

The Australian Compliance Institute's Quick Guide to Culture, Ethics, Governance, Compliance, Risk and Corporate Social Responsibility



ACI – Supporting you, your organisation, your profession

Principal Members

The Australian Compliance Institute would like to thank our Principal Members for their support.



© Copyright 2024 The Australian Compliance Institute. All rights reserved.

This material may not be copied or reproduced in any form except with the written permission of the owner of the copyright.

Introduction

Welcome to the Fourth edition of the Quick Guide to Culture, Ethics, Governance, Compliance, Risk and Corporate Social Responsibility. We trust that you will find this guide to be an insightful and practical tool for your organisation and staff. We believe that this important publication is an effective platform for generating awareness and discussion around these key topics and for communicating the value that compliance, ethics, governance, risk and corporate social responsibility can bring to any organisation.

Over the past 20 years since ACI's inception, we have seen a significant growth and evolution of the compliance and risk profession across all industries and organisations whether in the private, public or not for profit sector. As a result of recent global economic challenges, business and government alike have realised the essential role that GRC professionals can play within the organisation, and the benefits that an effective compliance culture can have on long term sustainability and success.

Community and consumer expectations on an organisation's conduct, ethical behaviour, and environmental footprint, as well as the ever-changing regulation and increasing Directors' liability continues to highlight the importance of good governance.

In light of this, ACI believes that there are five key elements that are essential in establishing an effective compliance and risk framework:

Cultural elements – An organisation's tone from the top, support and direction from Directors and senior management, perceptions and response to compliance and risk overall.

Structural elements – The organisation's strategic positioning of compliance and risk within its business.

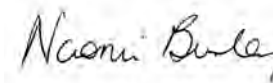
Operational elements – How compliance and risk is 'done' within the organisation in terms of processes and procedures.

Implementation elements – How compliance and risk procedures are identified and put into place.

Maintenance elements – How the compliance and risk framework is maintained, reviewed and improved.

In line with the above philosophy, the Quick Guide poses a series of key questions for you to consider in the context of your own workplace, to help identify and assess your own organisation's approach to these core areas. In effect, the questions act as a 'health check' for your organisation and are a valuable tool in helping to assess your organisation's level of activity and commitment to these areas, whilst providing some suggestions to the way in which you can achieve the greatest impact on your business.

We trust that you will enjoy reading this guide and find it of value.



Naomi Burley
Managing Director

Culture



An organisation's culture is the body of learned behaviours, which act as a template, shaping future behaviour. The formation, maintenance and change of culture is complex. Each organisation's culture is unique as is the existence of sub-cultures.

Culture is a function of the organisation's history, mythology, structure, industry and, most critically, leadership. Culture is a complex amalgam of ethics, values, risk appetite, structures, systems, leadership, controls, freedom, authority and accountability.

An appropriate culture reduces the level of controls required to ensure performance.

A defective culture will subvert even the most rigorous systems and processes.

Culture questions to ask yourself and your key managers:

- 1 Is there an open board culture which promotes active thinking, robust discussion, and challenging (where appropriate) of management reports?
- 2 Have you articulated the attributes of the culture you want and identified the gaps between that and what exists?
- 3 What percentage of staff at all levels believe they can raise issues without fear of retribution?
- 4 What percentage of staff believe managers do what they say?
- 5 Do your organisation's codes, words and actions of senior management align with the desired culture?
- 6 Are there key pockets of negative culture that impact adversely on behaviour and increase risk?
- 7 Are staff at all levels treated in the same manner for their successes and failures?
- 8 Have you implemented a confidential hotline to facilitate the communication of issues, complaints and allegations? If so, is it effective in dealing with the issues and reporting the results?



Ethics



Ethics provide the overarching principles and rules which govern individual and organisational behaviour. These rules are normally documented in a values statement and reflected in policies, procedures and expected behaviours.

An organisation with a strong ethical base is less likely to breach legal obligations, particularly where the law or circumstances are ill-defined, or where there is considerable variability in the circumstances that are likely to be encountered.

While an organisation will have cultures appropriate to the various functions, it can have only one set of values.

The outcome from a coherent set of values is an increase in stakeholder trust leading to lower costs of doing business, ease in raising capital and greater market appeal.

Ethics questions to ask yourself and your key managers:

- 1 Do you have a values statement, or code of conduct, that is clear and precise, which sets out the true values of your organisation (and is not simply a wish list full of 'motherhood' statements, or a statement of your personal values)?
- 2 Does the code reflect and align with the mission and vision and support the organisation's goals, ambitions and desired behaviours?
- 3 When was the code last issued or reviewed and does it carry the signatures of the current chairman and CEO?
- 4 Do all staff receive training on the code on induction and periodically thereafter?
- 5 What percentage of staff believe management (at all levels) adhere to the spirit and letter of the code?
- 6 What do employees feel is more important; meeting budget, or doing the right thing?
- 7 Do staff believe their leaders keep their promises?
- 8 Do Board members, managers, employees at all levels and other stakeholders feel free to raise ethical questions without fear of ridicule or retribution?
- 9 Do you have a whistleblower protection program that staff trust and feel comfortable using?



Governance



Governance is the system by which organisations are directed and controlled, involving the allocation of rights and responsibilities across all constituencies including the Board, management, staff, shareholders and other stakeholders.

Governance provides the rules for decision making and accountability – setting levels and measurement of performance against objectives – the structure and the compliance requirements, ranging from mandatory to discretionary.

The process by which performance against objectives and obligations is met, authority is delegated and monitored and control over the creation, effectiveness and efficiency of organisational systems and structures is maintained.

Governance questions to ask yourself and your key managers:

- 1 Is there a process for ensuring effective levels and distribution of Board competence and independence?
- 2 Are there effective Board committees for compliance, ethics and risk?
- 3 Are the Board processes clearly documented and have they been reviewed for effectiveness?
- 4 Are there clear delegations to staff of their authority, responsibility, accountability and reporting obligations?
- 5 Are people adequately trained to implement their delegations?
- 6 Does your compliance system address performance against the delegations?
- 7 Is there active cooperation and coordination between compliance, ethics and risk management to avoid duplication?
- 8 Do you have an effective integrated software solution for managing and reporting compliance, ethics, governance and risk issues?



Compliance



Compliance is the process by which organisations identify and meet their strategic obligations whether arising in law, standards, codes of practice or from stakeholder expectations.

Focusing on legal obligations in isolation results in a minimalist and narrow approach, which cannot leverage an organisation's ability to efficiently manage all aspects of compliance.

The Board should articulate the compliance philosophy and ensure adequate seniority, level of authority and support is given to the compliance function.

Compliance questions to ask yourself and your key managers:

- 1 Does the Board issue the compliance policy and endorse the compliance plan?
- 2 Is there a Board or management compliance committee?
- 3 Are your Board and senior management knowledgeable about the content and operation of your compliance program and do they oversee and monitor its implementation and effectiveness?
- 4 When was the compliance policy last reviewed and issued?
- 5 Does the person responsible for compliance have sufficient seniority and authority and have direct access to the Board and CEO?
- 6 Regardless of structure, (centralised or decentralised), is compliance independent of operational and business drivers?
- 7 Is the compliance program sufficiently integrated into the organisation so that business units and all staff can understand, perform and be assessed against, their compliance obligations?
- 8 Are the compliance requirements, rules, structures, resources, policies and procedures documented and implemented across the organisation?
- 9 Is compliance training integrated into induction and the annual training plan for all staff?
- 10 Are compliance obligations included in each staff member's position description?
- 11 Does compliance form part of business key performance indicators?





Risk Management

The purpose of risk management is to identify potential events that may impact on an entity, quantify the impact and likelihood of occurrence and then manage the risk in accordance with the organisation's risk appetite.

Risk appetite – the amount of risk an organisation will assume in pursuit of its goals – this should be defined by each organisation.

The risk appetite should be aligned to the risk culture, particularly as the risk appetite of different functions and individuals will impact on the adherence to the official (accepted) 'appetite stance'.

Organisations, even with extreme risk appetite, cannot deliberately choose to ignore the law. They may however allocate less resources to ensure strict compliance.

There is no one risk model.

Risk questions to ask yourself and your key managers:

- 1 Is the organisation's risk appetite clearly defined, aligned to the risk culture and clearly communicated across the organisation?
- 2 Is the process used for identifying risks supported by a system for managing compliance with the risk management plan?
- 3 Is there a common language and set of metrics for assessing likelihood and impact/severity to allow comparability across functions and levels?
- 4 Do all staff have appropriate training to understand the risks involved in their role and to manage them in accordance with the risk plan?
- 5 Does the risk policy contain procedures for disciplining breaches of policy?
- 6 Does the risk policy state that the organisation will not tolerate deliberate or negligent breaches of laws and regulations?
- 7 Does your risk management plan cover financial, capital, operational and strategic risks?
- 8 Does your organisation understand that risk management is not about eliminating risk taking, but managing the risk taken in an informed environment?
- 9 Is your risk management reporting system likely to give you early warning of a pending catastrophe?



The Australian Compliance Institute is the peak professional body for compliance professionals across Asia Pacific, providing support to individuals and their organisations. We serve our members by:

Advocacy

Engaging with government and key regulators to reduce compliance costs and encourage balanced and pragmatic regulation. Assisting members to communicate their issues and concerns through the facilitation of ACI working groups and committees.

Career Development, Accreditation, Training and Education

Providing excellent career development opportunities and training through our innovative National Recognised Training (Cert IV & Grad Cert), our highly respected Professional Accreditation and our events, seminars, Annual Conference and our tailored in-house training programs offering all facets of compliance and risk.

Benchmarking and Research

Conducting research and benchmarking across industry sectors in the areas of compliance, governance, risk, ethics, corporate social responsibility internationally such as the Compliance Salary Survey and Compliance Benchmarking Maturity Model.

Publications and Tools

ACI works in conjunction with their partners to provide exclusive discounts and special offers for members on compliance and risk solutions.

Networking

Providing valuable opportunities to network with international GRC professionals.

Investment in your profession

ACI is a not-for-profit organisation. All revenue and earnings from ACI membership, events and activities are reinvested back into the Institute to fund the development of additional benefits, tools and resources to help support compliance and risk professionals. Funds are also reinvested to enable ACI's work in advocacy and education within the business community regarding the importance of compliance and risk management.

The Professional

How a good compliance professional can add value to the business

Organisations are increasingly taking advantage of the true value-add that a trained and accredited compliance professional brings to corporate decision making and the bottom line.

Factors such as complexity and sophistication of products and services, distribution channels, customer demands and unprecedented advances in technology have resulted in increased political and regulatory intervention into business.

Compliance professionals are at the forefront of these changes. They have a broad understanding of the businesses and industries in which they operate and take the role of a trusted adviser and consultant to the business.

Compliance professionals assist with the simplification of complex requirements. This unique skill can enable the business to manage costs and risk without jeopardising the achievement of strategic business outcomes.

The compliance professional also provides support and leadership at times of challenge and crisis. One major value add that a compliance professional delivers is their contribution as a cultural change agent. They influence behaviour at all levels of the organisation. They help deliver assurance that the culture of the organisation includes ethical considerations about what is fair and just for all stakeholders. Compliance professionals help balance regulatory and ethical requirements and the achievement of corporate goals.

Supporting and engaging staff to do what is right not just because it is the law is a key contribution a compliance professional can make, and compliance professionals are able to embed this message into the organisation.

This increases investor confidence; protects and enhances brand and reputation; and increases employee retention and productivity while building loyalty and trust.

The trained and accredited compliance professional is a key player in modern corporate governance, risk management, ethical trading, responsive regulation, corporate social responsibility and best practice in compliance and risk.

ACI – Supporting you, your organisation, your profession



The Australian Compliance Institute

ABN 42 862 119 377

Ph +612 92901788

PO BOX R268, 38-40 Pitt Street, Sydney,
NSW, 2000

compliance.org.au