports to Audit & Risk Committee.

Compliance Policy

Compliance policy should be aligned to the organisation's strategy supported by operational policies, procedures and processes. The policy must clearly articulate the commitment, scope, responsibilities and consequence of non compliance. The policy should emphasise the independence of the compliance function and be based on the specific local and regional obligations, organisation's objectives, values and the structure. Consideration should also be given to internal policies and standards, management of internal / external relationship, integration of compliance with risk, audit and legal functions and embedding compliance into operational processes and systems. The policy should be widely available and readily available to all employees.

ACI's compliance framework is an integral part of the institutes overall governance framework. The compliance policy assigns responsibility to all levels of managers from CEO, although the policy des not adequately maintain the independence of the compliance function by appointing a dedicated senior compliance officer. The institute's annual business plans do accommodate requirements from compliance program. All institute's members and staff are expected to strictly adhere to the standards set in terms of applicable laws, regulations, codes and organisational standards. This expectation also includes external partners, outsourcing arrangements and any other parties. Any breaches of the compliance policy may result in action and/or termination.

Resources

Appropriate and adequate resources are to be made available for the development of effective compliance program and maintain and improve the program for achieving successful compliance.

The institute is committed to maintain adequate human and technological resources for the compliance function. This includes adequate resources, reference material and training for ongoing maintenance of the compliance function and facilitated by the annual planning and budgeting process.

Compliance Objectives & Strategy

Clear, time related objectives should be set and aligned with overall strategic objectives. The compliance strategy should include structure of the program, roles & responsibilities, resources, priorities, monitoring & measuring and be embedded into operational practices and processes. Individual performance agreements should compliance objectives and linked to remuneration.

An operational compliance plan is in place with the obligations and the monitoring and reporting mechanism to ensure the effectiveness of the program. The CEO and the National Manager participate in meetings to review the compliance strategy that includes resourcing and prioritising. The institute's members and staff have clear accountability for the compliance responsibility with specific reference within position descriptions and performance reviews.

Identifying and assessing compliance obligations

Organisations should systematically identify compliance obligations and proactively manage regulatory and other changes by putting in place a structured approach. Compliance obligations are to be assessed and ranked and resources are to be allocated to mitigate any potential failures.

The risk management framework of the institute identifies, assesses and ranks the compliance risks and reporting mechanism is in place to escalate serious breaches. The CEO monitors significant changes in laws, regulations and industry codes and ensures appropriate actions are taken.

Assignment of responsibilities for positive compliant outcomes

Top management and governing body should ensure commitment to compliance is always upheld by active involvement & supervision and appointing a senior independent compliance person with access to CEO and the board. This includes allocating appropriate resources and ensuring effective and timely reporting. Depending on the size of the organisation, a compliance manager should be appointed with appropriate skills to cast the responsibilities such as identifying, monitoring and reporting compliance obligations and providing training to business managers. Business managers should cooperate and support the compliance manager in achieving the desired compliance outcomes. Outsourcing arrangements do not relieve compliance obligations to the organisation and the compliance program sufficiently address the issues.

The Audit & Risk Committee oversees the compliance function in which the CEO is accountable for monitoring the performance of the compliance program and adequate resourcing. ACI's National Manager has a specific task as a compliance officer and facilitates in developing individual business unit policies and procedures in line with ACI's governance framework. This includes regular communication to all staff and providing relevant training. Individual staff members are responsible for ensuring compliance within their area of accountability.

Competence & Training

All employees have compliance obligations and should be competent to discharge responsibilities effectively. Training should be in-line with the organisation's compliance culture and commitment. The training requirements are to based on knowledge gaps and should be aligned to corporate training framework.

Staff education and training are the responsibility of the National Manager. Individual training programs are developed appropriately to address knowledge gaps.

Promoting compliance behaviours

Top management and governing body should ensure appropriate compliance behaviours are promoted by aligning to the strategic objectives by encouraging and rewarding the positive compliance behaviours. This includes creating environment for reporting issues. .The development of compliance culture with compliance performance within job descriptions, induction program, training with pre-employment screening.

The institute has a complaint handling process that is in accordance with the Australian standard AS-4629. The staff has accountability to ensure compliance part of the performance review process. CEO and the National Manager ensure the right culture is maintained within the institute by overseeing and put in place a coaching and mentoring program.

Controls

Effective controls are to be in place to manage compliance obligations. These include documented policies, procedures, systems, monitoring of exception reports, segregation of duties and appropriate system access controls. Controls are to be periodically evaluated for their effectiveness and measured and reported of their performance.

The institute's governance framework stipulates that reasonable care to organise and control it affairs responsible and effectively, including implementing an adequate risk management and supervisory system and maintaining appropriate corporate governance standards. This involves fulfilling its financial commitments and where possible compliance is embedded within the operating policies and procedures and day-to-day activities.

Monitoring & Measuring

Organisations are required to have mechanism to monitor and report compliance program and its performance, including the compliance culture, resourcing, identification of obligations, issues, the effectiveness of the controls.

The institute has both formal and informal process to monitor the compliance program. The CEO and the National Manager conducts regular monitoring of the compliance program and provides reports to

the board and the Audit & Risk Committee, including performance statistics. Standard reporting protocols are in place to escalate issues appropriate with mitigation strategies.

Record-Keeping

Accurate and up-to-date records of the compliance activities should be maintained and appropriately stored to assist in the compliance monitoring and review process. The records include failures, complaints, near misses etc.

The institute has complaints management system that is compliant withAS-4629 standard. In addition to this, a risk register is maintained along with a centralised data collection process for breaches.

Continual Improvement

Top management should ensure that the organisation's compliance program is reviewed regularly to ensure its effectiveness. Corrective actions must be taken to address any issues.

The institute undertakes an annual review of its compliance program to ensure the effectiveness and appropriateness of the program.

Compliance Plan

A compliance plan is a document that sets out procedures put into place to ensure all business operations are within its legislative, statutory, standards or contractual obligations. The business managers will be fully responsible and accountable under the Australian Standard AS-3806 for compliance and ACI's compliance policy. The business managers ensure compliance by implementing controls and procedures to address the compliance risks and obligations.

The compliance plan for ACI has been developed in consultation with Legal counsels to address the following objectives;

- Identify ACI's compliance obligations,
- Identify the key risks,
- Identify and establish controls and assign ownership,
- Regular assessment of the risks and controls,
- Monitoring and reporting of the performance of the compliance plan.

Legislation / Internal Policy

The following are some of the laws, regulations and codes that govern ACI supplemented by internal policies, procedures and guidelines.

Laws & Regulations

- Australian Standards
- Associations Incorporation Act (NSW)

- Privacy Act (Commonwealth)
- Spam Act (Commonwealth)
- Anti-Discrimination Act 1977 (NSW)

Internal Policies

- Constitution
- Governance Framework
- Code of Conduct
- Technology Code of Use
- Records Management
- Discrimination & Harassment
- Conflicts of Interest
- Gifts & Hospitality
- Whistle Blower Protection
- Employee Guidelines
- Health & Safety

Risk Assessment

ACI's compliance obligations are identified and assessed for the likelihood of breaches and their impact. The risk assessment process identifies and/or develops necessary controls and monitors the performance of their design and operational effectiveness.

Monitoring & Review

Compliance plans will be reviewed annually or whenever material legislative or business change occurs.

Compliance obligations are continually monitored for appropriate risk rating and the performance of the controls. The assessment includes the following;

- Any internal incidents and issues
- Any external incidents and issues
- Action plan to enhance the controls
- Any changes in legislative requirements
- Any changes in the business

1. AS 3806 – 2006 Compliance Frameworks

Purpose

Compliance Framework that meets the requirements set out in AS 3806 (2006)

External legislation / Regulation

AS 3806 (2006)

Internal Policy / Process / Training

Overall control assessment (RI/Q/E)

Effective

Risk assessment

Impact: Insignificant Likelihood: Extremely Rare Residual risk: Low

Obligation	Key Risks	Procedures/Controls	Control Effectiveness	Monitoring	Frequency	Responsible Manager/Area	Date last reviewed
'Buy in' for the compliance function from Senior Management / Executives To have sufficient personnel and systems resources Access to adequate resources including legal advice and compliance specialists A framework (including compliance plans) based on AS 3806	Regulatory and external audit risks Lack of knowledge around legislation and obligations Inadequate or incorrect controls and procedures in place	Compliance Framework and Group framework which is reviewed by all stakeholders annually	**Effective**	Audit & Risk Committee monitors completion of annual reviews of Group policies; annual review of Compliance framework	Annually		
		Training for compliance employees – quarterly seminars etc	**Effective**	Adhoc review of the training calendar	Quarterly		
		Master plan to give consistency and aid the regulatory change process	**Effective**	Ensure all business line plans are reviewed annually	Annually		
		Audit review of the framework and compliance plans (internal and external)	**Effective**	Internal Audit to provide an annual compliance framework report	Annually		
		Regulatory Change Program	**Qualified**	No formal procedure. Ensure monthly completion	Monthly		

2. Adequacy of Resources

External legislation / Regulation	Associations Incorporation Act (NSW)
Internal Policy / Process / Training	Training Governance Framework
Overall control assessment (RI/Q/E)	Effective
Risk assessment	Impact: Insignificant Likelihood: Extremely rare Residual risk: Low

Obligation	Key Risks	Procedures/Controls	Control Effectiveness	Monitoring	Frequency	Responsible Manager/Area	Date last reviewed
To ensure there are adequate human, financial and technological resources to service members key persons meet all requirements as documented in the relevant legislation	Associations Incorporation Act (NSW) Reputational Risk Regulator audit or enforceable undertaking Public liability insurance claims	Medium and long term business planning and budget setting	**Effective**	Annual financial budgeting exercise	Annual		
		Assessment of staffing and systems for future operational needs	**Effective**	National Manager responsible for monitoring of Resourcing and systems	Annual		
		Employee and senior manager succession planning	**Effective**	Annual review of the succession planning process	Annual		
		Ensure delegations of authority are reviewed periodically and are appropriate and up-to-date	**Effective**	Review documented delegations	Annual		

3. Ethical Behaviour

To promote honest and ethical business conduct towards members, suppliers and competitors

Purpose

External legislation / Regulation

Associations Incorporation Act (NSW)
Spam Act 2003

Internal Policy / Process / Training

Ethical framework
Code of Conduct and Values

Overall control assessment (RI/Q/E)

Effective

Risk assessment

Impact: Insignificant Likelihood: Extremely Rare Residual risk: Low

Obligation	Key Risks	Procedures/Controls	Control Effectiveness	Monitoring	Frequency	Responsible Manager/Area	Date last reviewed
ACI must conduct business with its member, suppliers and competitors in an honest manner at all times	Non compliance of Trade Practices Act.	All employees have undertaken the training required by their job profile	**Qualified**	Stock take of staff accreditation. No formal role specific accreditation program.	Monthly		
We must not engage in price fixing, third line forcing, or dishonest or misleading conduct etc	Reputational risk.	Breaches are raised and recorded through Risk register	**Effective**	Ensure all issues and incidents are recorded in the Risk register	Monthly		
	Potential for large fines and legal action	All employees are aware of, and abide by the Gifts and Hospitality Policy	**Effective**	Undertaken in team meeting	Annually		

4. Business Continuity

Purpose

Business Continuity Planning

External legislation /Regulation

Associations Incorporation Act (NSW)

Internal Policy / Process / Training

Policy / Process / Training

Overall control assessment (RI/Q/E)

Effective

Risk assessment

Impact: Insignificant Likelihood: Extremely Rare Residual risk: Low

Obligation	Key Risks	Procedures/Controls	Control Effectiveness	Monitoring	Frequency	Responsible Manager/Area	Date last reviewed
		Change process in place to ensure that as business changes take place that change requests are submitted to facilitate that change.	**Effective**	Awareness of change procedures, evidence they have been followed	Annually		
		Formal roles and responsibilities are in place and BCP support managers and co-ordinators have been trained and that management is aware of their responsibilities.	**Effective**	Awareness of role and responsibility, attendance at training.	Annually		

5. Internal Policies

Purpose

Internal Policy – all employees must be made aware of and have access to all internal policies and procedures, and to follow the Code of Conduct at all times

External legislation / Regulation

All

Internal Policy / Process / Training

All internal policies (particularly Code of Conduct and Technology Code of Use)
Induction training / Governance framework, Employee Guidelines

Overall control assessment (RI/Q/E)

Effective

Risk assessment

Impact: Insignificant Likelihood: Extremely Rare Residual risk: Low

Obligation	Key Risks	Procedures/Controls	Control Effectiveness	Monitoring	Frequency	Responsible Manager/Area	Date last received
All employees are to follow all internal policies and procedures at all times to ensure ongoing compliance	Likely breaches of compliance and legislative requirements	Reference in procedures as appropriate. Agenda items in team meetings as appropriate	**Effective**	Procedures reviewed by legal and / or compliance representatives	Annually		
The Code of Conduct is to be followed at all times	Legal and regulatory risk	Policies are listed on the intranet site.	**Effective**	Intranet site page is reviewed by Group Op. Risk and Compliance	Twice yearly		
Up to date copies of all corporate policies must be freely available on the ACIintranet	Reputational risk Poor member service and retention	Training materials and policies are regularly reviewed and when significant regulatory changes take place	**Effective**	Changes to training programs and assessments are monitored by Learning Logistics	Annually		

9. Safety and Wellbeing / OHS

Purpose

To ensure the safety and wellbeing of all employees and visitors to office locations

External legislation / Regulation

Occupational Health and Safety Act 2000 Pt 2, Division 1, 2 & 3.
Workcover Acts (state based)

Internal Policy / Process / Training

Health & Safety Policy

Overall control assessment (RI/Q/E)

Effective

Risk assessment

Impact: Insignificant Likelihood: Extremely Rare Residual risk: Low

Obligation	Key Risks	Procedures/Controls	Control Effectiveness	Monitoring	Frequency	Responsible Manager/Area	Date last reviewed
		discussed in team meetings.		agenda item in team meetings twice a year	Six monthly		
		manual available if system is down. Both online and paper versions of reporting are available	**Effective**	manual reporting template and confirm bi-annually	Six monthly		
		Emergency contacts and evacuation procedures displayed in relevant areas.	**Effective**	confirm annually	Annually		

10. Discrimination and Harassment

Purpose

To prohibit discrimination & harassment in the workplace, and to ensure all employees are treated equally and not discriminated against on the basis of gender, age, background, religion, sexual preference, disability etc

External legislation / Regulation

Anti-Discrimination Act 1977
Disability Discrimination Act 1992

Internal Policy / Process / Training

Equal Opportunity and Non-discrimination Policy
Anti-bullying Policy
Code of Conduct

Overall control assessment (RI/Q/E)

Effective

Risk assessment

Impact: Insignificant Likelihood: Extremely Rare Residual risk: Low

Obligation	Key Risks	Procedures/Controls	Control Effectiveness	Monitoring	Frequency	Responsible Manager/Area	Date last reviewed
		Discrimination & Harassment is discussed in team meetings.	**Effective**	Discussed in team meetings and recorded on the Compliance Calendar	Six-monthly		
		Breaches are managed as per guidelines.	**Effective**	breach reporting to Risk and Compliance management	Monthly		
		Employee Guidelines has a Grievance Process for employees with issues Employees have access to concern online for confidential reporting	**Effective**	employee issues raised under the Grievance Process	Event		

11. Privacy

To ensure the privacy of member information by only using this data for the purposes as prescribed by the National Privacy Principles

Purpose

External legislation / Regulation

Privacy Act 1988 Pt 2 6A, 16A, 8 & 9
National Privacy Principles

Internal Policy / Process / Training

Privacy Policy, Information Security Policy

Overall control assessment (RI/Q/E)

Effective

Risk assessment

Impact: Insignificant Likelihood: Extremely Rare Residual risk: Low

Obligation	Key Risks	Procedures/Controls	Control Effectiveness	Monitoring	Frequency	Responsible Manager/Area	Date last reviewed
		Breaches are raised and recorded through incidents register.	**Effective**	Updates form the register	Monthly		
		Standard correspondence content is signed off by legal, and Risk and Compliance before being used	**Effective**	Documents are not loaded to relevant Standard Letters system / Documentation site until all relevant approvals are obtained	Event		
		Privacy policy available on the ACIwebsite	**Effective**	Check to ensure up-to-date info	Annually		

13. Systems Use / Technology Code of Use

Purpose

To ensure that employees only use systems and hardware for the permitted work purpose, and follow the Technology Code of Use at all times

External legislation / Regulation

Privacy Act,

Internal Policy / Process / Training

Technology Code of Use, Code of Conduct, Information Security Policy
Privacy Policy etc

Overall control assessment (RI/Q/E)

Effective

Risk assessment

Impact: Insignificant Likelihood: Extremely Rare Residual risk: Low

Obligation	Key Risks	Procedures/Controls	Control Effectiveness	Monitoring	Frequency	Responsible Manager/Area	Date last reviewed
		Technology Code of Use sign off	**Effective**	monitor training	Monthly		
		Logging of staff internet usage	**Effective**	Breaches of the Code will be monitored on an exception basis	Exception Basis		
		Password and physical security (such as locks) for laptops	**Effective**	Compliance to check on an ongoing basis	Quarterly		
		Ensure secure access to service provider/vendor systems eg: Token security	**Effective**	ISG	Quarterly		

16. Conflicts of Interest

To avoid or manage conflicts of interest, and to minimise instances of insider trading. Also to ensure provisions on continuous disclosure are met.

Purpose

External legislation / Regulation

Associations Incorporation Act (NSW)

Internal Policy / Process / Training

Etics Framework,

Overall control assessment (RI/Q/E)

Effective

Risk assessment

Impact: Insignificant Likelihood: Extremely Rare Residual risk: Low

Obligation	Key Risks	Procedures/Controls	Control Effectiveness	Monitoring	Frequency	Responsible Manager/Area	Date last reviewed
To avoid conflicts of interest / insider trading.	Fines and legal action Breach leading to regulator actions	All employees have access anonymous reporting and whistleblower policy.	**Effective**	Monitor the process	Six monthly		
To manage conflicts of interest		Gift policy to be acknowledged by employees. Recording of any gifts from a service provider in gifts register.	**Effective**	Policy to be discussed in team meeting and recorded on the Compliance Calendar	Annually		

Acknowledgements

- Gordano Knowledge Base
- ACI Website
- Westpac Banking Corporation - Compliance Framework
- Australian Pipeline Trust – Compliance Plan
- J B Were Global High Yield Wholesale Fund – Compliance Plan