AS 3806—2006

Australian Standard™

Compliance programs

STANDARDS Australia

This Australian Standard was prepared by Committee QR-014, Compliance Systems. It was approved on behalf of the Council of Standards Australia on 23 January 2006.
This Standard was published on 9 March 2006.

The following are represented on Committee QR-014:

Australian Competition and Consumer Commission
Australian Compliance Institute
Australian Record Industry Association
Australian Securities and Investments Commission
Australian Taxation Office
Consumers' Federation of Australia
Law Council of Australia
Society of Consumer Affairs Professionals
The Institute of Internal Auditors – Australia
University of Western Sydney

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Web Shop at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Global Standard*, has a full listing of revisions and amendments published each month.

Australian Standards™ and other products and services developed by Standards Australia are published and distributed under contract by SAI Global, which operates the Standards Web Shop.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to the Chief Executive, Standards Australia, GPO Box 476, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 04505.

Australian Standard™

Compliance programs

Originated as AS 3806-1998.
Second edition 2006.

Published by Standards Australia, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 7296 X

PREFACE

This Standard was prepared by the Standards Australia Committee QR-014, Compliance Systems to supersede AS 3806—1998.

This Standard was initially developed following a request from the Australian Competition and Consumer Commission.

The Standard provides principles for the development, implementation and maintenance of effective compliance programs within both public and private organizations. These principles are intended to help organizations identify and remedy any deficiencies in their compliance with laws, regulations and codes, and develop processes for continual improvement in this area.

CONTENTS

Page

FOREWORD

Compliance is an outcome of an organization meeting its obligations. Policies and procedures to achieve compliance must be integrated into all aspects of how the organization operates. Compliance should not be seen as a stand-alone activity, but should be aligned with the organization's overall strategic objectives. An effective compliance program will support these objectives. Compliance should, while maintaining its independence, be integrated with the organization's financial, risk, quality, environmental and health and safety management systems and its operational requirements and procedures.

An effective organization-wide compliance program will result in an organization being able to demonstrate its commitment to compliance with relevant laws, including legislative requirements, industry codes, organizational standards as well as standards of good corporate governance, ethics and community expectations.

An organization's approach to compliance should be shaped by its core values and generally accepted corporate governance, ethical and community standards.

Failure to embrace the above values at all levels of an organization's operation risks exposing that organization to a compliance failure. On numerous occasions the courts have considered an organization's commitment to compliance when determining the appropriate penalty to be imposed for contraventions of relevant laws. While the Standard sets out the principles required for an effective compliance program, the implementation and management elements of the program will not be the same for all organizations due to their size, structure and nature of their activities.

STANDARDS AUSTRALIA

Australian Standard
Compliance programs

SECTION 1 SCOPE AND GENERAL

1.1 SCOPE

This Standard provides principles and guidance for designing, developing, implementing, maintaining and improving a flexible, responsive, effective and measurable compliance program within an organization.

Section 2 sets out the essential principles which will be common to all effective compliance programs. Sections 3 to 6 contain guidance regarding those principles, recognizing that the implementation and management of an effective compliance program which complies with those principles will differ for each organization depending on the size, nature and complexity of its operations and its specific circumstances.

This Standard is designed to complement the documents listed in the Bibliography at Appendix A.

1.2 OBJECTIVE

The objective of this Standard is to provide principles and guidance for organizations designing, developing, implementing, maintaining and improving an effective compliance program.

1.3 DEFINITIONS

For the purpose of this Standard, the definitions below apply.

1.3.1 Code

A statement of recommended practice developed internally by an organization or by an international, national or industry body or other organization.

NOTE: The code may be mandatory or voluntary.

1.3.2 Competence

Application of knowledge, understanding and ability to a work related task to achieve an acceptable level of performance.

1.3.3 Compliance

Adhering to the requirements of laws, industry and organizational standards and codes, principles of good governance and accepted community and ethical standards.

1.3.4 Compliance culture

The values, ethics and beliefs that exist throughout an organization and interact with the organization's structures and control systems to produce behavioural norms that are conducive to compliance outcomes.

1.3.5 Compliance failure

An act or a omission whereby an organization has not met its compliance obligations, processes or behavioural obligations.

1.3.6 Compliance program

A series of activities that when combined are intended to achieve compliance.

1.3.7 Employee

Person, whether remunerated or not, working on an organization's behalf including part time staff, fulltime staff, sub-contractors, temporary staff and volunteers.

1.3.8 Governing body

The body of one or more people who have overall accountability, responsibility and authority for the direction and control of the organization.

1.3.9 Organization

A company, firm, enterprise or association (including a government body), whether incorporated or not.

1.3.10 Organizational and industry standards

Documented codes of ethics, codes of conduct, good practices and charters that an organization has adopted for its operations.

1.3.11 Regulatory authority

Any government body or other organization responsible for regulating or enforcing compliance with legislative and other requirements.

1.3.12 Top management

The level of management within an organization directly accountable to its governing body, shareholders or the owner.

SECTION 2 COMPLIANCE PRINCIPLES

2.1 COMMITMENT

The principles supporting the compliance program that relate to commitment are as follows:

Principle 1: Commitment by the governing body and top management to effective compliance that permeates the whole organization.

Principle 2: The compliance policy is aligned to the organization's strategy and business objectives, and is endorsed by the governing body.

Principle 3: Appropriate resources are allocated to develop, implement, maintain and improve the compliance program.

Principle 4: The objectives and strategy of the compliance program are endorsed by the governing body and top management.

Principle 5: Compliance obligations are identified and assessed.

2.2 IMPLEMENTATION

The principles supporting the compliance program that relate to implementation are as follows:

Principle 6: Responsibility for compliant outcomes is clearly articulated and assigned.

Principle 7: Competence and training needs are identified and addressed to enable employees to fulfil their compliance obligations.

Principle 8: Behaviours that create and support compliance are encouraged and behaviours that compromise compliance are not tolerated.

Principle 9: Controls are in place to manage the identified compliance obligations and achieve desired behaviours.

2.3 MONITORING AND MEASURING

The principles supporting the compliance program that relate to monitoring and measuring are as follows:

Principle 10: Performance of the compliance program is monitored, measured and reported.

Principle 11: The organization is able to demonstrate its compliance program through both documentation and practice.

2.4 CONTINUAL IMPROVEMENT

The principle supporting the compliance program that relates to continual improvement is as follows:

Principle 12: The compliance program is regularly reviewed and continually improved.

SECTION 3 COMMITMENT

3.1 PRINCIPLE 1

Commitment by the governing body and top management to effective compliance that permeates the whole organization.

Effective compliance requires an active commitment from top management, including the board or governing body and chief executive. The level of commitment is indicated by the degree to which:

(a) The governing body, chief executive and all levels of management actively demonstrate commitment to designing, developing, implementing, maintaining and improving an effective compliance program.

(b) The Chief Executive Officer takes responsibility for ensuring that the commitment of the organization is fully realized.

(c) Management consistently conveys to employees the clear message that the organization will meet its compliance obligations, and that lip-service does not constitute compliance.

(d) The compliance manager is given a level of seniority which reflects the importance of effective compliance.

(e) The level of resources are allocated to developing, implementing, maintaining and improving a robust compliance culture.

(f) The organization assigns and requires accountability for compliance to relevant management levels across the organization.

(g) Comprehensive policies, procedures and processes are developed that make compliance readily understandable and achievable.

(h) Policies, procedures and processes reflect not just the legal requirements, but voluntary codes and the organization's values.

(i) The commitment is communicated widely in clear and convincing statements supported by action.

(j) Regular review of the compliance program is required.

(k) Continually improving its compliance performance is valued.

3.2 PRINCIPLE 2

The compliance policy is aligned to the organization’s strategy and business objectives, and is endorsed by the governing body.

3.2.1 Purpose

The compliance policy establishes the overarching principles and commitment to action for an organization with respect to achieving compliance. It sets the level of responsibility and performance required within the organization against which actions will be assessed. The policy should be appropriate to the organization’s compliance obligations that arise from its activities and the products or services that it provides.

The policy is not a stand-alone document but is supported by other documents including operational policies, procedures and processes.

3.2.2 Content

The policy should articulate the—

(a) commitment to compliance;

(b) scope of the compliance program;

(c) application and context of the program in relation to the size, nature and complexity of the organization and its operating environment;

(d) responsibility for managing and reporting compliance; and

(e) required standard of conduct, accountability and consequences of non-compliance.

3.2.3 Development

In developing the policy, consideration should be given to the—

(a) specific local or regional obligations and requirements;

(b) organization's strategic objectives and values;

(c) organization's structure and governance framework;

(d) severity of risk of non-compliance;

(e) other internal policies, standards and codes (e.g. financial, risk, quality, environment, occupational health and safety);

(f) principles on which relationships with internal and external stakeholders will be managed;

(g) extent to which compliance will be integrated with other support functions such as risk, audit and legal;

(h) degree to which compliance will be embedded into operational processes and systems; and

(i) degree of independence and autonomy of the compliance function.

3.2.4 Documentation

The policy should—

(a) be written in plain language so that all employees can easily understand the principles and intent;

(b) be communicated and readily available to all employees;

(c) be translated into languages other than English if that is necessary for the policy to be comprehended by employees from non-English-speaking backgrounds; and

(d) be updated to ensure it remains relevant.

3.3 PRINCIPLE 3

> Appropriate resources are allocated to develop, implement, maintain and improve the compliance program.

Top management should ensure that the necessary resources are provided and deployed effectively to design, develop, implement, maintain and improve the compliance program and its outcomes to ensure that the compliance program meets its objectives, and that compliance is achieved. Resources include financial and human resources, including access to external advice and specialized skills, organizational infrastructure, contemporary reference material on compliance management and legal obligations, professional development and technology.

Middle and other levels of management should implement the same principles.

Resource allocation should include allowing employees sufficient time to perform their compliance responsibilities.

3.4 PRINCIPLE 4

The objectives and strategy of the compliance program are endorsed by the governing body and top management.

3.4.1 Objectives

An organization should set objectives and targets to fulfil the commitments established in its compliance policy. The compliance objectives should align with its overall strategic objectives.

Clear targets should be established to achieve the compliance objectives. When targets are set, they should be measurable, time-related and indicate the level of performance required. These targets should form part of the performance management agreements of the individuals concerned and should be linked to remuneration.

3.4.2 Strategy

The organization should document its strategy for establishing the compliance program and ensure that its strategy is consistent with the principles in this Standard. The strategy should be approved by the governing body and should include:

(a) The structure of the program.

(b) The roles and responsibilities of people managing the compliance program.

(c) The resources to be applied in the compliance program.

(d) The priorities set for the compliance program.

(e) How compliance obligations will be embedded in operational practices and procedures.

(f) A process for identifying, reporting and responding to compliance failures.

(g) How the organization will monitor and measure its delivery on its strategy.

3.5 PRINCIPLE 5

Compliance obligations are identified and assessed.

3.5.1 Identification of compliance obligations

An organization should systematically identify its compliance obligations and the way in which they impact on its activities, products and services. The organization should ensure that these requirements are taken into account in establishing, implementing and maintaining and improving its compliance program.

The organization should document its compliance obligations in a manner that is appropriate to its size, complexity, structure and operations. This may take a range of forms, for example, a register, list or database.

Sources of compliance obligations may include:

(a) Common Law.

(b) Legislation, including statutes, regulations and mandatory codes.

(c) Directives.

(d) Permits, licences or other forms of authorization.

(e) Orders issued by regulatory agencies.

(f) Judgments of courts or administrative tribunals.

(g) Customary or indigenous law.

(h) Treaties, conventions and protocols.

(i) Relevant industry codes and standards.

Depending on its circumstances and needs, an organization may commit to additional compliance obligations, for example:

(i) Agreements with community groups or non-governmental organizations.

(ii) Agreements with public authorities and customers.

(iii) Organizational requirements.

(iv) Voluntary principles or codes of practice.

(v) Voluntary labelling or environmental commitments.

3.5.2 Maintenance of compliance obligations

Organizations should have processes in place to receive timely advice of changes to laws, regulations, codes and other compliance obligations to ensure ongoing compliance. Ongoing liaison with regulatory authorities is normally necessary so that the organization is aware of current compliance issues and practices.

Such information could be obtained by:

(a) Arrangements with legal advisors.

(b) Being on relevant regulators' mailing lists.

(c) Membership of professional groups.

(d) Subscribing to relevant information services.

(e) Attending industry forums and seminars.

(f) Monitoring regulators' web-sites.

3.5.3 Prioritization

Prior to the implementation of its compliance program an organization should identify compliance risks and rank the likelihood and consequences of potential compliance failures and allocate resources for their treatment accordingly. (See Principle 9)

NOTE: AS/NZS 4360 provides guidance on undertaking risk assessments.

The risk of compliance failure should be reassessed whenever there are—

(a) new or changed activities, products or services;

(b) changes to the structure or strategy of the organization;

(c) significant external changes; or

(d) changes to compliance obligations.

SECTION 4 IMPLEMENTATION

4.1 PRINCIPLE 6

Responsibility for compliant outcomes is clearly articulated and assigned.

4.1.1 Assigning responsibility to management

The active involvement of, and supervision by, management is an integral part of an effective compliance program. This helps ensure that employees fully understand the organization's policy and operational procedures and how these apply to their jobs, and that they carry out compliance obligations effectively.

For a compliance program to be effective the governing body and top management need to lead by example, both by adhering to and actively supporting compliance and by being seen to adhere to and actively support, the compliance program.

Many larger companies have a dedicated compliance manager with overall day-to-day responsibility for compliance, and a cross-functional compliance committee to co-ordinate compliance across the organization. Smaller organizations should have someone who has overall compliance responsibility, though this may be in addition to other roles.

This should not be seen as absolving other management of their compliance responsibilities, as all managers have a role to play with respect to the compliance program. It is therefore important that their respective responsibilities are clearly set out and included in their position profiles.

Compliance responsibilities of managers will, by necessity, vary according to levels of seniority, influence and other factors, such as the nature and size of the organization. However, some responsibilities are likely to be common across a variety of organizations.

NOTE: This Standard does not distinguish between the concept of responsibility and that of accountability. Accountability is implicit in the use of the term 'responsibility'.

4.1.2 Top management responsibility

Top management should:

(a) Ensure that the commitment to compliance is upheld at all times and that failures and conduct that are prejudicial to compliance culture are dealt with appropriately.

(b) Allocate the appropriate resources to implement, develop, maintain and improve the compliance program and performance outcomes.

(c) Ensure that effective and timely systems of reporting are in place.

(d) Appoint or nominate a competent senior compliance executive(s) with—

  (i) authority and responsibility for the overall design, consistency and integrity of the compliance program;

  (ii) clear and unambiguous support from and direct access to the Chief Executive Officer and the Board; and

  (iii) access to—

    (A) senior decision-makers and the right to participate in the decision-making processes;

    (B) all levels of the organization; and

    (C) expert advice on relevant laws, regulations, codes and organizational standards.

(e) Include compliance responsibilities in position statements of top managers.

(f) Be measured against compliance key performance indicators.

Top management should ensure that the compliance function has authority to act independently and is not compromised by conflicting priorities, particularly where compliance is embedded in the business.

4.1.3 Compliance manager responsibility

Not all organizations will create a discrete functional role for a compliance manager, some may assign this function to an existing appointment. However, responsibility for compliance management will need to be allocated.

The compliance manager in conjunction with operational management is responsible for:

(a) Identifying compliance obligations with the support of legal and other relevant resources and translating those requirements into actionable policies and procedures.

(b) Integrating compliance obligations into existing practices and procedures.

(c) Providing or organizing ongoing training support for managers to ensure that all relevant persons are trained on a regular basis.

(d) Ensuring compliance is factored into position descriptions and employee performance management processes.

(e) Setting in place a compliance reporting and documenting system.

(f) Developing and implementing systems for sourcing information such as complaints, feedback, hotlines, whistleblowing and other mechanisms.

(g) Establishing compliance performance indicators.

(h) Monitoring and measuring compliance performance.

(i) Analysing performance to identify the need for corrective action.

(j) Ensuring compliance capabilities and performance are factored into contracts with external suppliers.

(k) Overseeing outsourcing arrangements for compliance.

(l) Ensuring the compliance program is reviewed on a regular basis.

(m) Ensuring there is access to appropriate legal and other professional advice in the design and implementation of the program.

In allocating responsibility for compliance management, consideration should be given to ensuring that the person with the responsibility for compliance has demonstrated—

(i) a record of integrity and commitment to compliance;

(ii) effective communication and influencing skills;

(iii) an ability and standing to command acceptance of advice and guidance; and

(iv) relevant competence.

4.1.4 Line management responsibility

Line management is responsible for achieving compliance within its area of responsibility. This includes:

(a) Cooperating with and supporting the compliance manager and encouraging employees to do the same in relation to each of the considerations set out in Clause 4.1.3.

(b) Personally complying and being seen to comply and follow operational procedures.

(c) Formally raising with top management any inadequacies in resourcing to achieve compliance.

(d) Identifying, documenting and communicating compliance exposures in their operations.

(e) Actively encouraging, mentoring, coaching, and supervising employees to promote compliant behaviour.

(f) Integrating compliance obligations into business practices.

(g) Actively participating in the management and resolution of compliance related incidents and issues.

(h) Developing employee awareness of compliance obligations and requiring them to meet training and competence requirements.

(i) Integrating compliance performance into employee performance appraisals.

(j) Encouraging employees to escalate compliance incidents.

(k) Providing employees with access to—

   (i) resources such as detailed manuals or guides on compliance procedures and reference materials and databases;

   (ii) adequate work tools, training and facilities; and

   (iii) support mechanisms, such as access to the compliance manager and whistleblower systems.

(l) Identifying compliance obligations with the support of legal and other relevant resources and translating those requirements into actionable policies and procedures.

(m) Working with the compliance manager to integrate compliance obligations into existing practices and procedures in their areas of responsibility.

(n) Providing or organizing ongoing training support for managers to ensure that all relevant persons are trained on a regular basis.

(o) Ensuring compliance is factored into position descriptions and employee performance management processes.

(p) In conjunction with the compliance manager, setting in place a compliance reporting and documenting system.

(q) In conjunction with the compliance manager, developing and implementing systems for sourcing information such as complaints, feedback, hotlines, whistleblowing and other mechanisms.

(r) In conjunction with the compliance manager, establishing compliance performance indicators.

(s) In conjunction with the compliance manager, analysing performance to identify the need for corrective action.

(t) Ensuring compliance capabilities and performance are factored into contracts with external suppliers.

(u) Overseeing outsourcing arrangements to ensure they take account of compliance obligations.

4.1.5 Employee responsibility

All employees, including managers, should—

(a) adhere to the compliance obligations rlevant to their position;

(b) perform their duties in an ethical, lawful and safe manner;

(c) undertake training in accordance with the compliance program; and

(d) report and escalate compliance concerns, issues and failures.

4.1.6 Outsourcing

Outsourcing of an organization’s operations does not relieve the organization of its legal responsibilities or compliance obligations. The standard that would be required for any outsourcing contractor should be the same as that for the organization itself.

If there is any outsourcing of the organization’s activities, the organization needs to undertake effective due diligence to ensure that its standards and commitment to compliance will not be lowered. Controls over contractors should also be in place to ensure that the contract is complied with effectively.

4.1.7 Internal communication

An organization should adopt multiple methods of communication to ensure that the compliance message is heard and understood by all employees. The communication should clearly set out the organization’s expectation of employees and those issues that need to be escalated and under what circumstances and to whom.

4.1.8 External communication

A practical approach to external communication, targeting all interested parties, should be adopted. Interested parties can include, but are not limited to, regulatory bodies, customers, contractors, suppliers, investors, emergency services, non-governmental organizations and neighbours.

Methods of communication may include: informal discussions, open days, focus groups, community dialogue, involvement in community events, websites and e-mail, press releases, advertisements and periodic newsletters, annual (or other periodic) reports and telephone hotlines. These approaches can encourage understanding and acceptance of an organization’s compliance commitment.

4.2 PRINCIPLE 7

Competence and training needs are identified and addressed to enable employees to fulfil their compliance obligations.

All employees have compliance obligations and should be competent to discharge these effectively. The attainment of competence can be achieved in many ways including through education, training or work experience.

The objective of a training program is to ensure that all employees are competent to fulfil their job role in a manner that is consistent with the organization’s compliance culture and its commitment to compliance.

Properly designed and executed training can provide an effective mechanism and forum for employees to communicate previously unidentified compliance exposures.

Education and training of employees should be:

(a) Based on an assessment of gaps in employee knowledge and competence.

(b) Ongoing from the time of induction.

(c) Aligned to the corporate training system.

(d) Practical and readily understood by employees.

(e) Relevant to the day-to-day work of employees and illustrative of the industry, organization or sector concerned.

(f) Sufficiently flexible to account for a range of techniques to accommodate the differing needs of organizations and employees.

(g) Assessed for effectiveness.

(h) Updated as required.

(i) Recorded.

Indicators for retraining in compliance would include:

(i) Change of position or responsibilities.

(ii) Changes in internal processes, policies and procedures.

(iii) Changes in organization structure, e.g. mergers.

(iv) Change in the external compliance environment, e.g. changes in legal or customer requirements.

(v) Change in products or services.

(vi) Issues arising out of monitoring, auditing, reviews, complaints and incidents.

4.3 PRINCIPLE 8

Behaviours that create and support compliance are encouraged and behaviours that compromise compliance are not tolerated.

4.3.1 Top management's role in encouraging compliance

Top management has a key responsibility for:

(a) Aligning the organization's commitment to compliance to its strategic objectives and values in order to position compliance appropriately.

(b) Communicating its commitment to compliance in order to build awareness and motivate employees to behave appropriately.

(c) Encouraging all employees to accept the importance of achieving the compliance objectives and targets for which they are responsible or accountable.

(d) Creating an environment where the reporting of compliance failures is encouraged.

(e) Encouraging employees to make suggestions that facilitate continual improvement in compliance performance.

(f) Ensuring compliance outcomes are incorporated into the broader organization culture and culture change initiatives.

(g) Identifying and acting promptly to correct or address compliance issues.

(h) Ensuring that organizational practices and policies support and encourage compliance outcomes.

4.3.2 Compliance culture

The development of a compliance culture requires the active, visible and consistent commitment of the chief executive and management to a common, published standard of behaviour that is required throughout every area of the organization. Factors that will support the development of a compliance culture include:

(a) A clear set of published values.

(b) Management actively seen to be implementing and abiding by the values.

(c) A consistency in the approach to reward and punishment for similar actions, regardless of position.

(d) The incorporation of compliance performance in every position description.

(e) Appropriate pre-employment screening of potential employees.

(f) Induction program that emphasizes compliance and the organization’s values.

(g) Ongoing compliance training and regular compliance failures updates.

(h) Mentoring, coaching and leading by example.

(i) Performance appraisal systems that include assessment of compliance behaviour and which link performance pay to achievement of compliance obligations.

(j) Highly visible rewarding of compliant behaviour.

(k) Prompt and visible disciplining in the case of wilful, negligent or reckless breaches.

(l) Minimizing unnecessary bureaucracy by simplifying processes.

(m) A clear link between the organization’s strategy and individual roles, reflecting compliance outcomes as essential to achieving business outcomes.

(n) Open, two-way communication about compliance outcomes.

(o) Process changes that are managed smoothly to minimize any negative impact on employees.

Evidence of a compliance culture is indicated by the degree to which—

(i) the items above are implemented;

(ii) employees believe that the items above have been implemented;

(iii) employees understand their personal compliance obligations and those of their business unit;

(iv) the obligation for compliance and the remediation of any breach is ‘owned’ by employees; and

(v) the role of the compliance team, and the compliance team’s objectives are regarded as valuable.

4.4 PRINCIPLE 9

Controls are in place to manage the identified compliance obligations and achieve desired behaviours.

Effective controls are needed to ensure that the organization's compliance obligations are met and that critical points of risk of compliance failure are addressed.

The types and levels of controls should be designed with sufficient rigour to facilitate achieving the compliance obligations that are particular to the organization’s operating environment. Such controls should, where possible, be embedded into normal business processes.

Such control methods should include:

(a) Documented operating policies and procedures.

(b) Work instructions.

(c) Systems and exception reports.

(d) Approvals.

(e) Systems of recommendations.

(f) Segregation of duties.

(g) System controls.

These controls should be maintained and evaluated periodically to ensure their continuing effectiveness.

Procedures should be established, documented, implemented, and maintained to support the compliance policy and translate the compliance obligations into practice.

In developing these procedures consideration should be given to:

(i) Integrating the compliance obligations into operating and administrative procedures including computer systems, forms, reporting systems and contracts.

(ii) Ongoing monitoring and measurement.

(iv) Specific procedures to deal with compliance failures that could arise.

(iv) Assessment and reporting (including management supervision) to ensure that employees comply with procedures.

(v) Specific arrangements for identifying, reporting and escalating instances of compliance failure and risks of compliance failure.

The issuing and ongoing review of all compliance documentation should be controlled to maintain integrity and consistency across the organization.

SECTION 5 MONITORING AND MEASURING

5.1 PRINCIPLE 10

Performance of the compliance program is monitored, measured and reported.

5.1.1 Monitoring

The compliance program should be regularly monitored to ensure compliance performance is achieved. A plan for continual monitoring should be established, setting out monitoring processes, schedules, resources and the data to be collected.

Compliance monitoring is the process of gathering data for the purpose of:

(a) Identifying and remedying problems.

(b) Checking that compliance obligations are being met.

(c) Reviewing the integrity and effectiveness of the compliance program.

(d) Tracking progress on meeting policy commitments, objectives and targets.

(e) Evaluating the effectiveness of operational controls.

The monitoring process relates to both the compliance program itself and compliance performance.

Monitoring of the compliance program itself typically includes:

(i) Effectiveness of training.

(ii) Adequacy of controls at critical points.

(iii) Effective allocation of responsibilities for meeting compliance obligations.

(iv) Currency of compliance obligations.

(v) Effectiveness in addressing issues previously identified.

Monitoring of compliance performance typically includes:

(A) Compliance failures and ‘near misses’.

(B) Instances where critical control point requirements are not met.

(C) Instances where objectives and targets are not achieved.

(D) Instances where compliance inspections are not performed as scheduled.

(E) Status of compliance culture.

5.1.2 Sources of information for monitoring and measuring

The organization should design, develop, implement and maintain procedures for seeking and receiving feedback on its compliance performance from a range of sources including:

(a) Employees, e.g. through hotlines, feedback, suggestion boxes.

(b) Customers, e.g. through a complaints handling system.

(c) Suppliers.

(d) Regulators.

(e) Process control logs and activity records (including both computer and paper based).

5.1.3 Methods of data collection

There are many methods for collecting information. Each method listed below is relevant in different circumstances and care should be taken to select the variety of tools appropriate to the organization and its particular issues. Methods include:

(a) Ad hoc reports of issues as they emerge or are identified.

(b) Information gained through hot lines, complaints and other feedback, including whistleblowing.

(c) Informal discussions and workshops.

(d) Sampling and integrity testing such as mystery shopping.

(e) Direct observations, formal interviews, facility tours and inspections.

(f) Audits and reviews.

5.1.4 Data analysis and classification

Effective classification and management of the data is critical. A system should be developed for classifying and storing the data in readily searchable databases. Data classification criteria could include:

(a) Source.

(b) Department.

(c) Issue type.

(d) Indicators.

The data management systems should capture both issues and complaints and allow classification and analysis of those that relate to compliance.

Once the information has been collected, it needs to be analysed and critically assessed to identify actions to be taken. The analysis should consider systemic and recurring problems as these are likely to carry significant risks for the organization and can be more difficult to identify.

5.1.5 Development of indicators

It is important that organizations develop a set of measurable indicators that will assist the organization in quantifying its compliance performance. The issue of what and how to measure compliance performance can be problematic and the following list of indicators should not be seen as exhaustive. Furthermore, the indicators needed will vary with the organization’s maturity and the timing and extent of new and revised programs being implemented.

Indicators may include:

(a) Percentage of employees trained effectively.

(b) Issues and breaches reported by type and area.

(c) Consequence of breaches, which may include valuation of impact resulting from monetary compensation, cost of remediation, reputation or cost of employees’ time.

(d) Frequency of contacts with regulators by category of contact.

(e) Usage of feedback mechanisms (including comments on the value of those mechanisms by users).

5.1.6 Compliance reporting

The governing body, top management and the compliance manager should ensure that they are adequately informed on all relevant compliance failures and actively promote the principle that the organization encourages and supports a culture of full and frank reporting.

Internal reporting arrangements need to ensure that:

(a) Appropriate criteria and obligations for reporting are set out.

(b) Timelines for regular reporting are established.

(c) An exception reporting system is in place which facilitates ad hoc reporting of emerging and crystallized issues.

(d) Systems and processes are in place to ensure the accuracy and completeness of information.

(e) Accurate and complete information is provided to the correct people or areas of the organization to enable remedial action to be taken.

(f) There is sign-off on the accuracy of reports to the governing body, including by the Compliance Manager (if the organization has one).

An organization should choose a format, content and timing of its internal compliance reporting that is appropriate to its circumstances, unless otherwise specified by law.

Reporting of compliance should be incorporated in standard organizational reports. Separate reports should only be prepared for major breaches and for urgent emerging issues.

All compliance failures need to be appropriately reported. While the reporting of systemic and recurring problems is particularly important, a one-off compliance failure can be of equal concern if it is major or deliberate. Even a small failure, if not reported in a timely manner, can lead to the view that the failure does not matter and can result in such failure becoming a systemic problem.

Employees should be encouraged to respond and report breaches of the law and other incidents of non-compliance, and to see reporting as a positive and non-threatening action. Reporting obligations should be set out clearly in the organization's compliance policy and procedures and reinforced by other methods, such as informal reinforcement by managers during their day-to-day work with employees.

5.1.7 Content of compliance reports

Compliance reports typically include:

(a) Any matters which the organization is required to notify to any regulatory authority.

(b) Significant changes to any compliance obligations.

(c) Measurement of compliance performance, including compliance failures and areas of improvement.

(d) Number and details of alleged breaches of relevant laws, codes and organizational standards that have been identified, and an assessment of the extent to which similar conduct could have subsequently occurred.

(e) Corrective action undertaken.

(f) Evidence of the compliance program's effectiveness, achievements and trends.

(g) Contacts, and developments in relationships, with regulators.

(h) Changes in compliance obligations, their impact on the organization and the proposed course of action to meet the new obligations.

The compliance policy should promote the immediate reporting of materially significant matters which arise outside the timelines for regular reporting.

5.1.8 Issues management

Once an issue is identified as a compliance failure or a potential compliance failure:

(a) It should be reported.

(b) It should be investigated, analysed and classified to determine the cause and extent of required corrective and or preventive actions.

(c) Corrective action should address the specific issue as well as a recurrence of compliance failures.

(d) It should be followed up to ensure that corrective and preventive actions have been implemented and are effective.

Data from analysing compliance problems can be used to:

(i) Redesign products and services.

(ii) Change organizational practices and procedures.

(iii) Retrain employees.

(iv) Re-assess consumer information needs.

(v) Assess service performance.

(vi) Give early warning of potential problems.

(vii) Redesign or review controls.

5.1.9 Escalation

A clear escalation process should be adopted and communicated to ensure all compliance failures are raised and reported to the line manager, escalated to the manager responsible for the compliance program; and where appropriate, escalated to top management and the governing body. The process should specify to whom, how and when issues are to be reported and the timelines for internal and external reporting.

Where there are reportable breaches, regulatory authorities should be informed of—

(a) the actions being taken to mitigate the impact of the breach and prevent further occurrences;

(b) any suspected, but yet to be fully investigated, reportable breaches;

(c) the actions being taken to complete the investigations and the likely time frame for resolutions;

(d) any genuine difficulties in complying with particular laws; and

(e) any unintended consequences of laws and regulations which make compliance difficult.

5.2 PRINCIPLE 11

The organization is able to demonstrate its compliance program through both documentation and practice.

5.2.1 Record-keeping

Accurate, up-to-date records of the organization's compliance activities should be maintained to assist in the monitoring and review process and demonstrate conformity with the program.

Record-keeping should include recording and classifying complaints, disputes and alleged compliance failures and the steps taken to resolve them.

Records should be stored in a manner that ensures they remain legible, readily identifiable and retrievable.

5.2.2 Documents and records

The organization's compliance program documents and records typically include:

(a) The organization's compliance policy.

(b) Register of relevant compliance obligations.

(c) Prioritization of the response based on the risk assessment process.

(d) The objectives, targets, structure and content of the compliance program.

(e) Allocation of roles and responsibilities for compliance.

(f) Training records.

(g) Information on compliance performance including compliance reports.

(h) Complaints and communications from the organization's interested parties and resolution.

(i) Details of compliance failures and corrective and preventive actions.

(j) Results of reviews and audits of the compliance program and actions taken.

5.2.3 Practices

The practices which demonstrate a commitment to compliance typically include:

(a) Communication in public and internally of the organization's commitment to compliance.

(b) Adequate resourcing of the compliance program.

(c) Necessary investment in compliance training to reflect its importance.

(d) Linking of compliance and behaviour to incentives and performance management.

SECTION 6 CONTINUAL IMPROVEMENT

6.1 PRINCIPLE 12

The compliance program is regularly reviewed and continually improved.

6.1.1 Compliance program review

Top management should ensure that the organization's compliance program is reviewed on a regular basis to ensure its continued suitability, adequacy and effectiveness. The actual depth and frequency of such reviews will vary with the nature of the organization and its policies.

The review should be conducted in accordance with good review and audit practices. The review should be carried out by a competent person who is free from bias and conflict of interest.

The inputs to the review may include:

(a) Whether the program is operating effectively.

(b) The extent to which objectives and targets have been met.

(c) Communication(s) from its interested parties, including complaints.

(d) Results of monitoring activities.

(e) Status of corrective and preventive actions and timeliness of resolution.

(f) Previous compliance reviews and their recommendations.

(g) Changes in the external and internal environment.

(h) Adequacy of resources.

(i) Adequacy of the compliance policy, its associated objectives and targets, systems, structure and personnel.

6.1.2 Compliance program review outcomes

Findings and recommendations of the review should be documented and provided to the governing body and top management.

Recommendations should include:

(a) Corrective actions with respect to compliance failures.

(b) The need for the changes to the compliance program including the compliance policy, its associated objectives and targets, systems, structure and personnel.

(c) Recognition of exemplary compliance behaviour by teams, work units and individuals.

(d) Longer term continual improvement initiatives.

(e) Changes to compliance processes to ensure effective integration with operational practices and systems.

APPENDIX A

BIBLIOGRAPHY

AS	
4269	Complaints handling
8000	Corporate governance—Good governance principles
8001	Corporate governance—Fraud and corruption control
8002	Corporate governance—Organizational codes of conduct
8003	Corporate governance—Corporate social responsibility
8004	Corporate governance—Whistleblower protection programs for entities
AS/NZS	
4360	Risk management
HB 436	Risk management guidelines—Companion to AS/NZS 4360: 2004
4801	Occupational health and safety management systems—Specification with guidance for use
AS/NZS ISO	
9001	Quality management systems—Requirements
14001	Environmental management systems—Requirements with guidance for use
19011	Guidelines for quality and/or environmental management systems auditing

NOTES

NOTES

NOTES

Standards Australia

Standards Australia is an independent company, limited by guarantee, which prepares and publishes most of the voluntary technical and commercial standards used in Australia. These standards are developed through an open process of consultation and consensus, in which all interested parties are invited to participate. Through a Memorandum of Understanding with the Commonwealth government, Standards Australia is recognized as Australia's peak national standards body. For further information on Standards Australia visit us at

www.standards.org.au

Australian Standards

Australian Standards are prepared by committees of experts from industry, governments, consumers and other relevant sectors. The requirements or recommendations contained in published Standards are a consensus of the views of representative interests and also take account of comments received from other sources. They reflect the latest scientific and industry experience. Australian Standards are kept under continuous review after publication and are updated regularly to take account of changing technology.

International Involvement

Standards Australia is responsible for ensuring that the Australian viewpoint is considered in the formulation of international Standards and that the latest international experience is incorporated in national Standards. This role is vital in assisting local industry to compete in international markets. Standards Australia represents Australia at both ISO (The International Organization for Standardization) and the International Electrotechnical Commission (IEC).

Electronic Standards

All Australian Standards are available in electronic editions, either downloaded individually from our web site, or via On-Line and DVD subscription services. For more information phone 1300 65 46 46 or visit Standards Web Shop at

www.standards.com.au

STANDARDS
Australia

GPO Box 476 Sydney NSW 2001
Administration Phone (02) 8206 6000 Fax (02) 8206 6001 Email mail@standards.com.au
Customer Service Phone 1300 65 46 46 Fax 1300 65 49 49 Email sales@standards.com.au
Internet www.standards.org.au

ISBN 0 7337 7296 X

Printed in Australia