ISO Central Secretariat

1, ch. de la Voie-Creuse
Case postale 56
CH - 1211 Genève 20
Switzerland

Telephone + 41 22 749 01 11
Fax + 41 22 733 34 30
E-mail central@iso.org
Web www.iso.org

Organisation internationale de normalisation
International Organization for Standardization
Международная Организация по Стандартизации

Our ref. TMB / NWIP

TO THE ISO MEMBER BODIES

Date 2012-06-01

New work item proposal – *Compliance programs*

Dear Sir or Madam,

Please find attached a new work item proposal submitted by SA (Autralia) on *Compliance programs*. It should be noted that, if the NWIP is approved, the work is proposed to be carried out in a Project Committee.

You are kindly invited to complete the ballot form (Form 05) which could be downloaded at www.iso.org/forms and send it, preferably in Word format, to the Secretariat of the ISO Technical Management Board at *tmb@iso.org* before **1 September 2012.**

Yours faithfully,

Sophie Clivio
Secretary to the Technical Management Board

Encl: NWIP (Form 04)
Draft Compliance programs
Justification Study

NEW WORK ITEM PROPOSAL	
Date of presentation 2012-06-01	Reference number (to be given by the Secretariat)
Proposer SA (Australia)	**ISO/TC** /PC XX **/ SC** N
Secretariat Proposed PC Secretariat (SA)	

A proposal for a new work item within the scope of an existing committee shall be submitted to the secretariat of that committee with a copy to the Central Secretariat and, in the case of a subcommittee, a copy to the secretariat of the parent technical committee. Proposals not within the scope of an existing committee shall be submitted to the secretariat of the ISO Technical Management Board.

The proposer of a new work item may be a member body of ISO, the secretariat itself, another technical committee or subcommittee, or organization in liaison, the Technical Management Board or one of the advisory groups, or the Secretary-General.

The proposal will be circulated to the P-members of the technical committee or subcommittee for voting, and to the O-members for information.

See overleaf for guidance on when to use this form.

IMPORTANT NOTE: Proposals without adequate justification risk rejection or referral to originator.
Guidelines for proposing and justifying a new work item are given overleaf.

Proposal (to be completed by the proposer)

Title of proposal (in the case of an amendment, revision or a new part of an existing document, show the reference number and current title)

English title: Compliance programs

French title (if available): Programmes de conformité

Scope of proposed project

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

It can be used to implement a compliance program to assist the organisation with meeting any legislative and/or other commitments (voluntary or mandatory) to which an organisation is obligated to comply with or has committed to meet on a voluntary basis. The commitments may include meeting legislation, codes of practice, industry and/or community agreements.

The Standard can also facilitate best practice benchmarking of compliance programs by both organisations and regulators.

The Standard is proposed to be based on the existing Australian Standard 3806-2006 Compliance programs , which has also been adopted by Standards New Zealand as an NZS/AS document.

Concerns known patented items (see ISO/IEC Directives Part 1 for important guidance)

☐ Yes ☒ No If "Yes", provide full information as annex

Envisaged publication type (indicate one of the following, if possible)

☒ International Standard ☐ Technical Specification ☐ Publicly Available Specification ☐ Technical Report

Purpose and justification (attach a separate page as annex, if necessary)

There is a need to create a Compliance programs ISO standard as an MSS to harmonise existing guidelines or guidance. This standard is a MSS - Type B however it also cover elements of MSS Type-A. (ISO/IEC Directives Part1:2012 9th edition Annex SL)

A Justification Study and NWI Draft (both attached) have been developed based on former ISO Guide 72 .

Target date for availability (date by which publication is considered to be necessary) 2015

Proposed development track ☐ 1 (24 months) ☒ 2 (36 months - default) ☐ 3 (48 months)

Relevant documents to be considered

The following standards will be considered as part of the development of MSS.
ISO 14001:2004 – Environmental management
ISO 9001:2008 – Quality management
ISO 26000:2010 – Social responsibility
ISO 31000:2009 – Risk management
ISO/IEC 38500:2008 Corporate governance of information technology
ISO 19011:2011 Guidelines for auditing management systems
ISO 17021:2011 Conformity assessment -- Requirements for bodies providing audit and certification of management systems

Relationship of project to activities of other international bodies

To be decided after the first meeting

Liaison organizations

Liaison would be considered to establish with the following committees as they have a strong relation of this proposal.
ISO/CASCO Committee on conformity assessment
ISO/TC 176/SC 2 Quality systems
ISO/TC 176/SC 3 Supporting technologies
ISO/TC 207/SC 1 Environmental management systems
ISO/PC 262 Risk Management
JTC 1/WG 6 Corporate Governance of IT
ISO/TMB – ISO Technical Management Board

Need for coordination with:

☐ IEC ☐ CEN ☐ Other (please specify)

Preparatory work (at a minimum an outline should be included with the proposal)

☒ A draft is attached ☐ An outline is attached. It is possible to supply a draft by

The proposer or the proposer's organization is prepared to undertake the preparatory work required ☒ Yes ☐ No

Proposed Project Leader (name and address)

Martin Tolar CCP, GAICD
Australian Compliance Institute,
Managing Director
Level 1, 50 Clarence Street, Sydney, NSW, 2000, Australia
GPO Box 4117, Sydney, NSW, 2001, Australia
E-mail: Martin.Tolar@acigrc.com
Phone: +61 2 9290 1788 | F +61 2 9262 3311

Name and signature of the Proposer
(include contact information)

Agnes Simai, Project Manager, Operations
Standards Australia
Level 10, 20 Bridge Street Sydney NSW 2000
GPO Box 476 Sydney NSW 2001
E-mail: agnes.simai@standards.org.au
P +61 2 9237 6109 | F +61 2 9237 6010 |

Comments of the TC or SC Secretariat

Supplementary information relating to the proposal

☒ This proposal relates to a new ISO document;

☐ This proposal relates to the amendment/revision of an existing ISO document;

☐ This proposal relates to the adoption as an active project of an item currently registered as a Preliminary Work Item;

☐ This proposal relates to the re-establishment of a cancelled project as an active project.

Other:

Voting information

The ballot associated with this proposal comprises a vote on:

☒ Adoption of the proposal as a new project

☒ Adoption of the associated draft as a committee draft (CD)

☐ Adoption of the associated draft for submission for the enquiry vote (DIS or equivalent)

Other:

Annex(es) are included with this proposal (give details)

☒ Justification and Draft

Date of circulation	Closing date for voting	Signature of the TC or SC Secretary
2012-06-05	2012-09-05	Agnes Simai, Project Manager, Operations Standards Australia Level 10, 20 Bridge Street Sydney NSW 2000 GPO Box 476 Sydney NSW 2001 E-mail: agnes.simai@standards.org.au P +61 2 9237 6109 | F +61 2 9237 6010 | Standards Australia (SA) is prepared to undertake the ISO/PC secretariat responsibilities of the proposed project.

Use this form to propose:

a) a new ISO document (including a new part to an existing document), or the amendment/revision of an existing ISO document;

b) the establishment as an active project of a preliminary work item, or the re-establishment of a cancelled project;

c) the change in the type of an existing document, e.g. conversion of a Technical Specification into an International Standard.

This form is not intended for use to propose an action following a systematic review - use ISO Form 21 for that purpose.

Proposals for correction (i.e. proposals for a Technical Corrigendum) should be submitted in writing directly to the secretariat concerned.

Guidelines on the completion of a proposal for a new work item

(see also the ISO/IEC Directives Part 1)

a) Title: Indicate the subject of the proposed new work item.

b) Scope: Give a clear indication of the coverage of the proposed new work item. Indicate, for example, if this is a proposal for a new document, or a proposed change (amendment/revision). It is often helpful to indicate what is not covered (exclusions).

c) Envisaged publication type: Details of the types of ISO deliverable available are given in the ISO/IEC Directives, Part 1 and/or the associated ISO Supplement.

d) Purpose and justification: Give details based on a critical study of the following elements wherever practicable. *Wherever possible reference should be made to information contained in the related TC Business Plan*.

1) The specific aims and reason for the standardization activity, with particular emphasis on the aspects of standardization to be covered, the problems it is expected to solve or the difficulties it is intended to overcome.

2) The main interests that might benefit from or be affected by the activity, such as industry, consumers, trade, governments, distributors.

3) Feasibility of the activity: Are there factors that could hinder the successful establishment or global application of the standard?

4) Timeliness of the standard to be produced: Is the technology reasonably stabilized? If not, how much time is likely to be available before advances in technology may render the proposed standard outdated? Is the proposed standard required as a basis for the future development of the technology in question?

5) Urgency of the activity, considering the needs of other fields or organizations. Indicate target date and, when a series of standards is proposed, suggest priorities.

6) The benefits to be gained by the implementation of the proposed standard; alternatively, the loss or disadvantage(s) if no standard is established within a reasonable time. Data such as product volume or value of trade should be included and quantified.

7) If the standardization activity is, or is likely to be, the subject of regulations or to require the harmonization of existing regulations, this should be indicated.

If a series of new work items is proposed having a common purpose and justification, a common proposal may be drafted including all elements to be clarified and enumerating the titles and scopes of each individual item.

e) Relevant documents and their effects on global relevancy: List any known relevant documents (such as standards and regulations), regardless of their source. When the proposer considers that an existing well-established document may be acceptable as a standard (with or without amendment), indicate this with appropriate justification and attach a copy to the proposal.

f) Cooperation and liaison: List relevant organizations or bodies with which cooperation and liaison should exist.

ISO TC XX/SC TMB N

Date: 2010-07-12

ISO/WD

ISO TC XX/SC TMB/WG

Secretariat: SA

Compliance programs

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

S:\Standards Development\International\SA Secretariats\ISO Compliance\ISO Compliance Submission 2012-06-01\ISO_(E) Compliance programs.doc STD Version 2.1c

Contents

Page

Foreword ..... **iv**

Introduction ..... **v**

1 Scope **1**

2 Normative references **1**

3 Terms of definitions **1**

4 Compliance principles **2**
4.1 Commitment **2**
4.1.1 General **3**
4.1.2 Compliance policy **3**
4.1.3 Develop, implement, maintain and improve **4**
4.1.4 Objectives and strategy **5**
4.1.5 Obligations **5**
4.1.6 Responsibility **7**
4.1.7 Competence and training **10**
4.1.8 Behaviours **11**
4.1.9 Controls **13**
4.1.10 Performance **13**
4.1.11 Recordkeeping **18**
4.1.12 Review and Improvement **19**

Annex A (normative/informative **– <*delete which doesn't apply*>) (<*Insert Annex heading*>)** **20**
A.1 Compliance principles **20**

Bibliography **21**

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO was prepared by Technical Committee ISO/TC XX, *XX*, Subcommittee SC TMB, *Technical Management Board*.

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

Introduction

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.

Compliance programs

1 Scope

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

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

Annex A sets out the essential principles which will be common to all effective compliance programs. Paragraph 4 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.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9001 *Quality management systems—Requirements*

ISO 14001 *Environmental management systems—Requirements with guidance for use*

ISO 19011 *Guidelines for quality and/or environmental management systems auditing*

3 Terms of definitions

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

3.1
Code
A statement of recommended practice developed internally by an organization or by an international, national or industry body or other organization.

The code may be mandatory or voluntary.

3.2
Competence
Application of knowledge, understanding and ability to a work related task to achieve an acceptable level of performance.

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.

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.

3.5
Compliance failure
An act or an omission whereby an organization has not met its compliance obligations, processes or behavioural obligations.

3.6
Compliance program
A series of activities that when combined are intended to achieve compliance.

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.

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.

3.9
Organisation
A company, firm, enterprise or association (including a government body), whether incorporated or not.

3.10
Organisational and industry standards
Documented codes of ethics, codes of conduct, good practices and charters that an organization has adopted for its operations.

3.11
Regulatory authority
Any government body or other organization responsible for regulating or enforcing compliance with legislative and other requirements.

3.12
Top management
The level of management within an organization directly accountable to its governing body, shareholders or the owner.

4 Compliance principles

4.1 Commitment

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

4.1.1 General

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.

4.1.2 Compliance policy

The compliance policy is aligned to the organizations strategy and business objectives, and is endorsed by the government body.

4.1.2.1 General

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.

4.1.2.2 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.

4.1.2.3 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.

4.1.2.4 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.

4.1.3 Develop, implement, maintain and improve

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

4.1.3.1 General

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.

4.1.4 Objectives and strategy

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

4.1.4.1 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.

4.1.4.2 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.

4.1.5 Obligations

Compliance obligation are identified and assessed.

4.1.5.1 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:

1) Agreements with community groups or non-governmental organizations.

2) Agreements with public authorities and customers.

3) Organizational requirements.

4) Voluntary principles or codes of practice.

5) Voluntary labelling or environmental commitments.

4.1.5.2 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.

4.1.5.3 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.

4.1.6 Responsibility

Responsibility for compliant outcomes is clearly articulated and assigned.

4.1.6.1 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'.

4.1.6.2 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—

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

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

   3) access to—

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

ii) all levels of the organization; and

iii) 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.

4.1.6.3 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, whistle blowing 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—

1) a record of integrity and commitment to compliance;

2) effective communication and influencing skills;

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

4) relevant competence.

4.1.6.4 Line manager 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—

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

2) adequate work tools, training and facilities; and

3) 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, whistle blowing 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.

4.1.6.5 Employee responsibility

All employees, including managers, should—

a) adhere to the compliance obligations relevant 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.

4.1.6.6 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.

4.1.6.7 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.

4.1.6.8 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.

4.1.7 Competence and training

4.1.7.1 General

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:

1) Change of position or responsibilities.

2) Changes in internal processes, policies and procedures.

3) Changes in organization structure, e.g. mergers.

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

5) Change in products or services.

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

4.1.8 Behaviours

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

4.1.8.1 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.

4.1.8.2 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—

1) the items above are implemented;

2) employees believe that the items above have been implemented;

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

4) the obligation for compliance and the remediation of any breach is 'owned' by employees; and

5) the role of the compliance team, and the compliance team's objectives are regarded as valuable.

4.1.9 Controls

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

4.1.9.1 General

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:

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

2) Ongoing monitoring and measurement.

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

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

5) 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.

4.1.10 Performance

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

4.1.10.1 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:

1) Effectiveness of training.

2) Adequacy of controls at critical points.

3) Effective allocation of responsibilities for meeting compliance obligations.

4) Currency of compliance obligations.

5) Effectiveness in addressing issues previously identified.

Monitoring of compliance performance typically includes:

i) Compliance failures and ‘near misses’.

ii) Instances where critical control point requirements are not met.

iii) Instances where objectives and targets are not achieved.

iv) Instances where compliance inspections are not performed as scheduled.

v) Status of compliance culture.

4.1.10.2 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).

4.1.10.3 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

Whistle blowing.

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.

4.1.10.4 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.

4.1.10.5 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).

4.1.10.6 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.

4.1.10.7 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.

4.1.10.8 Issue 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:

1) Redesign products and services.

2) Change organizational practices and procedures.

3) Retrain employees.

4) Re-assess consumer information needs.

5) Assess service performance.

6) Give early warning of potential problems.

7) Redesign or review controls.

4.1.10.9 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.

4.1.11 Recordkeeping

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

4.1.11.1 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.

4.1.11.2 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 organizations 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.

4.1.11.3 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.

4.1.12 Review and Improvement

The compliance program is regularly reviewed and continually improved.

4.1.12.1 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.

4.1.12.2 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.

Annex A
(normative/informative – <*delete which doesn't apply*>)

(<*Insert Annex heading*>)

A.1 Compliance principles

4.1 Commitment

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

4.1.1 Commitment (Principle 1)	Commitment by the governing body and top management to effective compliance that permeates the whole organization.
4.1.2 Compliance policy (Principle 2)	The compliance policy is aligned to the organization's strategy and business objectives, and is endorsed by the governing body.
4.1.3 Develop, implement, maintain and improve (Principle 3)	Appropriate resources are allocated to develop, implement, maintain and improve the compliance program.
4.1.4 Objectives and strategy	The objectives and strategy of the compliance program are endorsed by the governing body and top management.
4.1.5 Obligations	Compliance obligations are identified and assessed.

4.2 Implementation

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

4.1.6 Responsibility (Principle 6)	Responsibility for compliant outcomes is clearly articulated and assigned.
4.1.7 Competence and training (Principle 7)	Competence and training needs are identified and addressed to enable employees to fulfil their compliance obligations.
4.1.8 Behaviours (Principles 8)	Behaviours that create and support compliance are encouraged and behaviours that compromise compliance are not tolerated
4.1.9 Controls (Principles 9)	Controls are in place to manage the identified compliance obligations and achieve desired behaviours

4.3 Monitoring

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

4.1.10 Performance (Principles 10)	Performance of the compliance program is monitored, measured and reported.
4.1.11 Recordkeeping (Principles 11)	The organization is able to demonstrate its compliance program through both documentation and practice.

4.4 Continual improvement

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

4.1.12 Review and Improvement (Principles 12)	The compliance program is regularly reviewed and continually improved.

Bibliography

[1] AS 4269:1995 *Complaints handling*

[2] AS 8000:2003 *Corporate governance—Good governance principles*

[3] AS 8001:2003 *Corporate governance—Fraud and corruption control*

[4] AS 8002:2003 *Corporate governance—Organizational codes of conduct*

[5] AS 8003:2003 *Corporate governance—Corporate social responsibility*

[6] AS 8004:2003 *Corporate governance—Whistleblower protection programs for entities*

[7] AS/NZS 4360:2004 *Risk management*

[8] HB 436:2004 *Risk management guidelines*

[9] AS/NZS 4801:2001 *Occupational health and safety management systems—Specification with guidance for use*

Justification Study for ISO adoption of AS/NZS 3806 Compliance programs standard to an ISO MSS standard

1. Purpose and Scope of MSS Proposal

Purpose and scope of the Management System Standards (MSS) for compliance programs.

This proposal is for the development of an international Management System Standard for compliance programs. It would be developed at a time when G20 governments are talking about global regulations for the financial sector and at a time when national economies are seen as interrelated and rules and regulations are being harmonised. It would seem logical that a guidance document designed to assist organisations to implement effective compliance programs should also be global.

The ISO Standard for Risk Management Programs 31000 has been a companion document of the Australian Standard on Compliance Programs AS/NZS 3806 and it is not uncommon for companies to have a combined Risk and Compliance Department or Group. The risk management standard has already been developed as an international standard and it would seem logical that the companion document for compliance programs also be elevated to an International Standard.

This paper argues that there are significant potential benefits that may arise from the creation of an MMS, with little negative impact, based on the Australian experience with an Australian Standard for compliance programs.

Type of product to be produced by MSS for Compliance Programs

The proposed work under the MSS for Compliance Programs would result in an International Standard (IS) for compliance programs.

Inclusion of product (including service) specifications, product test methods, product performance levels, or other forms of guidance or requirements directly related to products produced or provided by the implementing organisation

The scope does not include any type of standards for products or services produced or provided by an implementing organisation.

Other existing ISO technical committee or non-ISO organisation that could logically have responsibility for the proposed MSS

Throughout the history of Australia and New Zealand's use of the 3806 Standard for Compliance Programs, no other committees or organisations had made any claims for responsibility for the development or management of such a standard. In fact, in these countries, other organisations are reliant on the standard and the industry contribution to its development provided through the Standards Committee process.

Identification of relevant reference materials

Relevant materials have been identified.

Existing National Standards: AS/NZS 3806 - 2006 – Compliance Programs. This standard would form the basis of the submission to the ISO.

Availability of technical experts to support the standardization work, and their representation

Technical experts from Australia and a variety of countries are available to support the standardisation work. These representatives have the specialist technical knowledge and expertise to contribute to actively this work.

Efforts required to develop the document/s

The current National Committee is capable of working with the existing Australian Standard 3806 to contribute to the discussion of a wider ISO Committee.

Anticipated completion date

At most it is anticipated that the International Standard could be fully developed within a three year program of work, given the experience with the existing standard and comparing this against relevant standard developments at the ISO level from draft Australian Standards.

2. Affected Parties

Identification of all the affected parties

All affected parties have been identified as follows:

1) Organisations of various types and sizes: the decision-makers within an organsation who use standards to improve business processes and accountability. These include public, private and non-profit organisations; large, medium and small organisations; and sections or entities within organisations which may wish to implement any component of the MSS for compliance programs.

   The decision-makers may include people with responsibility for corporate governance, risk management, company/corporate secretary, compliance, quality assurance or any manager responsible for the general management of an organisation or for its specific functions or programs.

2) Customers/end-users, i.e. individuals or parties that pay for or use a service from an organisation. Customers of organisations that implement the proposed MSS for compliance programs will benefit from effective governance, accountability, responsiveness, forward planning and efficient operations.

3) Supplier organisations, e.g. producer, distributor, retailer or vendor of a product, or a provider of a service or information. Suppliers using the MSS for compliance programs can demonstrate effective and accountable business processes and sustainable services to their customers. This assists in trade and supplier/customer relations.

4) Companies supplying compliance, governance and risk support services. For example, software vendors using the MSS for compliance programs will be able to develop specialist products to be in conformance with the principles and guidelines in the standard. This assists in the acceptance and penetration of their products in a local or global market.

5) MSS service providers, such as: MSS certification bodies, accreditation bodies or consultants. MSS service providers would include national standards bodies, consultants providing 3rd party audit or assessment services, training organisations offering training (accredited or otherwise) in

implementing any or all components of the proposed MSS family. Some countries have identified a strong requirement for certification against AS/NZS 3806, although it is not a certifiable standard.

6) Regulatory bodies for all industries. Regulatory bodies can encourage these industries to use an MSS for compliance programs as an authoritative way to demonstrate their regulatory compliance.

7) Non-governmental organisations. The private sector and the non-profit sector would be customers and users of the MSS for compliance programs.

8) Society as a whole through improved compliance performance and market and economic stability.

MSS intended to be a guidance document, contractual specification or regulatory specification for an organisation?

The proposed MSS for compliance programs would be a voluntary guidance standard.

Any or all components could be adopted by government at any level and mandated for their jurisdiction, and in turn used for assessing and auditing practice. This would be a choice for the implementing jurisdiction or body.

However it should be noted that the current Australian Standard is a principles based document and as such is not prescriptive, being designed to be scalable and adaptable to organsiational circumstances and size. Auditing of this kind of program is a specialised skill that needs to be sensitive to the adaptations that may have been necessary to make the program fit for purpose.

3. Need for an MSS

The need

There is quite a deal of evidence of failure in the markets for goods and services, particularly in the area of financial services. Governments are looking at ways to address these market failures and an effective compliance program is an important means of achieving this.

One of the key reasons for market failures is that many organisations do not understand, nor do they have in place, the processes and procedures that are required to ensure effective regulatory compliance.

All organisations, regardless of their size or nature of their business, will have regulations and legislation that apply to them, most frequently with multiple regulators and supervision points and with some complexity in their requirements and reporting. An effective organisation-wide compliance program can result in an organisation being able to demonstrate to its interested parties/stakeholders that it has systems in place to help ensure compliance with relevant laws, including legislative requirements, industry codes and best practice.

Compliance programs can also form an important part of a firm's risk management program. As outlined in the Australian Standard, the structure of a good compliance program also contributes to an organisation realising its strategic goals through the discipline of an organisation wide program, including controls and monitoring required by the Standard, especially if its application is not limited to only regulatory compliance, but compliance with the internal policies and strategy of the organisation as well.
An international MSS for compliance programs would give guidance about how to set up the right procedures and processes to reduce the risk of non compliance, even inadvertently, with the law; an organisation's own internal policies; and any other voluntary standards or benchmarks the organsiation may be trying to meet.

An international MSS for compliance programs would provide a “road map” for organisations showing them the necessary structural elements or infrastructure required for an effective compliance program; what is needed for the program to operate on a day-to-day basis; and the requirements to maintain the program to operate effectively on an ongoing basis.

With the move towards the globalisation of rulemaking there is no universally acknowledged set of guidelines for how to establish and maintain effective systems to ensure compliance with these rules. If an international MSS for compliance systems was developed and implemented, an expected outcome would be that consumers could feel more confident in organisations that had a compliance system based on a standard for compliance programs, as they would have a greater chance of delivering the outcomes proposed by regulation. The assurance of an international MSS for compliance programs would also positively affect international trade as consumers and investors would have greater confidence in overseas organisations operating with a commonly understood and standardised compliance program.

In summary the development of an International MSS for Compliance Programs would:

- Provide a practical reference tool for organisations worldwide developing compliance programs (as it has already in Australia)
- It would provide an internationally recognised, agreed and understood benchmark for best practice in all organisation contexts.
- Such compliance programs provide an internal structure for organisations to ensure their stability; strategic execution and compliance with regulatory requirements (at a minimum)
- Increase market confidence
- Increase consumer confidence
- Improve outcomes for consumers and investors
- Provide a standard for regulators to assess the compliance performance of organisations without having to wait for breaches to occur
- It would enhance their risk management processes, including compliance, security, reputation management, business continuity planning and implementation
- Increased capability for effective decision-making and strategic planning, bearing in mind the regulatory and legislative parameters in which their business operates
- Provide evidence of ethical conduct, including openness, trust and meeting expectations of external stakeholders

The proposed MSS for compliance programs would be needed at global, regional, national and local levels, by all sectors.

The proposed MSS for compliance programs would apply to developed countries; countries such as Australia, Canada, USA and many areas of Europe where organisations are experienced in regulatory and legislative requirements and where these requirements are monitored and there are fines or other penalties in place for non compliance.

The proposed MSS for compliance programs would also apply to developing countries, especially for governments which are concerned with improvements in compliance, governance, accountability and appropriate administration. In particular, those countries developing their regulatory regimes would be interested in the standard as a benchmark for managing principles based regulation and compliance and for those countries interested in increasing their share of international financial and other trade by ensuring cross border consistency.

Need across sectors

The need for the proposed MSS for compliance programs is generic. The need exists in all sectors and in all organisations, of all sizes. The standard can be implemented on a ‘fit for purpose’ basis, meaning

organisations can apply it to best suit their organisation structure, size, market and sector and the scope of regulations and legislation that may apply to them. The Australian market already has experience of the standard being applied in this manner across a huge variety of sectors.

Importance of the need

The need is important for the following reasons:

- Intensified commercial competition and increased shareholder interests.
- Technological change leading to e-commerce and e-government practices, which brings with it increased international exposure and compliance requirements for organisations who may not previously have been exposed to these requirements.
- Increasingly open environment that requires partnerships and collaboration, knowledge sharing, and peering.
- Speed of communications and dissemination of information through the internet.
- Increasing complexity of the regulatory environment – local, national and international and increased exposure to cross border requirements.
- Increased expectations of citizens and customers that organisations should operate in a trustworthy, accountable, transparent and socially responsible manner.
- Heightened risk from the external environment including, for example, economic instability, security threats and natural disasters.
- Availability of a connected, integrated and internationally accepted standard is useful to governments as compliance requirements are managed in an international context.
- Alignment of compliance management with business processes. The proposed standard currently in use in Australia promotes consideration of and integration with business systems and strategic planning. Additionally, the existing standard in use in Australia is compatible with the ISO Risk Management Standard.
- It provides a robust structure to enable certification processes in countries which wish to do so.
- It provides an assessable practice benchmark for commercial arrangements involving multiple jurisdictions and/or countries.

The need will continue. There will be continuing and increasing demand for new requirements standards, guidelines standards and their regular review, to keep up-to-date with regulatory changes and business requirements and practices.

Determination of the importance of the need

Consultation with relevant parties leads us to believe that there is strong support for the development of an ISO standard.

The Australasian Compliance Institute has extensive overseas networks in Hong Kong, Singapore, Indonesia, South Africa, New Zealand, United States, Netherlands and the United Kingdom who have indicated support for an ISO standard as well as a need for such a standard. Anecdotal feedback from industry via ACI suggests that in the absence of an International Standard, many overseas organisations already make use of the Australian Standard informally when designing their programs but that their programs would attract greater support if the Standard was recognised by the ISO.

Known or expected support for the proposed MSS

Australasian Compliance Institute.

ACI members are drawn from many sectors of the economy and hold a variety of roles within large and small organisations including Heads of Compliance and Risk, Chief Executive Officers, Chief Financial Officers, General Counsel and Company Secretaries, General Managers, Senior Analysts, Compliance & Ethics Managers and Compliance Officers.

Industries represented within the membership include finance, insurance, utilities, mining, manufacturing, gaming, health, wholesale and retail, government, consulting and legal firms to name a few. We also have a growing body of regulators, including (but not limited to):

- **ASIC** - Australian Securities & Investment Commission
- **ACCC -** Australian Competition & Consumer Commission (Trade Practices)
- **APRA** - Australian Prudential Regulation Authority (Finance and Superannuation)
- **ASX** - Australian Securities Exchange
- **ATO** - Australian Tax Office
- **EPA** - Environmental Protection Authority
- **ICAC** - Independent Commission Against Corruption
- **AUSTRAC** – Australian Transaction Reports and Analysis Centre
- **Customs**
- **Essential Services Commission**
- **WorkCover Queensland**
- **Department of Climate Change**

(Contact: Martin Tolar, Chief Executive Officer, 02 92901788, Level 1
50 Clarence St Sydney NSW 2000

Australian Competition and Consumer Commission

Contact: John Martin, Commissioner, 02 62431111

Australian Government: The Treasury

The Australian Government has indicated significant support for this project and sees it as vital to all markets. Treasury is providing ACI with funding to enable the project to progress to ISO.

No bodies have indicated opposition.

4. Sector-specific MSS proposals

Application of the MSS for a single specific sector

The MSS for compliance programs is not intended for any single specific sector or industry. It would be applicable to all sectors and industries.

Referencing or incorporating existing ISO MSS

The ISO for Risk Management would also be utilised by many professionals and organisations who would use the proposed MSS for compliance programs, however it would not necessarily need to be referenced within the standard, although there is opportunity if the Committee considered that it would add value.

The need for particular sector-specific deviations from a generic MSS

The scope of MSS for compliance programs does not require sector-specific deviations.

If there is a requirement for a sector-specific deviation from a generic MSS, it would not be included in the products produced. Reference may be made to specific exclusions.

5. Value of an MSS

Public health and safety
Positive: An international standard could assist organisations of all sizes to set in place a program to implement health and safety regulations and laws which, in turn, should deliver positive outcomes for the public.
Negative: No foreseeable negative impacts.

Environmental impact
Positive: An international standard could assist organisations of all sizes to set in place a program to implement environmental regulations and standards which, in turn, should deliver positive outcomes for the public. Environmental concerns are increasing in importance with the impending implementation of the Carbon Emissions Trading Schemes in various jurisdictions.
Negative: No foreseeable negative impacts

Competition
Positive: Compliance and the Compliance Standard encourages and assists with the compliance of organisations with competition legislation. The Standard encourages the rewarding of behaviours by staff that support compliance, including behaviours that enable market competition (and discourages behaviours that are non-compliant such as collusion, etc.). The application of the Standard by an organisation may encourage consumer confidence in that individual organisation, giving it a competitive advantage, however that is also by definition the nature of a competitive market and does not in itself exclude any other organisation making use of the same tool to improve the reputation and consumer relationship with their organisation.
Negative: The international standard would have no negative impact on competition. For a start it is a guideline standard and, being principles based, not prescriptive. It is also a voluntary standard with no compulsion to be implemented.

Economic impact
Positive: Increased consumer and investor confidence in organisations and the market(s) due to improved compliance with rules and regulations through the application of the Standard by organisations. Potential for increased confidence in international markets due to a consistent standard being available in all countries. Potential for lowering of compliance program, system and training costs for organisations operating across multiple jurisdictions by the application of a standardised compliance program, that being principles based, can be applied to a variety of regulations and rules.
Negative: Use of the standard should impose only minimal cost on the user. Organisations already have a legal obligation to comply with the law and should already have structures in place to ensure this occurs. An international standard on compliance programs would simply be a guidance tool for how to set up an effective compliance program to meet those compliance obligations, establishing a best practice guide rather than a new 'regime' of regulations to comply with. In some instances it may, in fact, reduce compliance costs.

Standard and legislation
As stated above the intention would be to write a guideline standard for voluntary use, which would also provide a best practice benchmark.

Other benefits
For consumers
The ISO process offers real opportunities for the meaningful input of consumer perspectives, through the ISO Consumer Policy Committee (COPOLCO) and also through participation on Technical Committees, sub-committees and working groups. The potential benefits for consumers flowing from widespread adoption of an ISO standard on compliance programs includes:

- Consumers can be more confident that an organisation that implements an international standard on compliance programs will have a system that offers a greater certainty of

meeting its compliance commitments that may include laws, regulations and standards, rules covering cross-border and global issues
- Use of a practical and internationally recognised approach to implementation that offers the prospect of meaningful, verifiable, and measurable claims by organisations about progress towards standard objectives
- Increased level of customer satisfaction with organisations which adhere to ISO standards in the global market, thus enhancing the consumer-business relationship
- Increased confidence of the consumer that they are dealing with a reputable merchant whose system is ISO compliant
- Improved complaints-handling procedures (as part of the compliance program) to solve problems when they arise

For investors

The ISO process offers real opportunities for the meaningful input of investor perspectives, as it does for consumers. The potential benefits for investors flowing from widespread adoption of an ISO standard on compliance programs includes:

- Investors can be more confident that an organisation that implements an international standard on compliance programs will have a system that offers a greater certainty of meeting its compliance commitments that may include laws, regulations and standards, rules covering cross-border and global issues
- Use of a practical and internationally recognised approach to implementation that offers the prospect of meaningful, verifiable, and measurable claims by organisations about progress towards standard objectives
- Increased confidence of the investor that they are investing in a reputable organisation whose system is ISO compliant
- Likelihood of better outcomes for organisations, and thereby their investors, in volatile markets through compliance with regulation

For business

First and foremost, ISO represents a forum for the development of standards, with a long reputation for developing practical standards needed by the private sector. If business does not develop standards within an ISO framework, they may find that they will be developed for them. The potential benefits for business of an ISO standard on compliance programs includes that it:

- Gives business guidance on how to set up the appropriate in house procedures and practices to reduce the risk of breaching their commitment to compliance
- Reduces the risk of intervention by regulators
- Reduces the risk of reputational damage from non conformance with the law
- Reduce the risk of associated costs from non conformance with the law
- Provides a self regulatory mechanism for conformance with regulations
- Assists industry participants to become or remain responsible corporate citizens by providing them with a means of conforming to accepted norms of good behaviour
- Allows for regulators to recognise businesses who have implemented the standard
- Gives confidence that a foreign supplier has processes in place to meet local laws
- Through adequate documentation of a compliance program (as outlined in the Standard) may provide a due diligence defence mechanism should a breach occur
- Offers a standardised and strategic approach to compliance that may in practice lower compliance costs (especially if an organisation currently has an inefficient or ineffective program in place)
- Likelihood of better outcomes for organisations in volatile markets through compliance with regulation
- Provides an effective corporate compliance measurement approach

For regulators

The potential benefits for regulators of an ISO standard on compliance programs includes that it:

- Reduce regulatory costs for longer term
- Activate competition through consumer confidence in the market
- Utilised by a regulator, the standard could improve their understanding of compliance and assist them in assessing the state of compliance of an organisation
- This may mean that a regulator can get a sense of potential breaches or problems without the necessity of waiting for the breaches or market failures to occur
- Increased dialogue with industry (as encouraged by the Australian Standard)
- Increase effectiveness of policy outcomes
- Gets competitive advantages to organisations in the market

General expected benefits and costs to organisations

Benefits for small, medium and large organisations include:

- Common policy and practice benchmarks across geographical boundaries, including different countries, cultures and jurisdictions
- Ability to meet regulatory requirements, including accountability, ethical and corporate governance requirements; regulatory compliance; financial and practice audits
- Enables compliance with national and international legislation and codes of conduct
- Support of risk management, including security; reputation management; business continuity planning and implementation
- Ability to set and assess performance measures for the use of commercial service providers, and for inclusion in commercial contracts and conduct due diligence on suppliers, business partners and any organisations you may be outsourcing work to.
- Use of an MSS for compliance programs shows commitment to organisational governance, accountability and integrity
- The potential to make organisations more cost effective and efficient
- Scalable use of an internationally accepted system to meet business needs, resource availability and risk
- Similar guidelines do not exist in many countries at a national level
- Facilitation of communication between different countries on shared issues, and a forum for articulating common principles, minimum and best practice.

All organisations have compliance obligations which must be properly managed. Failure to do so incurs costs of human, physical and infrastructure resources. Managing compliance programs using an MSS standard supports cost effective operational processes.

The cost is commensurate with the scope of implementation within each organisation and is determined by business need and an assessment of risk.

The cost of implementing an MSS for compliance programs can provide short and long-term, positive return on investment.

How the benefits and the costs were determined

The assessment of the benefits and costs outlined above have been determined through ACI's strong understanding of the Australian experience with the implementation of AS 3806 for compliance programs; the experience of our members and their organisations and their feedback on the use of the standard;

and the experiences and feedback from regulators who supervise the various markets and sectors in Australia.

The MSS for compliance programs allows an organisation to competitively add to its management system beyond the standard

The proposed MSS for compliance programs will enable an organisation to implement its compliance management policies, processes, systems and practice to the level or levels required – based on assessment of business need, regulatory requirements and assessment of risk. An organisation can choose to go beyond a minimum level of conformance, and reach a higher level of capability which would improve overall organisational effectiveness and demonstrate continuous improvement. This could be for competitive advantage, market differentiation, or excellence in service delivery – depending on the sector in which the organisation operates.

Potential methods to demonstrate conformance for contractual or regulatory purposes

The MSS for compliance programs may be used for contractual or regulatory purposes in some jurisdictions in some countries.

This would be done by:

- Second or third party assessment
- Certification structures established by local (eg. national, state, regional) government authorities (eg. by an audit office)

First and second party assessments are likely to be done for business efficiency purposes.

The proposed MSS for compliance programs would enable organisations to be flexible in choosing the method of demonstrating conformance, and would be able to accommodate for changes in an organisation's operations, management, physical locations and equipment.

Benefits and costs to third-party registration/certification

Where third-party certification is adopted by a jurisdiction, the benefits to the organisation would include:

- Improving business processes and cost containment
- Attracting new customers
- Entering new markets, either locally or globally
- Qualification for a tender
- Qualification for a preferred supplier status
- Enhanced status.

Costs to the organisation may include costs of undertaking assessments prior to the certification audit/assessment – to determine the level of existing conformance and any corrective action that may be required. There may also be costs of audit/assessment services by the certifying body.

6. Risk of trade barriers

How the MSS facilitates or impacts global trade

The proposed MSS for compliance programs would facilitate global trade by:

- Provide a common standard for the transparency of compliance management arrangements and assurance

- Providing a framework for global certification – accepted and understood by potential trading partners
- Enabling a qualification framework for tendering.

The proposed MSS for compliance programs could not create a technical barrier to trade.

How the MSS could create or prevent a technical barrier to trade for small, medium or large organisations

The proposed MSS for compliance programs facilitates trade for organisations of all sizes by:

- Provide a common standard for the transparency of compliance management arrangements and assurance
- Providing a framework for global or local certification
- Enabling a qualification framework for tendering, or qualification for preferred provider status.

The proposed MSS for compliance programs would not create a technical barrier to trade for small, medium or large organisations.

How the MSS could create or prevent a technical barrier to trade for developing or developed countries

The proposed MSS for compliance programs prevents a technical barrier to trade for developing countries by:

- Provide a common standard for the transparency of compliance management arrangements and assurance
- Providing a framework for global certification – accepted and understood by potential trading partners
- Enabling a qualification framework for tendering.

The proposed MSS for compliance programs might create a technical barrier to trade for a developing country where trading partners require a level of compliance management capability that it is not able to meet. The barrier may be caused by political or economic factors. This is the same for all ISO standards.

Use of the proposed MSS in government regulations

The proposed MSS for compliance programs is likely to add to, enhance and support existing governmental regulations by providing practical guidance to organisationsation to assist them in implementing a management system or program to assist them in meeting their obligations.

7. Risk of incompatibility, redundancy and proliferation

Potential overlap or conflict with other existing or planned standards.

There is no known conflict or overlap with other ISO or non-ISO international standards, or standards at the national or regional level except as noted, with the existing Australian/New Zealand Standard for Compliance Programs, which is the proposed draft for consideration by the ISO.

Relationship of the MSS family and related conformity assessment activities to any existing developments

The proposed MSS family is not likely to replace, duplicate, conflict with or detract from any other ISO or non-ISO developments except the Australian/New Zealand Standard as earlier noted. However, this is

not anticipated to be an issue for either country because the adoption internationally would provide great benefit to those organisations already using this standard.

Likely promotion of other MSS's at the national or regional level

It is not likely that the proposed MSS for compliance programs will promote or stem proliferation of MSS's at the national or regional level, or by industry sectors. Where countries wish or plan to develop compliance management standards that may also be under development at ISO level, they may adopt the ISO standard as their national standard.

8. Other risk factors

The only foreseeable risks, which would be common to all standard proposals, would be:

- Lack of consensus;
- Loss of key people;
- Withdrawal of support.

We believe the likelihood of the above occurring would be low.

We base this on the fact that the Australian Standard for Compliance Programs 3806 was, and has been, embraced by industry and regulators as a best practice/benchmark document for compliance programs and has been actively promoted by the Australasian Compliance Institute.

At the time of drafting this proposal the G20 had recently met and agreed on the need for a global approach to the regulation of the financial services industry. An ISO standard on compliance programs would be a valuable tool to assist organisations to set in place effective regulatory systems based on agreed essential principles or features of a compliance program.

It would also provide regulators with a global standard that could be used to assess the effectiveness of compliance programs in organisations within their jurisdictions and help them to proactively assess the market weaknesses in regard to compliance and proactively take action, rather than needing to wait for breaches or failures to occur.

No other risks have been identified.