STANDARDS
Australia

AS 8001—2008

Fraud and Corruption Control

Australian
STANDARD

AS

This Australian Standard® was prepared by Committee MB-004, Business Governance. It was approved on behalf of the Council of Standards Australia on 26 October 2007.
This Standard was published on 6 March 2008.

The following are represented on Committee MB-004:

- Australian Corporate Lawyers Association
- Australian Federal Police
- Australian Institute of Company Directors
- Australian Institute of Professional Investigators
- Australian Society of Association Executives
- Centre for International Corporate Governance Research, Victoria University
- Chartered Secretaries Australia
- Engineers Australia
- Environment Institute of Australia and New Zeland
- Institute of Internal Auditors – Australia
- IAB Services
- Queensland University of Technology
- Risk Management Institution of Australasia
- Society of Consumer Affairs Professionals
- Transparency International Australia

This Standard was issued in draft form for comment as DR 06651.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Fraud and corruption control

Originated as AS 8001—2003.
Second edition 2008.

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

ISBN 0 7337 8522 0

PREFACE

This Standard was prepared by Standards Australia Committee MB-004, Business Governance, to supersede AS 8001—2003.

Major revisions to the Standard include—

- changes to structure and format;
- increased consideration of information systems as an enabler of fraud and corruption and as a means of detecting fraud and corruption;
- expanded guidance on the suggested role of the internal audit function in controlling the risk of fraud and corruption;
- separate consideration of corruption and the ways in which corruption risk can be managed;
- increased emphasis on example setting by senior executives as an important element of an entity's integrity framework;
- upgraded fraud risk assessment methodology (to bring it into line with changes to AS/NZS 4360:2004);
- upgraded employment screening guidelines;
- new customer and supplier vetting guidelines; and
- reference to the role of the external auditor in fraud detection.

The objective of this Standard is to provide an outline for a suggested approach to controlling the risk of fraud and corruption within a wide range of entities across all industry sectors and in government.

This revision reflects recent changes in the approach to controlling fraud and corruption in the Australian economy made necessary by technological advancement and the way business is conducted.

This Standard is part of the Corporate governance series which comprises—

AS 8000	Good governance principles
AS 8001	Fraud and corruption control (this Standard)
AS 8002	Organizational codes of conduct
AS 8003	Corporate social responsibility
AS 8004	Whistleblower protection programs for entities

In addition, the Standard links to other Standards as referred to herein—

AS/NZS 4360	*Risk management* (and companion handbooks—HB 436:2004, *Risk Management Guidelines—Companion to AS/NZS 4360:2004* and HB 158—2006, *Risk management—Delivering assurance based on AS/NZS 4360:2004*)
AS 4811	Employment screening

Additional guidance on applying this Standard in controlling the risk of fraud and corruption can be found in *Fraud Resistance—A practical guide* published by SIRCA and available from Standards Australia.

The term ‘informative’ has been used in this Standard to define the application of the accompanying appendices. An ‘informative’ appendix is for information and guidance only and should not be considered part of the Standard.

CONTENTS

Page

INTRODUCTION ... 6

SECTION 1 SCOPE AND GENERAL
1.1 SCOPE ... 11
1.2 APPLICATION ... 11
1.3 MINIMUM ACCEPTABLE COMPLIANCE AND GUIDANCE PROVISIONS ... 12
1.4 OBJECTIVE ... 12
1.5 REFERENCED DOCUMENTS ... 13
1.6 REFERENCES TO OTHER ANTI-FRAUD AND ANTI-CORRUPTION PRONOUNCEMENTS ... 14
1.7 DEFINITIONS ... 14
1.8 APPLICATION OF RISK MANAGEMENT PRINCIPLES TO FRAUD AND CORRUPTION RISK ... 16
1.9 STRUCTURE OF THIS STANDARD ... 17

SECTION 2 PLANNING AND RESOURCING
2.1 APPLICATION ... 19
2.2 FRAUD AND CORRUPTION CONTROL PLANNING ... 19
2.3 REVIEW OF THE FRAUD AND CORRUPTION CONTROL PLAN ... 20
2.4 FRAUD AND CORRUPTION CONTROL RESOURCES ... 21
2.5 INTERNAL AUDIT ACTIVITY IN THE CONTROL OF FRAUD AND CORRUPTION ... 22

SECTION 3 PREVENTION
3.1 APPLICATION ... 25
3.2 IMPLEMENTING AND MAINTAINING AN INTEGRITY FRAMEWORK ... 25
3.3 SENIOR MANAGEMENT COMMITMENT TO CONTROLLING THE RISKS OF FRAUD AND CORRUPTION ... 27
3.4 LINE MANAGEMENT ACCOUNTABILITY ... 28
3.5 INTERNAL CONTROL ... 29
3.6 ASSESSING FRAUD AND CORRUPTION RISK ... 30
3.7 COMMUNICATION AND AWARENESS ... 38
3.8 EMPLOYMENT SCREENING ... 39
3.9 SUPPLIER AND CUSTOMER VETTING ... 40
3.10 CONTROLLING THE RISK OF CORRUPTION ... 41

SECTION 4 DETECTION
4.1 APPLICATION ... 43
4.2 IMPLEMENTING A FRAUD AND CORRUPTION DETECTION PROGRAM ... 43
4.3 ROLE OF THE EXTERNAL AUDITOR IN THE DETECTION OF FRAUD ... 45
4.4 AVENUES FOR REPORTING SUSPECTED INCIDENTS ... 45
4.5 WHISTLEBLOWER PROTECTION PROGRAM ... 46

SECTION 5 RESPONSE
5.1 APPLICATION ... 47
5.2 POLICIES AND PROCEDURES ... 47
5.3 INVESTIGATION ... 47
5.4 INTERNAL REPORTING AND ESCALATION ... 49
5.5 DISCIPLINARY PROCEDURES ... 49

Page

5.6 EXTERNAL REPORTING 50
5.7 CIVIL ACTION FOR RECOVERY OF LOSSES—POLICY FOR RECOVERY ACTION 50
5.8 REVIEW OF INTERNAL CONTROLS 51
5.9 INSURANCE—CONSIDERATION OF THE NEED FOR FIDELITY GUARANTEE INSURANCE 51

APPENDICES

A SUGGESTED FRAMEWORK FOR A FRAUD AND CORRUPTION CONTROL PLAN 52
B FRAUD RISK SUMMARY 54

INTRODUCTION

Recent events within Australia and internationally suggest a strong nexus between fraud and corruption within entities on the one hand and fundamental governance failure at senior levels on the other.

Many corporate collapses arise from a conflict between the objectives of the entity and the personal objectives of the custodians of the entity's assets—the Directors and senior executives. This has resulted in an increasing incidence of financial reporting manipulation, sometimes excessive payment of remuneration and other benefits for senior executives and, at times, a crisis of confidence within global equity markets.

Managing business risk has, in recent years, increasingly been accepted as an important governance issue. This has been brought into focus by the Corporate Governance Guidelines issued by the Australian Stock Exchange and the CLERP 9 amendments to the *Corporations Act*. By logical extension, controlling the risk of fraud and corruption is a governance issue which must be given due attention by the controllers of all entities. Increasingly, major fraud incidents or endemic corruption within an entity will be viewed as indicative of a failure of the entity's controllers to discharge these more prescribed governance obligations.

Fraud and corruption involving Australian entities

A number of studies and surveys of fraud within the Australian economy have been conducted over the past ten years. The findings of this research[1] suggest:

- Fraud costs the Australian economy at least $3 billion per year.[2]
- The incidence of fraud within the Australian economy is increasing year by year[3] with up to 63% of Australian organizations experiencing economic crime over a two year period.[4]
- The larger the organization the more likely it is that it will suffer fraud or corruption at some point in its business cycle. For example, in one recent survey it was found that one hundred percent of organizations with more than 5000 employees reported at least one incident of economic crime over two years.[5]
- Survey results indicate that Australian organizations may suffer a higher rate of reported fraud than the global average.[6]
- Research into fraud and corruption in Australia over many years has consistently confirmed that, for the majority of Australian business entities (other than those conducting business in banking or insurance sectors), the main source of fraudulent and corrupt conduct will be from within the entity itself—typically for organizations external to the banking and insurance sectors, internal fraud will account for up to 75% in number of incidents and value of loss suffered.[7]

[1] See in particular, PricewaterhouseCoopers, *Global Economic Crime Survey* (Australian results) released in November 2005 and KPMG Australia Fraud Survey released in November 2006.

[2] Australian Institute of Criminology estimate of fraud in the Australian economy (1997).

[3] Statistics maintained by the Australian Institute of Criminology suggest that the rate of fraud reported to Australian police services per 100 000 head of population has doubled on average every ten years since the mid 1950s.

[4] PricewaterhouseCoopers (2005).

[5] PricewaterhouseCoopers (2005).

[6] PricewaterhouseCoopers (2005).

[7] PricewaterhouseCoopers (2005) and KPMG (2006).

- The financial impact of fraud and corruption on the victims, and in particular, Australian entities engaged in some form of business activity, is steadily increasing.
- The average financial loss associated with fraudulent conduct continues to increase.
- The involvement of organized crime in external attack on the financial sector within the Australian economy is increasing. It is apparent also that much external attack on Australian entities is instigated by or at the direction of criminal gangs based in other parts of the world who use tried and tested frauds against Australian entities.
- Identity theft which is made possible by the penetration of information systems within the wider community, the pace of business and increased educational standards of the perpetrators, is becoming the most important fraud-related threat within the Australian economy.
- Many Australian entities are ill-prepared to detect and prevent fraud against their business with many having made little or no progress in developing or implementing any form of effective fraud control strategy.
- A significant and increasing proportion of cases of fraud detected are not reported to the police or other law enforcement agency for investigation.

Fraud examples in Australian business

Examples of fraud (as distinct from the concept of ‘corruption’ which is dealt with later in this introduction) which occur in Australian business and therefore fall within the intended scope of this Standard are:

- Theft of plant and equipment by employees.[8]
- Theft of inventory by employees.[9]
- False invoicing (involving a staff member of the entity or a person external to the entity creating a fictitious invoice claiming payment for goods or services not delivered or exaggerating the value of goods delivered or services provided).
- Theft of funds other than by way of false invoicing.[10]
- Theft of cash (particularly in retail or other cash businesses) usually involving some form of concealment, e.g. lapping.
- Accounts receivable fraud (misappropriation or misdirection of remittances received by an entity from a debtor).
- Credit card fraud involving the unauthorized use of a credit card or credit card number issued to another person (the most common fraud against the banking sector) or the use of stolen or fraudulently generated credit card numbers by merchants.
- Lending fraud (loan application made in a false name and supported by false documentation).
- Theft of intellectual property or other confidential information.

[8] Theft of plant, equipment, inventory or other property by persons unconnected to the entity suffering the loss and where deception is not involved is not considered ‘fraud’ for the purposes of this Standard.

[9] Inventory theft is probably the most common employee instigated fraud type within the Australian economy and represents a significant loss in industries that handle large volumes of inventory. In the retail sector for example, it has been estimated by ECR Australia (Efficient Consumer Response) that 1.5% of retail turnover is lost to shrinkage. Traditionally, 45-50% of retail shrinkage is thought to be employee instigated.

[10] Workplace based on-line banking fraud has increased in frequency in recent years. This will typically involve an employee with some form of control over the management of the accounts payable function substituting their own account number for the account number of a legitimate vendor.

- Financial reporting fraud (falsification of the entity's financial statements with a view to obtaining some form of improper financial benefit).
- Release or use of misleading or inaccurate information for the purposes of deceiving, misleading or to hide wrongdoing.
- Insider trading (buying and selling shares on the basis of information coming into the possession of the perpetrator by reason of his or her position but which is not known to investors generally).
- Misuse of position by senior executives or directors in order to gain some form of financial advantage.

Fraudulent conduct by agents of Australian entities

Australian entities themselves (through their Directors and managers as their agents) sometimes become involved as perpetrator of fraudulent conduct in a number of ways including:

- Material and deliberate misstatement of accounting information for an improper purpose (for example to underpin a share price or to meet profitability or cash flow forecasts).
- Overcharging for goods and services in invoices rendered to customers and clients.
- Taking-up as revenue remittances received in error rather than allowing a credit to the payer.
- Tax evasion.
- Money laundering.
- Insider trading.
- Theft of intellectual property.

Explaining the increasing incidence of fraud

The reasons for the increasing incidence of fraud are many and varied but there are a number of consistent and recurring themes:

- The continual striving for greater efficiencies in business which leads to reduced staffing levels and a consequent reduction in internal control adherence.
- The increasing use and reliance on technology and the associated changes in payment systems and channels. Of particular concern is the ease with which commercial crime can operate globally, access accounts in countries on the other side of the globe and then transfer funds very quickly between accounts in a different jurisdiction with the intention of making it impossible to follow the trail let alone recover any of the proceeds.
- The continuing trend towards 'flattening' of organizational structures and the resulting reduction in management focus on enforcing internal controls and managing risk.
- Rapid and continuous changes to business operations.
- The increasing pace of business.
- The inability of the criminal justice system, the police, the Australian Securities and Investments Commission and other law enforcement agencies and the Courts, to keep pace with the ever-increasing workload and greater complexity of matters reported.
- The accessibility of gambling which has become a significant motivator for employees to commit fraud against their employer.
- Greater complexity of business relationships.

- Changing remuneration and incentive structures and arrangements.

The value to an entity of information held cannot be overstated. The loss of information through unauthorized system access can cause significant damage to an entity's reputation in the short- and long-term and must be treated as a serious threat. Controlling the risk of information theft by unauthorized internal or external access should be a matter of priority for entities whose businesses rely heavily on the information held.

Corruption involving Australian entities

Transparency International's *Corruption Perception Index* ('CPI') is a measure of the perception of the propensity for corruption of public officials within each country surveyed. The 2007 survey of 179 countries[11] found that Australia ranked equal 11th in terms of transparency in business dealings within the country. In other words, the Australian economy was seen as having a relatively low propensity for payment of bribes to the country's public officials in their business dealings with the private sector.

This compares with the *Bribe Payers Index 2006*[12] ('BPI') where Australia was ranked third out of the world's 30 leading exporting countries in terms of its perceived transparency in business dealings with public officials in foreign economies. This means that Australia is perceived as having a relatively low likelihood of paying bribes to public officials in foreign jurisdictions.

While this might be seen as a relatively good result for Australia, it does underscore the fact that there is at least the perception if not the reality of a measurable level of public corruption within the Australian economy.

Corrupt conduct to which Australian entities are subject and which are therefore within the intended scope of a corruption control program contemplated by this Standard include:

- Payment or receipt of secret commissions (bribes), which may be paid in money or in some other form of value to the receiver (e.g. building projects completed at an employee's private residence) and may relate to a specific decision or action by the receiver or generally.
- Release of confidential information for other than a proper business purpose in exchange for some form of non-financial benefit or advantage accruing to the employee releasing the information.
- Collusive tendering (the act of multiple tenderers for a particular contract colluding in preparation of their bids).
- Payment or solicitation of donations for an improper political purpose.
- Serious conflict of interest involving a Director or senior executive of an entity or other entity acting in his or her own self-interest rather than the interests of the entity to which he or she has been appointed (e.g. failing to declare to a Board an interest in a transaction the entity is about to enter into or excessive payment of remuneration to Directors and senior executives).
- Serious nepotism and cronyism where the appointee is inadequately qualified to perform the role to which he or she has been appointed.

[11] Transparency International *Corruption Perception Index* 2007 http://www.transparency.org/policy_research/surveys_indices/cpi/2007/ 'The index defines corruption as the abuse of public office for private gain, and measures the degree to which corruption is perceived to exist among a country's public officials and politicians'.

[12] Transparency International *Bribe Payers Index* 2006

- Manipulation of the procurement process by favouring one tenderer over others or selectively providing information to some tenderers. This frequently involves allowing tenderers to resubmit a ‘non-complying’ tender after being provided with the details of other bids.
- Gifts or entertainment intended to achieve a specific or generic commercial outcome in the short- or long-term—an essential element rendering conduct of this type corrupt would be that it is in breach of the entity’s values, behavioural code or gifts policy (or that of any relevant external party’s values or behavioural code) or that it was done without the appropriate transparency within one or more of the entities affected.
- Bribing officials (locally or in foreign jurisdictions) in order to secure a contract for the supply of goods or services.
- Private sector to private sector secret commissions to secure contracts.

Losses associated with the corruption of the procurement process result from reduced competition and the acceptance of substandard delivery of goods and services that would normally be rejected.

Private and public sector entities may also suffer loss if the winning tenderer attempts to recover the cost of the secret commission paid by loading the value of the bid either before or after the contract is awarded.

Managing the risks

An entity’s approach to managing the risks of fraud and corruption should be underpinned by an organization-wide policy developed with internal and external consultation with appropriate benchmarking against established best practice prevention and detection programs and standards. It should apply the principles of sound risk management, planning, monitoring and remedial action.

This Standard aims to provide entities with the tools they need to apply these general risk management principles to the control of fraud and corruption. While the Standard aims to provide a high-level framework for organizations to use in developing an anti-fraud program, additional guidance can be found in *Fraud Resistance—A practical guide* (SIRCA, 2003).

STANDARDS AUSTRALIA

Australian Standard
Fraud and corruption control

SECTION 1 SCOPE AND GENERAL

1.1 SCOPE

This Standard provides an outline for an approach to controlling fraud and corruption and, subject to the guidance at Clause 1.2 below, is intended to apply to all entities including government sector agencies, publicly listed corporations, private corporations, other business entities and not-for-profit organizations engaged in business or business-like activities.

Fraud and corruption contemplated by the Standard fall into three main categories[13]—

(a) fraud involving the misappropriation of assets;

(b) fraud involving the manipulation of financial reporting (either internal or external to the reporting entity); and

(c) corruption involving abuse of position for personal gain.

1.2 APPLICATION

While this Standard is intended to apply to all entities operating in Australia, the extent to which it would be applicable to individual entities will be dependent on the entity's—

(a) size;

(b) turnover;

(c) business diversity;

(d) geographic spread;

(e) reliance on technology; and

(f) the industry in which it operates.

By way of general guidance, it is anticipated that the whole Standard would apply to publicly listed corporations, large privately owned corporations and all government departments and agencies. These entities should typically look to implement this Standard in its entirety for maximum effect or to ensure that pre-existing fraud and corruption control measures are at least as robust as in this Standard.

Only relevant parts of this Standard are applicable to small and medium sized enterprises.

[13] Refer to Clause 1.7.3. for a definition of 'corruption' and to Clause 1.7.8 for a definition of 'fraud'.

1.3 MINIMUM ACCEPTABLE COMPLIANCE AND GUIDANCE PROVISIONS

Throughout this document, text given in bold is intended to represent minimum acceptable compliance for entities seeking to fully comply with the Standard. Content given in plain text is provided as guidance in interpreting and implementing the minimum acceptable compliance elements given in bold. Any entity claiming to be fully compliant with the Standard will, as a minimum, have implemented all of the minimum acceptable compliance level elements set out herein.

1.4 OBJECTIVE

The objective of this Standard is to outline a suggested approach to controlling fraud and corruption against and by Australian entities.[14]

The distinction between fraudulent and corrupt conduct against or by Australian entities is an important one because they involve quite different considerations and the differentiation is not just a matter of internal and external environments. In the first category, the entity is the victim or intended victim and will suffer, in most cases, a relatively minor impact to its reputation (depending on the quantum) should a fraud or corruption incident occur in addition to any economic loss suffered.

In the second category, the entity will usually be a beneficiary of the conduct until the conduct is discovered and exposed in which case the reputational impact on the organization and its business is likely to be substantial. Apart from the need to demonstrate that an entity is a responsible corporate citizen, avoidance of fraudulent or corrupt conduct by or on behalf of Australian entities is essential in order to safeguard the entity's ongoing reputation, which, once damaged, may prove difficult to repair.

The Standard is intended to be practical and effective guidance for entities wishing to implement a fraud and corruption control program covering the risks of fraud and corruption committed within the entity (with the entity as victim) as well as fraud and corruption committed by or in the name of the entity.

The Standard proposes an approach to controlling fraud and corruption through a process of—

(a) establishing the entity's fraud and corruption control objectives and values;

(b) setting the entity's anti-fraud and anti-corruption policies;

(c) developing, implementing, promulgating and maintaining an holistic integrity framework;

(d) fraud and corruption control planning;

(e) risk management including all aspects of identification, analysis, evaluation treatment, implementation, communication, monitoring and reporting;

(f) implementation of treatment strategies for fraud and corruption risks with a particular focus on intolerable risk;

(g) ongoing monitoring and improvement;

(h) awareness training;

(i) establishing clear accountability structures in terms of response and escalation of the investigation;

(j) establishing clear reporting policies and procedures;

(k) setting guidelines for the recovery of the proceeds of fraud or corruption; and

[14] Where the entity is the victim of fraud or corruption on the one hand and the perpetrator of fraud or corruption on the other.

(l) implementing other relevant strategies.[15]

Adoption of this Standard requires an appropriate level of forward planning and application of a structured risk management approach. The application of contemporary risk management principles is seen as fundamental to the prevention of fraud and corruption.

The objective of the fraud and corruption control program outlined by this Standard is the —

(i) elimination of internally and externally instigated fraud and corruption against the entity;

(ii) timely detection of all instances of fraud and corruption against the entity in the event that preventative strategies fail;

(iii) recovery for the entity of all property dishonestly appropriated or secure compensation equivalent to any loss suffered as a result of fraudulent or corrupt conduct; and

(iv) suppression of fraud and corruption by entities against other entities.[16]

While 'elimination' of fraud and corruption will, for many entities, be unachievable, it nevertheless should remain the ultimate objective of a fraud and corruption risk mitigation program subject to the appropriate cost-benefit analysis.

In some Australian industry sectors, there is an argument that fraud and corruption is so entrenched that it can never be fully eradicated. For example, it is unfeasible for externally instigated fraud to be eliminated within the banking sector—the nature of banking is such that a certain level of fraud and attempted fraud will always exist. On the other hand, in many entities operating within certain industry sectors, the complete elimination of opportunistic 'one-off' fraud and corruption incidents by application of an effective risk management approach would be feasible.

Any fraud prevention program will need to have regard to the resourcing constraints of the entity and the realities of the industry in which it operates.

1.5 REFERENCED DOCUMENTS

This Standard should be read, construed and applied in conjunction with the following Standards and Handbooks:

AS	
4811—2006	Employment screening
8000—2003	Good governance principles
8002—2003	Organizational codes of conduct
8003—2003	Corporate social responsibility
8004—2003	Whistleblower protection systems for entities
AS/NZS	
4360:2004	Risk management
HB	
158—2006	Delivering assurance based on AS/NZS 4360:2004 Risk Management
436:2004	Risk Management Guidelines (Companion to AS/NZS 4360:2004)

[15] Derived in part from the *Commonwealth Fraud Control Guidelines*.

[16] For example, corrupt activity by an entity involving the payment of bribes to officials in a foreign jurisdiction as defined within the *Criminal Code Act 1995 (Cwth)*.

ASA 240	The Auditor's Responsibility to Consider Fraud in an Audit of a Financial Report.

In addition, significant reference is made to the International Standards for the Professional Practice of Internal Auditing as applied by the Institute of Internal Auditors Australia.

1.6 REFERENCES TO OTHER ANTI-FRAUD AND ANTI-CORRUPTION PRONOUNCEMENTS

This Standard draws on a number of pronouncements and anti-fraud and anti-corruption initiatives developed in Australia and elsewhere including the following—

(a) The OECD Convention on Countering Bribery of Foreign Public Officials in International Business Transactions.[17]

(b) The Rules of Conduct to Combat Extortion and Bribery by the International Chamber of Commerce.[18]

(c) The Anti-Bribery provisions of the revised OECD Guidelines for Multinationals.

(d) *The Criminal Code Act* (Cwth).

(e) Commonwealth Fraud Control Guidelines.

(f) Commonwealth Fraud Control Schedules.

(g) Australian Government Investigation Standards.

(h) The Professional Practices Framework of the Institute of Internal Auditors (PPF).

(i) Fraud Resistance: A practical guide (SIRCA—2003).[19]

(j) Fraud and corruption prevention policies and guidelines used by various agencies in different levels and jurisdictions of government.

(k) Business Principles for Countering Bribery—TI Six Step Process'.[20]

1.7 DEFINITIONS

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

1.7.1 Bribe

The act of paying a secret commission to another individual. It is also used to describe the secret commission itself.[21]

1.7.2 Code of behaviour

A document (variously referred to as a 'Code of Ethics', 'Code of Conduct' and various other titles) broadly communicated within the entity setting out the entity's expected standards of behaviour.

1.7.3 Control (also 'internal control')

An existing process, policy, device, practice or other action that acts to minimize negative risks or enhance positive opportunities.[22]

[17] Effective from 15 February 1999.

[18] Adopted 26 March 1996.

[19] Available through Standards Australia

[20] http://www.transparency.org/global_priorities/private_sector/business_principles

[21] Refer definition of 'secret commission', Clause 1.7.15.

[22] Refer AS/NZS 4360:2004 Clause 1.3.

1.7.4 Corruption

Dishonest activity in which a director, executive, manager, employee or contractor of an entity acts contrary to the interests of the entity and abuses his/her position of trust in order to achieve some personal gain or advantage for him or herself or for another person or entity.[23] The concept of 'corruption' within this standard can also involve corrupt conduct by the entity, or a person purporting to act on behalf of and in the interests of the entity, in order to secure some form of improper advantage for the entity either directly or indirectly.[24]

1.7.5 Effective (*in the context of internal control effectiveness*)

In the context of fraud and corruption risk, an effective control is one that is considered to be effective in preventing or detecting fraud or corruption and therefore contributes to enabling the entity to achieve its overall goals and objectives.[25]

1.7.6 Entity

A corporation, government agency, not-for-profit organization or other entity engaged in business activity or transacting with other entities in a business-like setting.

1.7.7 Evidence

Oral testimony either given in legal proceedings or which a witness indicates he or she is prepared to give under oath or affirmation in legal proceedings and documents of any description that can legally be admitted as evidence in a Court of Law.

1.7.8 Fraud

Dishonest activity causing actual or potential financial loss to any person or entity including theft of moneys or other property by employees or persons external to the entity and where deception is used at the time, immediately before or immediately following the activity. This also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit.

The theft of property belonging to an entity by a person or persons internal to the entity but where deception is not used is also considered 'fraud' for the purposes of this Standard.

NOTE: The concept of fraud within the meaning of this Standard can involve fraudulent or corrupt conduct by internal or external parties targeting the entity or fraudulent or corrupt conduct by the entity itself targeting external parties.[26]

1.7.9 Fraud and corruption risk assessment

The application of risk management principles and techniques in the assessment of the risk of fraud and corruption within an entity.[27]

1.7.10 Fraud and corruption control plan

A document summarizing an entity's anti-fraud and anti-corruption strategies.

[23] Refer Clause 1.8 for examples of the types of corrupt conduct contemplated by this Standard.

[24] Refer to Introduction for examples of the types of fraudulent conduct contemplated by this Standard.

[25] Refer HB 158—2006.

[26] Refer to Foreword for examples of the types of fraudulent conduct contemplated by this Standard.

[27] Refer to AS/NZS 4360:2004.

1.7.11 Ineffective (*in the context of internal control effectiveness*)

An internal control which, by reason of its not operating as intended or some other factor, is making little or no contribution to mitigating the fraud or corrupt risk under consideration and therefore makes little or no contribution towards the entity's achievement of its business goals and objectives.[28]

1.7.12 Investigation

A search for evidence connecting or tending to connect a person (either a natural person or a body corporate) with conduct that infringes the criminal law or the policies and standards set by the affected entity.

1.7.13 Partially effective (*in the context of internal control effectiveness*)

An internal control which, by reason of its not operating as intended or due to some other factor, is not fully effective in managing the risk it is intended to manage but is making some contribution towards managing the fraud and corruption risk under consideration and therefore makes some contribution towards the entity meeting its goals and objectives.[29]

1.7.14 Risk

The chance of something happening that will have an impact upon objectives.[30] In consideration of fraud and corruption risk, this will generally be a negative impact.

1.7.15 Secret commission

A payment in money or in kind which will or is intended to cause a person to act in a way that is contrary to the interests of his or her principal or employer, is contrary to the principal's or employer's policy on a given issue or is against the public interest. Secret commissions, by definition, will typically be paid without the knowledge or express or implicit agreement of the principal or employer and include payments intended to influence the outcome of a specific action or event as well as the actions generally over a period of time.

1.7.16 Senior management

Personnel associated with an entity at the senior management, Director or principal level and who have authority over the direction or management of the entity.

1.7.17 Serious (*in the context of a risk or event*)

Likely to have more than an immaterial impact on the entity, if it occurred, with the potential to threaten the business' economic viability in the short, medium or long term or to have a noticeable impact on the organization's business reputation.

1.8 APPLICATION OF RISK MANAGEMENT PRINCIPLES TO FRAUD AND CORRUPTION RISK

Fraud and corruption is a risk to business and can have a similar impact on an affected entity as other types of enterprise risk in terms of—

(a) financial loss;

(b) reputational impact;

(c) diversion of management energy;

(d) organizational morale;

[28] Refer HB 158—2006.

[29] Refer HB 158—2006.

[30] Refer to AS/NZS 4360:2004 Clause 1.3.13.

(e) organizational disruption;

(f) loss of employment;

(g) reduced performance; and

(h) diminished safety.

All entities operating in all sectors deal with risk on a daily basis. Risk-conscious entities manage enterprise risk by a targeted and strategic process of—

(i) identifying serious risks;

(ii) measuring the risks relative to all other serious risks facing the entity;

(iii) identifying the source/cause of the risk and the scenario(s) under which it can occur;

(iv) prioritizing identified risks from most serious to least serious;

(v) evaluating the degree of tolerance towards the risk;

(vi) developing action items aimed at treating the entity's risks;

(vii) installing a process for feedback and reporting non-compliance; and

(viii) monitoring and reporting including consideration of the changing status of the context and status of risks, ongoing effectiveness of controls and progression treatment.

An entity can use these principles in a structured and strategic way in order to control the risk of fraud and corruption within its business operations.

1.9 STRUCTURE OF THIS STANDARD

Fraud and corruption control is generally a narrowly applied concept in this country.

In many Australian entities, 'fraud and corruption control' frequently is seen as a 'reactive' strategy that does not commence until an incident is discovered following which an investigation is conducted and appropriate disciplinary or other action taken against employees and external parties involved. In those entities, little or no emphasis is placed on a proactive fraud and corruption risk management program.

In some entities, at the other extreme, fraud and corruption control is almost wholly 'proactive' with no effective response if a fraud or corruption incident does occur. In those organizations, employees who have defrauded their employer of significant sums are allowed to leave the organization with no requirement to make restitution and no risk of criminal action, the organization content to rectify any internal control weaknesses to ensure such an incident does not recur.

In some entities, there are proactive prevention and reactive programs in place but nothing in terms of fraud and corruption detection.

This Standard views fraud and corruption control as an holistic concept involving implementation and continuous monitoring and improvement across three key themes[31]—

(a) prevention;

(b) detection; and

(c) response.

In addition to these key themes, the Standard includes guidance on planning and resourcing the elements of a fraud and corruption control program.

[31] This structure for a fraud and corruption control program was suggested by the KPMG Forensic Fraud Risk Management Whitepaper issued in November 2005.

The Fraud and Corruption control Plan is set out in four sections of this Standard, as follows:

Section 2 Planning and resourcing

Section 3 Prevention

Section 4 Detection

Section 5 Response

Figure 1 is a diagrammatic overview of the structure of this Standard.

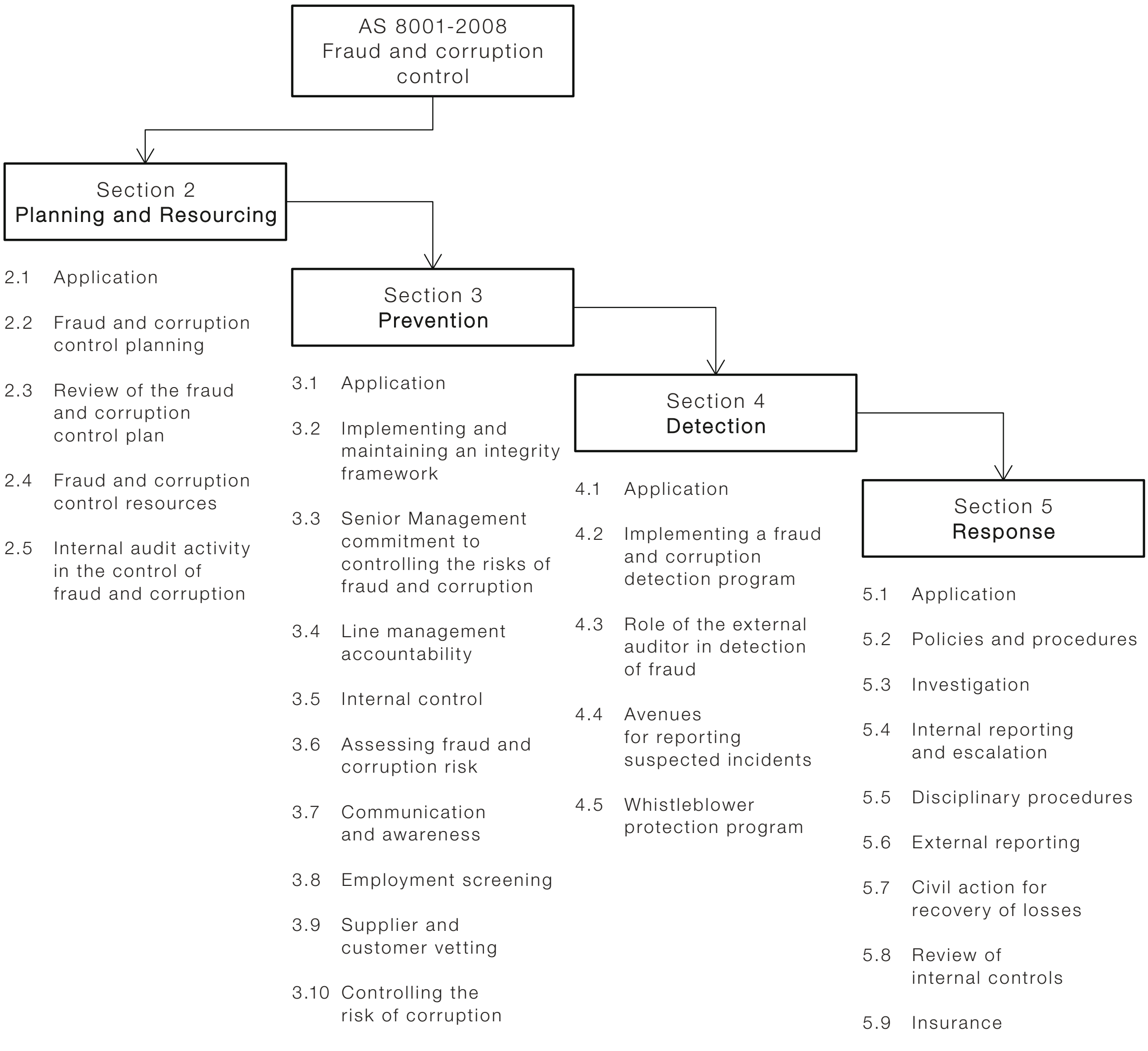

AS 8001-2008
Fraud and corruption control
Section 2
Planning and Resourcing
2.1 Application
2.2 Fraud and corruption control planning
2.3 Review of the fraud and corruption control plan
2.4 Fraud and corruption control resources
2.5 Internal audit activity in the control of fraud and corruption
Section 3
Prevention
3.1 Application
3.2 Implementing and maintaining an integrity framework
3.3 Senior Management commitment to controlling the risks of fraud and corruption
3.4 Line management accountability
3.5 Internal control
3.6 Assessing fraud and corruption risk
3.7 Communication and awareness
3.8 Employment screening
3.9 Supplier and customer vetting
3.10 Controlling the risk of corruption
Section 4
Detection
4.1 Application
4.2 Implementing a fraud and corruption detection program
4.3 Role of the external auditor in detection of fraud
4.4 Avenues for reporting suspected incidents
4.5 Whistleblower protection program
Section 5
Response
5.1 Application
5.2 Policies and procedures
5.3 Investigation
5.4 Internal reporting and escalation
5.5 Disciplinary procedures
5.6 External reporting
5.7 Civil action for recovery of losses
5.8 Review of internal controls
5.9 Insurance

FIGURE 1 STRUCTURE OF THIS STANDARD

SECTION 2 PLANNING AND RESOURCING

2.1 APPLICATION

The planning and resourcing elements outlined in this Section represent the suggested actions to be undertaken by entities wishing to develop and implement a fraud and corruption control program. Proper planning and coordinated resourcing are key elements in any anti-fraud/anti-corruption program.

Compliance with this Standard requires an entity to implement each of the minimum acceptable compliance[32] planning and resourcing initiatives in a way that is appropriate to the entity having regard to its size, diversity, geographic spread, risk profile and the industry sector in which it operates.

2.2 FRAUD AND CORRUPTION CONTROL PLANNING

2.2.1 Implementing a Fraud and Corruption Control Plan

Entities should develop and implement a Fraud and Corruption Control Plan documenting the entity's approach to controlling fraud and corruption exposure at strategic, tactical and operational levels. The Fraud and Corruption Control Plan should detail the entity's intended action in implementing and monitoring the entity's fraud and corruption prevention, detection and response initiatives.

It is important that entities view the Fraud and Corruption Control Plan as an integral part of an overall risk management plan on the premise that fraud and corruption are business risks that are controlled by the application of risk management principles.

In terms of the development of a Fraud and Corruption Control Plan, a preliminary assessment of fraud and corruption risk should be completed in order to better scope the entity's future fraud control program that will be documented in the plan.

Accountability for the implementation and ongoing monitoring of the plan should be allocated to a person with appropriate seniority, skills and experience and sufficient time allotment to discharge this responsibility under the direction of an appropriately constituted committee appointed for the purpose. [33]

NOTE: The need for a specific Fraud and Corruption Control Plan may arise out of the results of an enterprise-wide risk assessment where fraud or corruption risk has been identified as a serious threat to the entity.

2.2.2 Developing a Fraud and Corruption Control Plan

The Fraud and Corruption Control Plan should take into account any existing policies dealing with fraud and corruption risk. Duplication, inconsistency and uncertainty should be avoided. The Fraud and Corruption Control Plan should be viewed as a comprehensive framework for addressing fraud and corruption risk with appropriate linkage to other entity-wide pronouncements aimed at reducing the entity's exposure.

NOTE: Entities developing a Fraud and Corruption Control Plan should have regard to the framework set out at Appendix A.

[32] Refer to Clause 1.3 for the distinction between 'minimum acceptable compliance' and 'guidance' provisions of the Standard.

[33] See Clause 2.4 for a description of the level of seniority of the fraud control resource within the entity.

2.2.3 Monitoring the operation of a Fraud and Corruption Control Plan

A program for monitoring the implementation of the Fraud and Corruption Control Plan should be established, setting out internal and external monitoring processes and outlining key milestones, the resources required and the objectives to be achieved.

Review of the Fraud and Corruption Control Plan is necessary to identify and understand reasons for any non-conformance and to identify and design measures for improvement. The purpose of such a review is to ensure that the fraud and corruption control program is—

(a) appropriate for the entity's current operations; and

(b) achieving the objectives for which it was established.

2.2.4 Communicating the Fraud and Corruption Control Plan

An entity's commitment to its Fraud and Corruption Control Plan should be communicated to all external stakeholders, for example, by way of—

(a) an appropriate note to the entity's annual report as part of a general declaration of integrity or corporate governance;

(b) declarations in general terms and conditions of business dealings with external parties;

(c) declarations in 'requests for tender' or similar invitations to propose to the entity; and

(d) on the entity's website.

Internally, regular communication is necessary to ensure management and staff are informed of fraud and corruption control issues including current best practice. The Fraud and Corruption Control Plan should be accessible to all personnel, particularly those with specific (as distinct from generally applicable) fraud and corruption control accountabilities.

2.3 REVIEW OF THE FRAUD AND CORRUPTION CONTROL PLAN

2.3.1 Frequency of review

An entity's Fraud and Corruption Control Plan should be reviewed and amended at intervals appropriate to the entity but, at a minimum, once every two years. Entities operating in rapidly changing business conditions (including and in particular, in conditions of significant technological change) should review and update the Fraud and Corruption Control Plan more frequently.

2.3.2 Process of continuous improvement

An entity's Fraud and Corruption Control Plan should be viewed as a document in a constant state of evolution given the rapidly changing environment in which Australian businesses operate.

2.3.3 Factors to be considered in reviewing a Fraud and Corruption Control Plan

In reviewing the entity's Fraud and Corruption Control Plan, regard should be given to—

(a) confirmation or amendment to the entity's fraud and corruption control objectives;

(b) significant changes in the entity's business conditions;

(c) strategies arising out of recently detected fraud or corruption control incidents;

(d) the results of any fraud and corruption risk assessments that have been completed since the most recent version of the Fraud and Corruption Control Plan;

(e) changes in fraud and corruption control practice locally and internationally;

(f) resourcing requirements and, in particular, ensuring that the anti-fraud and anti-corruption human resources are appropriately senior[34] and skilled for the role and that they have a sufficient allocation of time to discharge their responsibilities; and

(g) the changing nature of fraud and corruption in specific industry sectors globally e.g. the global shift of organized crime to fraud underpinned by more effective investigation of traditional organized crime activities, greater technology available to organized crime and higher educational standards of organized criminals.[35]

2.4 FRAUD AND CORRUPTION CONTROL RESOURCES

2.4.1 Allocation of resources

Entities should ensure that an appropriate level of resources is applied to controlling fraud and corruption risk. This should include an allocation of specialized personnel (on a full-time or part-time basis as appropriate) to implement the entity's fraud and corruption control initiatives, to coordinate the fraud and corruption risk assessment process, to record and collate fraud and corruption incident reports and to conduct or coordinate the entity's investigations into allegations of fraud and corruption.

Entities should consider the recruitment of specialist resources (internal or external to the entity) with the requisite skills and experience or alternatively, training existing personnel in this role.

A large entity should demonstrate its commitment to fraud and corruption control by allocating to a senior person (ideally no more than two levels removed from the CEO or, alternatively, with a direct line of reporting to the CEO on fraud and corruption control issues), overall responsibility for implementing and overseeing the fraud and corruption control program. Smaller entities should use a senior person who would include fraud and corruption control supervision as part of their broader responsibilities.

2.4.2 Appointment of a Fraud and Corruption Control Officer

Larger organizations should consider the appointment of a Fraud and Corruption Control Officer with either a full-time or part-time responsibility for managing the entity's exposure to these risks (whether the position is a full-or part-time responsibility will depend mainly on the size of the entity). The position description for this role should include reference to fraud and corruption control as a primary accountability.

It is desirable that the person appointed to the position of Fraud and Corruption Control Officer should have the capacity to understand and translate current best practice in fraud and corruption control into user-friendly practices and procedures in addition to delivering/coordinating training on relevant procedures, particularly to line management.

A Fraud and Corruption Control Officer should remain up-to-date with current best practice in fraud and corruption control by—

(a) a program of formal training;

(b) attendance at relevant seminars, conferences and workshops;

(c) maintaining a library of reference materials; and

(d) networking with other fraud and corruption control people.

[34] See Clause 2.4.1

[35] Banks and other entities in the financial services sector need to remain ever vigilant for the latest trends in fraud and corruption and adopt an approach aimed at managing the risk and reducing or eliminating fraud and corruption incidents within the entity.

In many larger entities, parts of the entity's fraud and corruption control infrastructure will already be in place and therefore practices may only need modification to bring them into line with current best practice.

2.4.3 Other fraud and corruption control resources

Other important resources within the entity in terms of controlling fraud and corruption include—

(a) human resources/industrial relations;

(b) occupational health and safety personnel;

(c) compliance professionals;

(d) corporate counsel;

(e) quality assurance;

(f) records management;

(g) corporate risk management;

(h) insurance manager;

(i) information security specialists and consultants;

(j) regulatory affairs managers; and where relevant

(k) environmental impact practitioners.

The Fraud Control Officer (if appointed) should have responsibility for ensuring that all of the entity's fraud and corruption control resources are coordinated so that they work together in a coordinated fashion in a way that achieves the objectives set out in the Fraud and Corruption Control Plan.

An oversighting committee should have ultimate responsibility for ensuring that fraud and corruption control outcomes are delivered, including a responsibility for ensuring that fraud and corruption control resources are effectively coordinated.

2.5 INTERNAL AUDIT ACTIVITY IN THE CONTROL OF FRAUD AND CORRUPTION

2.5.1 Application of internal audit resource in controlling fraud and corruption

While primary responsibility for the identification of fraud and corruption within an entity rests with management, entities should recognize that internal audit activity can be, in the context of addressing all business risks, an effective part of the overall control environment to identify the indicators of fraud and corruption.

Internal audit activity should be planned and conducted in accordance with fraud detection, deterrence and response provisions of The Professional Practices Framework (PPF) of the Institute of Internal Auditors.[36]

2.5.2 Application of The Professional Practices Framework of the Institute of Internal Auditors

Experience has shown that internal audit activity can be effective in the detection of fraud and also in the prevention of fraud by ensuring due adherence to internal control systems.[37]

[36] Refer to The Professional Practices Framework—PA 1210 for more specific guidance on the role of internal audit activity in the identification and detection of fraud.

[37] The Ernst and Young 9thGlobal Fraud Survey concluded that 30% of the Australian respondents identified Internal Audit as the most important factor in fraud prevention and detection (compared with 46% who believed a strong internal control environment was the most important factor).

Organizations should consider the role of internal audit in the detection, prevention and investigation of fraud and, in doing so, should have regard to the PPF which provides—

> *The internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.* [38]

Practice Advisory 1210.A2-1 and 1210.A2-2 issued on 5 January 2001 provide guidance in the interpretation of the International Standards for the Professional Practice of Internal Auditing as follows.

2.5.3 Internal auditor's role in deterring fraud

Practice Advisory 1210.A2-1[39] provides—

5. *Internal auditors are responsible for assisting in the deterrence of fraud by examining and evaluating the adequacy and the effectiveness of the system of internal control, commensurate with the extent of the potential exposure/risk in the various segments of the organization's operation. In carrying out this responsibility, internal auditors should, for example, determine whether—*

   - *The organizational environment fosters control consciousness.*
   - *Realistic organizational goals and objectives are set.*
   - *Written policies (e.g. code of conduct) exist that describe prohibited activities and the action required whenever violations are discovered.*
   - *Appropriate authorization policies for transactions are established and maintained.*
   - *Policies, practices, procedures, reports and other mechanisms are developed to monitor activities and safeguard assets, particularly in high risk areas.*
   - *Communication channels provide management with adequate and reliable information.*
   - *Recommendations need to be made for the establishment or enhancement of cost-effective controls to help deter fraud.*

2.5.4 Internal auditor's role in responding to fraud detected or suspected

Practice Advisory 1210.A2-1 provides—

6. *When an internal auditor suspects wrongdoing, the appropriate authorities within the organization should be informed. The internal auditor may recommend whatever investigation is considered necessary in the circumstances. Thereafter the auditor should follow up to see that the internal auditing activity's responsibilities have been met.*

Clauses 7 to 11 of the Practice Advisory deal with the role of the internal auditor in the investigation and reporting of detected fraud.

[38] Refer The Professional Practices Framework of the Institute of Internal Auditors PA 1210.A2.

[39] The numbering system within Practice Advisory 1210.A2-1 and 1210.A2-2 is used in the extracts given in this Section.

2.5.5 Internal auditor's role in detecting fraud

Practice Advisory 1210.A2-2 provides—

1. *Management and the internal audit activity have differing roles with respect to fraud detection. The normal course of work for the internal audit activity is to provide an independent appraisal, examination, and evaluation of an organization's activities as a service to the organization. The objective of internal auditing in fraud detection is to assist members of the organization in the effective discharge of their responsibilities by furnishing them with analyses, appraisals, recommendations, counsel, and information concerning the activities reviewed. The engagement objective includes promoting effective control at a reasonable cost.*

2. *Management has a responsibility to establish and maintain an effective control system at a reasonable cost. To the degree that fraud may be present in activities covered in the normal course of work as defined above, internal auditors have a responsibility to exercise due professional care as specifically defined in Standard 1220, with respect to fraud detection.*

3. *A well designed internal control system should not be conducive to fraud. Tests conducted by auditors, along with reasonable controls established by management, improve the likelihood that any existing fraud indicators will be detected and considered for further investigation.*

Practice Advisory 1210.A2-1 provides—

12. *Detection of fraud consists of identifying indicators of fraud sufficient to warrant recommending an investigation. These indicators may arise as a result of controls established by management, tests conducted by auditors, and other sources both within and outside the organization.*

13. *In conducting engagements, the internal auditor's responsibilities for detecting fraud are to—*

    - *Have sufficient knowledge of fraud to be able to identify indicators that fraud may have been committed.*

    - *Be alert to opportunities, such as control weaknesses, that could allow fraud. If significant control weaknesses are detected, additional tests conducted by internal auditors should include tests directed toward identification of other indicators of fraud.*

    - *Evaluate the indicators that fraud may have been committed and decide whether any further action is necessary or whether an investigation should be recommended.*

    - *Notify the appropriate authorities within the organization if a determination is made that there are sufficient indicators of the commission of a fraud to recommend an investigation.*

SECTION 3 PREVENTION

3.1 APPLICATION

The prevention elements outlined in this Section represent the suggested action to be undertaken by entities wishing to develop and implement a comprehensive fraud and corruption control program. The content of this Section considers the proactive elements of an entity's fraud and corruption control program.

Compliance with this Standard requires an entity to implement each of the minimum acceptable compliance[40] level preventive initiatives in a way that is appropriate to the entity having regard to its size, diversity, geographic spread, risk profile and the industry sector in which it operates.

3.2 IMPLEMENTING AND MAINTAINING AN INTEGRITY FRAMEWORK

3.2.1 Building an ethical culture

A key strategy in managing the risk of fraud and corruption within an entity is the implementation and maintenance of a sound ethical culture. An entity should aim to ensure that it has a healthy and sustainable ethical culture through the implementation of an integrity framework which should include a process of benchmarking and continuous monitoring underpinned by a program of example setting by senior management.

If the entity's observable ethical culture falls below acceptable levels, remedial action including a broad-based communication and training program should be undertaken as a matter of priority. All employees, including management, Directors and others concerned with the entity's business operations in any capacity, should be required to confirm in writing, annually, that they have, over the previous twelve months, complied with the entity's Code of Conduct and fraud and corruption policies and that they will so comply over the ensuing twelve months.

3.2.2 The elements of an integrity framework

Many entities take the view that promoting an ethical culture is achieved by issuing a code of expected behaviour (variously known as a Code of Conduct or Code of Ethics). Recent research has shown that promulgating a code of behaviour will be more effective if it is implemented as part of a coordinated approach—a code of behaviour is an important element, but not the only element, of an effective integrity framework.

The fundamental elements of a sound integrity framework are set out in Table 1. Entities should consider these concepts and implement them where appropriate.

[40] Refer to Clause 1.3 for the distinction between 'minimum acceptable compliance' and 'guidance' provisions of the Standard.

TABLE 1
FUNDAMENTAL ELEMENTS OF AN INTEGRITY FRAMEWORK

Element	Description
1 Integrity framework	An appropriate integrity framework developed using a participatory approach which builds commitment from all employees and is subject to ongoing monitoring and maintenance. Will include the development and promulgation of the other fundamental elements set out below.
2 Example setting	Observable adherence to the entity's integrity framework by senior management.
3 Senior management	Senior management group that recognizes the need for establishing and maintaining an ethical culture and actively promotes such a culture.
4 Codes of behaviour	A comprehensive Code of Ethics/Code of Conduct incorporating a high level aspirational statement of values with limited detail of unacceptable behaviour—a Code of Conduct will be more prescriptive as appropriate to the entity's content.
5 Allocation of responsibility	Responsibility assigned to a senior person for ensuring the entity's integrity initiatives are implemented and monitored. This person would have a direct line of reporting to the Ethics Committee or another senior management body with overall responsibility for the entity's ethical culture. In addition to allocation of specific responsibility for improving the entity's performance on this issue, it should be clearly communicated internally that every person associated with the entity has a role to play in driving integrity and ethical behaviour.
6 Ethics committee	An Ethics Committee, once appointed, will be the final arbiter on issues of apparent misconduct and ethical dilemmas that cannot otherwise be resolved at line-management level. It is typically also the body charged with overseeing the operation and maintenance of the entity's entire integrity framework. This committee can either be a board or management committee as appropriate to the entity's governance framework.
7 Communication	A program for communicating the entity's Code of Ethics/Code of Conduct. Communication of the importance of ethical standards through regular dissemination of material via newsletters and web sites.
8 Training	Specific ongoing training in the use of codes of behaviour and ethical tools for decision-making. Feature ethics components in all training.
9 Reinforcement	Incorporation of an integrated ethical standard into performance management, e.g. 360 degree feedback, performance appraisal systems and remuneration strategies.
10 Benchmarking	A program for continuous benchmarking of ethical standards aimed at identifying improvement in the entity's ethical standards over time and between different elements of the entity – the entity should also publish the results of a written social/ethics audit to all key stakeholders.
11 Reporting of complaints	A mechanism for the communication of ethical concerns inside and outside the normal channels of communication.
12 Compliance	A policy requiring all personnel to sign an annual statement to the effect that they have complied with all necessary corporate policies in connection with conflict of interest, disclosure of confidential information and other relevant ethics related issues.

3.2.3 Ongoing monitoring of an entity's ethical culture

An entity should conduct a regular assessment of its ethical culture for comparison between the various business units and for comparison of the entity's performance over time. This will involve the distribution of a structured questionnaire to all personnel and collating and analysing the results.[41] Remedial action based on the deficiencies noted (e.g. training, workshop series, intranet based training program, relaunching the entity's code of behaviour) should be undertaken.

3.2.4 Other guidance

Appendix B of AS 8000—2003 discusses the underlying values of ethical culture and the need for a sound ethical culture. AS 8002—2003 sets out more detailed guidance for implementing an effective Code of Conduct and entities should make reference to that Standard.

The Good Governance Principles developed by the Australian Stock Exchange provide useful guidance on developing and implementing a Code of Conduct under Principle 3—'Promote ethical and responsible decision making'.

Consideration of the guidelines is mandatory for publicly listed Australian corporations under the ASX Listing Rules.[42]

3.3 SENIOR MANAGEMENT COMMITMENT TO CONTROLLING THE RISKS OF FRAUD AND CORRUPTION

3.3.1 Risk consciousness

Entities should ensure that senior management[43] has an observably high level of commitment to controlling the risks of fraud and corruption both against the entity and by the entity (e.g. in terms of ensuring that the entity and the entity's own people do not engage in fraudulent or corrupt behaviour in their dealings with other parties).

A high level of risk consciousness for the risks of fraud and corruption should be present across the senior management group and, if found to be absent, should be the subject of appropriate awareness training at senior levels. This awareness training should include awareness of new types of technology that may be used for the commission of fraud and technological measures that can be used by an entity to minimize new types of fraud.

3.3.2 Consideration of fraud and corruption as a serious risk

An important factor contributing to a fraud and corruption-prone environment in Australian business is a fundamental failure of senior management to treat the risks as a serious threat to their entity and a consequent failure to allocate sufficient resources to managing the problem.

In many cases, senior management tend towards complacency and become concerned with fraud or corruption risk only after a major incident has occurred and, typically, only after serious financial and reputational damage has been done. One possible reason for this is that fraud or corruption incidents, for most entities, arise only occasionally—recent experience shows however, that when they do occur, significant economic loss and reputational damage can result.

Entities exhibiting 'best practice' in the control of fraud and corruption will invariably have a senior management group that recognizes the need for fraud and corruption prevention and detection even in the absence of recently detected incidents.

[41] This may be achieved by utilization of 'web-enabled' technology.

[42] http://www.asx.com.au/supervision/governance/principles_good_corporate_governance.htm

[43] Refer Definitions at Clause 1.7.

3.3.3 Senior management awareness of fraud and corruption issues

Senior management should, as a minimum, have an understanding of the following fraud and corruption issues:

(a) The incidence of fraud and corruption generally in Australia.

(b) The types of fraud and corruption common within the industry sector in which the entity operates and the losses typically associated with conduct of this type.

(c) The robustness of the entity's internal control environment in terms of its ability to prevent and detect the types of fraud and corruption likely to occur.

(d) A knowledge of the types of fraud and corruption that have been detected in the entity in the last five years and how those matters were dealt with in terms of disciplinary action and internal control enhancement.

(e) The entity's own fraud and corruption prevention and control strategy.

(f) Knowledge of new technology tools for detecting and preventing fraudulent activity.

3.4 LINE MANAGEMENT ACCOUNTABILITY

3.4.1 Accountability for prevention and detection of fraud

Entities should ensure that line managers are aware of their accountabilities for the prevention and detection of fraud and corruption. The management of fraud and corruption should be incorporated into the performance measurement system and each line manager's performance should be measured against benchmarks appropriate for the industry or sector in which the entity operates.

3.4.2 The need for a 'whole of business' approach to controlling fraud and corruption

Fraud and corruption control is often seen as a 'corporate' responsibility (i.e. the responsibility of central management at the corporate level) rather than as a responsibility for local or line management. Often fraud occurs in business operations geographically remote from the entity's central management because the local business operation is not subject to adequate corporate level scrutiny and local management do not see the need for fraud and corruption control measures.

It is an underlying principle of this Standard that no one strategy by itself can be effective in managing the risks of fraud and corruption and it follows therefore that no one person or category of person can be fully effective in managing the risks.

3.4.3 Achieving line management awareness of their accountability for controlling fraud and corruption

Line management needs to be made fully aware that managing fraud and corruption is as much part of their responsibility as managing other types of enterprise risk. In order to reinforce this, it is important that a program be developed and implemented including the following elements:

- Fraud and corruption control are incorporated into the performance management system.
- Preventing fraud and corruption should be specified in the position description of line managers.
- Any losses due to fraud and corruption should be allocated against the profit/cost centre in which the loss occurred and therefore have a financial impact on the performance of that profit/cost centre.

- Line managers should receive appropriate training on fraud and corruption control and during this training be informed of their specific fraud and corruption control accountabilities.

3.5 INTERNAL CONTROL

3.5.1 Implementing an effective system of internal control

Entities should ensure that all business processes, particularly those assessed as having a higher predisposition to the risks of fraud and corruption, are subject to a rigorous system of internal controls that are well documented, updated regularly and understood by all personnel.

> **NOTE: There is a strong link between the incidence of fraud and corruption and poor internal control systems within the entity. In many cases where fraud and corruption is detected, it is possible to identify a fundamental internal control weakness or failure that either allowed the incident to occur or failed to detect it quickly after it occurred. It follows that tight internal control is an effective weapon in protecting an entity against fraud.**

3.5.2 The role of the internal control system in preventing fraud and corruption

It can be difficult, in the current competitive business environment, to maintain or even bolster an internal control system at a time when business is seeking to streamline business operations in order to drive down costs. The role of internal control in securing the entity's property is often not well understood at senior levels in Australia's major corporations.

Internal control should be considered the first line of defence in the fight against fraud and corruption. While an entity that only has an effective internal control system is not fully protected against fraud, it is clear that such a system is an essential element of an adequate fraud control program.

3.5.3 Issues for consideration in developing an internal control system that will be effective in preventing fraud

The following are the suggested elements of an internal control system that will assist an entity to protect itself against the risk of fraud and corruption:

(a) Internal controls that are, to an appropriate degree, risk focused, in other words, they have been developed after the entity has taken into account the risks it faces and are aimed at mitigating those risks (ideally this will involve a development of internal controls that target risks identified by application of AS/NZS 4360:2004).

(b) Internal controls that are appropriately documented.

(c) A process of continuous improvement—internal controls that are reviewed and amended regularly.

(d) Internal controls that are communicated effectively to all personnel appropriate to their level of responsibility and position description.

(e) Internal controls that are accessible to personnel—if an entity's personnel have ready access to the entity's intranet site, the most recent version of a given internal control system can be quickly and efficiently accessed.

(f) A strong internal control culture in which all personnel understand the importance of adhering to internal control—this may include internal control adherence as an element of the regular performance review program.

(g) A program for assessing compliance with the entity's internal controls—this can be done by way of an online staff survey.

(h) Senior management setting an example of internal control adherence.

(i) An internal audit program that incorporates a review of adherence to internal control.

3.6 ASSESSING FRAUD AND CORRUPTION RISK

3.6.1 Implementing a policy for assessing the risk of fraud and corruption

Entities should adopt a policy and processes for the systematic identification, analysis and evaluation ('risk assessment') of fraud and corruption risk and should periodically conduct a comprehensive assessment of the risks of fraud and corruption within their business operations.

The frequency with which the entity should conduct an assessment of fraud and corruption risk will be dependent upon factors such as the entity's size, diversity of business functions, geographic distribution, the extent to which the entity is monitored by other entities or regulators, the rate of technological change and the risks inherent within the industry sector in which the entity operates. Typically such an assessment should be conducted at least every two years.

The fraud and corruption risk assessment should be conducted in accordance with AS/NZS 4360:2004 and companion handbook, HB 436:2004. The overarching principle of the recommended process is an assessment of consequence and likelihood for each risk relative to other fraud risks and relative to other enterprise risks.

The most important outcome of the fraud and corruption risk assessment process is the development of an effective anti-fraud and anti-corruption treatment program that specifically addresses the risks faced by the entity. These measures should be monitored for effectiveness over time.

NOTE: The need for a fraud and corruption risk assessment may be identified from an enterprise-wide assessment of business risk.

3.6.2 Application of risk management principles to assessment of fraud and corruption risk

AS/NZS 4360:2004 contemplates a seven stage process of risk assessment the main elements of which are—

(a) communicate and consult;

(b) establish the context;

(c) identify risks;

(d) analyse risks;

(e) evaluate risks;

(f) treat risks; and

(g) monitor and review.

Figure 2 is a diagrammatic summary of this process.

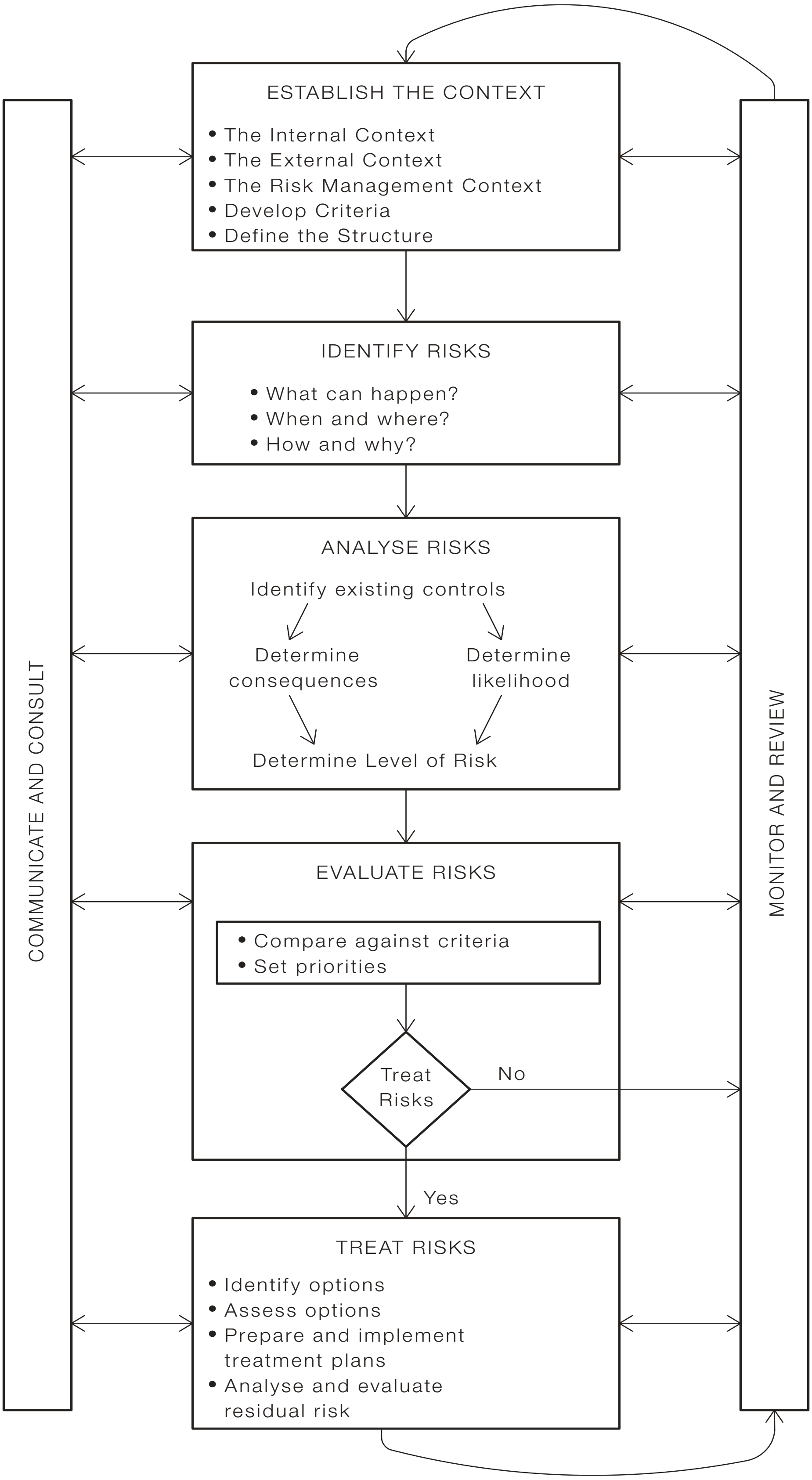


FIGURE 2 GENERIC RISK MANAGEMENT PROCESS[44]

[44] AS/NZS 4360:2004 Clause 2.2 (Figure 3.1).

3.6.3 Fraud and corruption risk assessment process

3.6.3.1 *Methodologies for assessing fraud and corruption risk*

Entities carrying out an assessment of fraud and corruption risk have traditionally used one of the following three alternative methodologies:

(a) Independent assessment of processes and procedures including a series of one-on-one interviews with relevant personnel and internal control documentation review.

(b) A survey of fraud and corruption risk by the issue and analysis of a questionnaire tailored for the entity or those business units or operational functions of the entity being assessed.

(c) A facilitated or consultative 'workshop' approach involving maximum input of personnel from the business unit being assessed wherein a 'risk assessment team' formed for each business unit identifies and assesses the risks relevant to the business unit.

This suggested approach is consistent with the guidance set out in HB 436:2004 which proposes the following four alternative methodologies in the identification of organizational risk[45]:

(1) Team-based brainstorming.

(2) Structured techniques such as flow charting, system design review, systems analysis, Hazard and Operability (HAZOP) studies and operational modelling.

(3) For less clearly defined situations, such as the identification of strategic risks, processes with a more general structure such as 'what if' and scenario analysis could be used.

(4) Where resources are constrained, a more flexible approach may need to be used for example, focusing on a smaller number of key elements or using a checklist approach.

The choice of the most appropriate approach (or combination of approaches) will be dependent upon a range of factors, including—budget, time availability of participants, urgency, structural and geographical constraints.

In relation to each risk identified, AS/NZS 4360:2004 requires that the assessment process include—

(i) preliminary assessment of the risks that have been identified in order to consider which risks should be subject to more detailed analysis;

(ii) evaluation of existing processes, devices or practices (internal controls) that act to minimize risks;

(iii) an assessment of consequences for the entity if the risk did occur;

(iv) an assessment of the likelihood of the event occurring in the context of the existing strategies and controls; and

(v) an estimate of the level of risk by combining the consequences and likelihood[46].

The ultimate objective of the risk assessment process will be an understanding of the risks of fraud and corruption facing the organization as a basis for developing and implementing action items aimed at further mitigation of the risks[47].

[45] Refer to HB 436:2004 Clause 5.5.

[46] AS/NZS 4360:2004 Clauses 3.4.1—3.4.5 and HB 436:2004 Section 6.

[47] Note also that in the 1999 edition of AS/NZS 4360:2004, there was a reference to 'Inherent Risk'. As all references to the concept of 'Inherent Risk' were removed from AS/NZS 4360:2004 they have been similarly removed from this Standard

The output from a consideration of these parameters could be a chart in the format shown in Appendix B, in which each risk is plotted according to its relative likelihood of occurrence and consequence for the entity if that fraud or corruption type did occur. While some form of graphical representation of the risks identified is considered advantageous, formats other than that shown in Appendix B could be used and would be equally valid.

3.6.3.2 *Steps of the risk assessment process*

Details of each of the steps of the risk assessment process as set out in Figure 2 having regard to the particular application of the process to the assessment of fraud and corruption risk follow:

(a) *Establishing the context*

For a risk assessment to be effective, it needs to be conducted with a full consideration of the context within which an entity operates. This will involve gaining an understanding of the entity's—

- external context which defines the relationship between the entity and its external environment, including consideration of the nature of threats facing the entity, 'fraud and corruption drivers' within the industry and broader environment within which the entity operates, and jurisdictional and regulatory requirements;
- internal context which provides an understanding of the entity, including consideration of the nature of the business, its culture, key stakeholders, historical fraud and corruption incidents and trends, key business drivers, its information systems and the operation of its control environment;
- risk management context, which involves determining the scope, boundaries and parameters of the fraud and corruption risk management activities to be undertaken;
- risk criteria, by which each risk will be evaluated to determine whether the risk can be tolerated or will require treatment; and
- approach and structure for the rest of the fraud and corruption risk management process to be undertaken.
- Documenting the establishment of the context is a good business practice that should be followed whenever practical.

(b) *Identifying the risks*

The objective of risk identification is to develop a listing of fraud and corruption risks and their sources that could have a potential impact on the achievement of the entity's objectives. A comprehensive list of risks should be created, irrespective of whether they are under the control of the entity or not. Such a listing is commonly referred to as a risk register, which should be documented with sufficient detail to facilitate both subsequent analysis and future reviews of fraud and corruption.

A number of approaches can greatly facilitate an improved understanding of risk sources, including—

- the mapping of business processes in consultation with the 'owners' and 'operators' of those processes;
- defining plausible modus operandi of potential fraud and corruption incidents; and
- examining the results of previous fraud and corruption investigations from within the entity and case studies from other entities.

(c) *Analysing the risks*

Risk analysis is a mechanism by which an improved understanding of those risks is achieved, ultimately to facilitate enhanced consideration of treatment options. The analysis of risk involves an examination of the consequences of those risks and their respective likelihoods in light of the effectiveness of the range of controls present.

A preliminary analysis of risk may be conducted as a screening device to eliminate 'low risks' and to allow attention and resources to focus on higher level risks for more detailed and thorough analysis. The more detailed analysis of risk will generally commence with an examination of the effectiveness of existing controls in managing those risks identified. The assessment should conclude, in relation to each control, whether it is or is likely to be—

- effective;
- partially effective; or
- ineffective,

in mitigating the fraud or corruption risk to which it relates.[48]

Controls that should be considered include any that may affect either the consequence or likelihood of the fraud or corruption risk, such as—

- regulatory requirements and standards;
- culture and ethical behaviour frameworks;
- policies and governance practices;
- recruitment practices, including pre- and in-employment screening;
- standard operating procedures;
- reconciliation, assurance and audit practices;
- logical and physical security practices, systems and infrastructure;
- incident reporting and investigation processes; and
- monitoring and management reporting.

The assessment of each internal control considered should not represent an assessment of the control in terms of its ability to mitigate business risk generally. Rather, it is an assessment of that control's perceived impact on the specific fraud or corruption risk under consideration.

In undertaking analysis of the risks, the measurement of consequence is commonly based on the level of financial loss that could potentially occur, which may be rated for either losses from a single incident or cumulative losses over a determined time period. However, fraud and corruption risks may also give rise to a range of non-financial consequences that should also be considered including regulatory, legal, safety, business performance, stakeholder confidence, reputation, staff welfare and morale impacts. For example, a fraud or corruption incident could occur that has an immediate minor financial consequence but a much more significant longer term erosion of brand value.

[48] Refer to Clause 1.7 for definitions relating to control effectiveness. Refer also to HB 158—2006 for addition guidance on internal control development.

The likelihood of a fraud or corruption event is measured in consideration of the *consequence of the risk should it occur*. The context will largely determine the likelihood scales[49] that should be used. For example, such scales could be based upon likelihood over the life of the entity, for the duration of the entity's presence in specific markets or locations, or over other defined periods of time or activity.

There is a range of other factors (generally specific to certain types of fraud and corruption risk) that may have an effect on either the consequence or likelihood which should be considered, including the following:

Consequence for the entity if the risk did occur

(1) The potential quantum of loss that would be suffered by the entity

The consequence of a fraud or corruption incident of the type contemplated will typically have a financial impact on the entity. The financial consequence directly associated with fraud or corruption of the type contemplated if it occurred, should be considered relative to all other risks facing the entity (i.e. not just limited to the financial impact likely to arise in relation to other fraud or corruption risks).

(2) The financial and non-financial impact to the entity of investigating and dealing with typical breaches of the risk contemplated.

The potential quantum of loss should also consider the 'legal consequences' flowing from a detected incident of fraud or corruption including Directors' liability, liability for employee actions and third party losses. Other financial impacts would include losses arising out of interruption of the business, diminution in share price and management distraction.

(3) The impact on the entity's reputation with stakeholders, government, shareholders and its business reputation generally

The consequences of such an incident will also include non-financial or reputational consequences which should be taken into account in assessing the impact on the entity.

Likelihood of the risk occurring

(4) The volume of transactions associated with the specific business function

The greater the number of transactions associated with a business function, the greater the relative risk of fraud or corruption associated with that business function.

(5) The extent to which technology is involved in the transactions associated with the fraud or corruption risk

Transactions that are heavily reliant on technology are at greater risk of fraud than those that involve manual processing because detailed human scrutiny of the transactions is often lacking or at a much higher level than manually processed transactions.

(6) The nature of the potential benefit to the perpetrators

Attractive assets such as cash or items that can be readily converted into cash are more likely to be misappropriated than less attractive assets and would be indicative of a higher disposition to fraud risk than assets that are less desirable.

(7) The previous incidence of the risk within the entity

Arguably, the higher the number of incidents of the type within entity, the more likely it is that

[49] HB 436:2004 has examples of consequence and likelihood scales that could be adapted to meet different entities' needs.

	such an incident would recur.
(8) The previous incidence of the risk within the industry in which the entity operates within the economy generally	The higher the number of incidents of the type within the industry in which the entity operates (or within the economy generally), the more likely it is that such an incident would occur within the entity's own operation.
(9) Current state of the entity's integrity culture (generally within the entity and specifically within the business unit concerned in which the risk is identified)	Fraud and corruption is more likely to occur in entities that have poor integrity culture. An entity's integrity culture should be considered separately to its internal control culture which would be taken into account when considering internal control risk.

Risk analysis can be conducted using qualitative (based upon descriptive rather than numerical methods), semi-quantitative (where values are assigned to descriptive scales) or quantitative (use of numerical scales) for both consequence and likelihood.[50]

Graphical approaches may be used to illustrate relative rankings and assist in subsequent evaluation of the risks.

(d) *Evaluating the risks*

Evaluation of fraud and corruption risks is undertaken to facilitate decisions on the needs and priorities for treatment of those risks. Such decision making is guided by those criteria developed as part of establishing the context in the early stages of the risk management process. These decision making criteria[51] may include—

- level of assessed risk;
- relative rankings of the risks;
- potential consequences should the risk eventuate, or the cumulative consequences of multiple events;
- likelihood of the events or of their outcomes;
- defined levels of tolerance; and
- the degree or range of uncertainty in the assessment of risk.

The output from the evaluation should present identified risks that are tolerable or intolerable, and that require treatment or not. The evaluation may however indicate that there is insufficient information on which a treatment decision can be made at that time and that further analysis is warranted.

(e) *Treating the risks*

In 'treating the risks' decisions are made on the most appropriate treatment options to be pursued for each fraud or corruption risk. Consideration of treatment options should consider both positive and negative outcomes that may arise from implementing each treatment option. Where an approach such as a 'cost benefit analysis' is used to assist decision making, care needs to be taken to ensure that both tangible (for example financial) and non-tangible outcomes are examined. The range of options that should be considered include—

- avoid the risk by not commencing or discontinuing activities that may give risk to the risk;

[50] Refer to HB 436:2006 for further information on different approaches to risk assessment.

[51] Refer to Clause 7.2 HB 436:2006.

- change the likelihood (reduce) of the event or of its negative consequences occurring, for example by improving defensive security measures;
- change the consequences (reduce negative, enhance positive) of the event, for example by having robust detection and investigation procedures in place;
- share the risk, for example through fidelity guarantee insurance and or business disruption insurance; and
- retain the risk, for example through accepting residual risk remaining following on from other treatment activities.

Decisions undertaken for evaluation and treatment of risk should consider the total cost of the fraud or corruption risk under consideration, including increases or reductions in spending on controls as a result of the proposed treatment options, such as—

- direct and collateral losses arising should the risk occur;
- costs of existing anticipatory controls and proposed treatment options, such as—

  —ongoing risk assessment;

  —prevention;

  —deterrence;

  —detection; and
- reactionary costs of responding to risk should it eventuate, such as—

  —investigation of the fraud or corruption event(s);

  —recovery of value lost as a result of the risk eventuating, including any legal costs incurred; and

  —restoration of the capacity and capability of the entity to its pre-event levels.

All actions proposed by the risk assessment team should be validated with management or senior management as appropriate prior to implementation.

It is important also to develop a strategy that will ensure comprehensive implementation and provide for a periodic check of progress. This will be assisted if personal responsibility is allocated at the time of the development of the action item. Such strategies usually form the basis of the Fraud and Corruption Control Plan.

3.6.4 Monitoring and review

Entities should regularly monitor and review any changes to the context, its risk environment and the effectiveness and efficiencies of its controls. Entities should also periodically review the progress of implementing agreed fraud and corruption risk treatments and their effectiveness at managing the risks. Any treatments that have not been fully implemented should be considered for relevance and likely impact on the relevant risk.

Entities should consider the involvement of external expertise in the review of fraud and corruption control strategies, for example, expertise in IT or legal compliance.

The entity should also consider benchmarking its own performance in this area against other entities operating in the same industry sector. The benefits flowing from each action item should be compared with the intended benefits and any necessary adjustments made.

3.7 COMMUNICATION AND AWARENESS

3.7.1 Awareness of fraud and corruption issues

Every staff member (management and non-management) should have general awareness of fraud and corruption and how he or she should respond if this type of activity is detected or suspected. Entities should regularly communicate to staff a clear definition of the types of behaviour that constitute fraudulent or corrupt practice, the fraud detection measures that are in place and an unequivocal statement that fraudulent and corrupt practices within the entity will not be tolerated.

NOTE:Internal fraud or corruption can be detected by observation, investigation and reporting by workplace colleagues of the perpetrator(s). Similarly, the most likely way for externally instigated fraud or corruption to be detected is by an employee of the victim entity.

3.7.2 The need for fraud and corruption awareness

An important element of any fraud and corruption control program is awareness in the minds of all management and non-management personnel of the various aspects of fraud and corruption risk including early warning signs and how to respond if fraud or corruption is suspected.

It is also important for all management and staff to have a clear understanding of the types of activities that the entity regards as fraudulent or corrupt (refer also to Clause 3.2 in relation to the need for developing an appropriate ethical culture).

The primary purpose of fraud and corruption awareness training is to assist in the prevention and control of fraud by raising the general level of awareness amongst all employees. A significant proportion of fraud and corruption is not identified at an early stage because of the inability of the entity's staff to recognize the warning signs, because they are unsure how to report their suspicions or they have a lack of confidence in the integrity of the reporting system or the investigation process.

3.7.3 Fostering fraud and corruption awareness within an entity

An awareness of the risk of fraud and corruption control techniques and the entity's attitude to control of fraud and corruption will be fostered by—

(a) ensuring all appropriate employees receive training in the entity's Code of Conduct and other elements of the entity's integrity framework at induction and throughout the period of their employment;

(b) ensuring all employees receive regular fraud awareness training appropriate to their level of responsibility;

(c) ensuring updates and changes to fraud-related policies, procedures, the Code of Conduct and other ethical pronouncements are effectively communicated to all employees;

(d) ensuring staff are aware of the alternative ways in which they can report allegations or concerns regarding fraud or unethical conduct[52]; and

(e) encouraging staff to report any suspected incidence of fraud or corruption.

Additionally, fraud and corruption awareness and standards of conduct should be promoted through regular meetings within each business unit, through staff newsletters or other internal publications, and through the overt, ongoing commitment demonstrated by senior management in all aspects of their relationship with the entity.

[52] Refer to Clause 4.4 for guidance on establishing alternative means of reporting suspicions of fraud and corruption.

Management need to have an awareness of their legal obligations in relation to employee rights, for instance, under the federal *Privacy Act 1988*.

3.8 EMPLOYMENT SCREENING

3.8.1 Implementing a robust employment screening program

The employment screening process is dealt with in AS 4811—2006 and it involves verifying, with the consent of the individual, the identity, integrity and credentials of an entrusted person. Organizations should consider the applicability of AS 4811 to their own circumstances, and if appropriate, implement the provisions of that Standard.[53]

Employment screening should be conducted within the confines of relevant legislation and with the informed and express consent of the entrusted person. Employment screening is contemplated for all new employees joining the organization (including contractors) and all personnel being transferred to a senior executive position or to a position considered by the entity to be 'higher-risk' in terms of the potential exposure to fraud or corruption associated with those positions.

NOTE: A thorough employment screening process is considered to be an effective way of reducing an entity's potential exposure to internally focused fraud and corruption. The objective of the screening process is to reduce the risk of a potential security breach and to obtain a higher level of assurance as to the integrity, identity and credentials of personnel employed by the entity.

3.8.2 Developing an employment screening policy

Many employees who have committed workplace fraud are found subsequently to have a history of dishonest conduct with previous employers.[54] It follows then that preventing employees with a history of dishonest conduct in the workplace joining the entity will reduce the risk of fraudulent or corrupt conduct.

A process should be developed that provides for effective employment screening of entrusted persons—

(a) before appointment;

(b) upon promotion or change of employment circumstances particularly if the person is being promoted to a senior position or to a position involving a higher risk of fraud or corruption; and

(c) prior to the completion of the probationary period.

The requirement for honest and full disclosure during the screening process should be a condition of initial and ongoing employment.

This process should also include systematic and regular reviews of—

(i) those positions with particular risk exposures; and

(ii) any changes in an employee's personal circumstances.

[53] For the purpose of AS 4811—2006, an entrusted person is defined as 'any individual that is, or is targeted to be, employed within an organization that is, or will be, entrusted with resources and/or assets.'

[54] Refer to KPMG Fraud Survey 2006 that found that 14% of employees involved in fraudulent conduct within the entity had a prior history of dishonest conduct with a previous employer compared with 7% in the 2004 survey.

With respect to changes to an entrusted person's personal circumstances, all current and potential trusted persons should be required to sign a declaration stating that they will notify their employer should there be a significant change in their circumstances (such as being charged with a criminal offence, bankruptcy etc.). This should be part of the annual declaration referred to in Clause 3.2 dealing with the requirement for management and employees to sign an annual statement of compliance with the entity's code of behaviour.

3.8.3 Enquiries to be undertaken

The types of enquiries which should be carried out as part of the employment screening process include, but are not limited to—

(a) verification of identity requiring at least two forms of identity document (passport, full birth certificate, driver's licence, rate notice);

(b) police criminal history search;

(c) reference checks with the two most recent employers—this will normally require telephone contact;

(d) a consideration of any gaps in employment history and the reasons for those gaps; and

(e) verification of formal qualifications claimed.

Refer to AS 4811—2006 for more particulars on employment screening.

3.9 SUPPLIER AND CUSTOMER VETTING

3.9.1 Verification of suppliers and customers

Entities should take steps to ensure the bona fides of new suppliers and customers and periodically confirm the bona fides of continuing suppliers and customers. The entity should consider its ongoing commercial relationship with the other party if enquiry finds a heightened risk of fraud or corruption in continuing to deal with that party.

NOTE: There is a significant risk of external party fraud and corruption in the Australian economy. This can take the form of a contracted party manipulating the procurement process or soliciting the payment of secret commissions.

3.9.2 The case for vetting of suppliers and customers

While much fraud and corruption in Australia is instigated by persons internal to an organization, there is a growing sense that Australian business is becoming increasingly susceptible to externally instigated fraud. The banking/finance and insurance sectors have traditionally been the targets of external perpetrators of fraud but this is now gradually extending to other parts of the economy[55]. In addition, there is growing evidence of the involvement of organized crime in external fraudulent attack on Australian corporations and government agencies.

Corruption typically perpetrated by external parties involves manipulation of the procurement process by paying or offering bribes. The risk of fraud or corruption will be reduced if the entity knows who it is dealing with in all significant commercial transactions.

Recent changes to anti-money laundering and financing of terrorism legislation around the globe have also changed requirements for more active vetting of other parties with which the entity deals.

[55] KPMG Fraud Survey 2006 Section 1.5.

3.9.3 Enquiries to be undertaken

A process should be developed that provides for effective vetting of suppliers and customers which may represent an extension of pre-existing credit checks already carried out by the entity. If the customer or supplier is a corporation, the enquiries would typically include—

(a) search of company register;

(b) ABN confirmation;

(c) verification of the personal details of directors;

(d) director bankruptcy search;

(e) disqualified director search;

(f) assessment of credit rating;

(g) search of legal proceedings pending and judgments entered;

(h) telephone listing verification;

(i) trading address verification; and

(j) media search.

3.10 CONTROLLING THE RISK OF CORRUPTION

3.10.1 Specific measures for countering the risk of corruption

Entities should separately consider measures aimed at controlling the risks of corruption—both corruption in which employees and others connected with the entity are targeted by external parties and corruption in which employees and others connected with the entity target external parties, in order to derive an improper benefit for the entity.

Specific measures to be included in an anti-corruption program should include—

- **a program for corruption resistance wherein the entity makes a strong anti-corruption statement (in terms of both incoming and outgoing corrupt conduct) which is properly communicated and then consistently applied throughout the entity;**
- **implementing a policy of personnel rotation so that improper relationships are less likely to develop;**
- **consideration of requiring ‘vendor audits’ of ‘high-risk’ providers;**
- **enhanced probity and contracting procedures;**
- **opening channels of communication within the entity so that employees have a range of alternative avenues for reporting concerns in relation to possible corrupt conduct**[56]**; and**
- **opening channels of communication with customers, vendors and other third parties aimed at encouraging those parties to come forward if there is an indication of corrupt conduct involving the entity or any person associated with the entity.**

[56] Refer Clause 4.4 for guidance on implementing alternative fraud and corruption reporting strategies.

3.10.2 Other guidance

An entity cannot successfully implement a ‘no corruption’ policy in order to defend the entity against corrupt attack from external parties while at the same time engaging in corruption itself.

Transparency International released a booklet titled ‘Business Principles for Countering Bribery — TI Six Step Process’.[57] The booklet provides guidance on six anti-corruption fundamentals—

- decide on a no-bribes policy;
- plan the implementation;
- develop the program content;
- implement the program;
- monitor the program; and
- evaluate the program.

This document represents valuable guidance in establishing a program specifically targeting corruption as contemplated by this Standard.

[57] http://www.transparency.org/global_priorities/private_sector/business_principles

SECTION 4 DETECTION

4.1 APPLICATION

The detection elements set out in this Section represent a number of action items to increase the likelihood of detecting fraud or corruption.

Compliance with this Standard requires an entity to implement each of the minimum acceptable compliance[58] detection initiatives in a way that is appropriate to the entity having regard to its size, diversity, geographic spread, risk profile and the industry sector in which it operates.

4.2 IMPLEMENTING A FRAUD AND CORRUPTION DETECTION PROGRAM

4.2.1 Detection systems

All entities should implement systems aimed at detecting fraud and corruption as soon as possible after it has occurred in the event that the entity's preventative systems fail.

These systems should include the following:

(a) Post-transactional review.

(b) Data mining and real-time computer system analysis to identify suspected fraudulent transactions.

(c) Analysis of management accounting reports.

NOTE: Even in entities that have implemented a comprehensive fraud and corruption control program, it is possible that fraud or corruption will occur from time to time.

4.2.2 Responsibility for the fraud and corruption detection program

Responsibility for developing systems to investigate and detect fraud and corruption should rest with a specified fraud and corruption control resource such as a Fraud and Corruption Control Officer[59] as discussed at Clause 2.4.2.

The Fraud and Corruption Control Officer will ideally work with line management and internal audit in applying the entity's findings from the fraud and corruption risk assessment process to formulate effective fraud and corruption detection systems and procedures (the Fraud and Corruption Control Officer should have sufficient authority to achieve this aim).

It is worthwhile considering whether the entity's fraud and corruption detection initiatives should be generally communicated to management and staff. This can have the effect of providing an additional deterrent for employees who may be motivated to commit fraud or become involved in corrupt conduct.

Each of the systems outlined in Clause 4.2.1 is considered in further detail below.

[58] Refer to Clause 1.3 for the distinction between 'minimum acceptable compliance' and 'guidance' provisions of the Standard.

[59] An entity's fraud and corruption detection program should be facilitated by other than line management as experience suggests that some line managers have a disincentive to detect fraud and corruption or if it is detected, fail to pursue it with the vigour expected by the entity.

4.2.3 Post-transactional review

A review of transactions after they have been processed can be effective in identifying fraudulent or corrupt activity. Such a review conducted by personnel unconnected with the business unit in which the transactions were effected, may uncover altered or missing documentation, falsified or altered authorization or inadequate documentary support. In addition to the possibility of detecting fraudulent transactions, such a strategy can also have a significant fraud prevention effect as the threat of detection may be enough to deter a staff member who would otherwise be motivated to engage in fraud and corruption.

For example, in a case of payroll fraud, a review of last minute changes to the entity's instructions to the banks may identify duplicated account numbers or non-existent employees. A review of contracts may indicate significant irregularities in relation to the awarding of a contract for the supply of labour or materials which may be indicative of an improper relationship between the contractor and a procurement manager.

4.2.4 Data mining and real-time computer system analysis

An entity's information systems are an important source of information on fraudulent and, to a lesser extent, corrupt conduct. By the application of sophisticated (and, in many cases, relatively unsophisticated) software applications and techniques, a series of suspect transactions can be identified and then investigated thus potentially detecting fraudulent and corrupt conduct at an early stage.

For example, a common type of fraud is false invoicing where a member of staff aware of internal control weakness inherent in the entity, may process fictitious invoices for goods or services that have not been supplied to the entity. It is not uncommon for an employee to use his or her residential address as the address of a fictitious entity in whose name the invoices have been raised. A relatively simple analysis of the entitys system may identify instances where the same address is recorded for the bogus supplier and the employee. The same process may identify the same address being used for two suppliers which may also be indicative of fraud.

Strategic computer analysis may involve off-line and real-time techniques. In off-line techniques, data is extracted from the computer system onto a personal computer system using appropriate software applications. This data is then analysed in such a way as to identify evidence of fraudulent or corrupt transactions having regard to the fraud and corruption risks identified during the risk assessment process described in Clause 3.6.

Real-time techniques will involve analysis of live data within the system. Examples of real-time fraud detection systems are the sophisticated software applications used within the banking system to detect credit card fraud (both issued card fraud and merchant fraud) within a very short time after the fraudulent transactions allowing for immediate suspension of the account. Other examples of real-time systems are data matching techniques allowing for the detection of social security fraud, money laundering and tax evasion.

4.2.5 Analysis of management accounting reports to identify trends

Using relatively straightforward techniques in analysing the entity's management accounting reports, trends can be examined and investigated which may be indicative of fraudulent or corrupt conduct. Some examples of the types of management accounting reports that can be utilized on a compare and contrast basis are monthly actual/budget comparison reports for individual cost centres, reports comparing expenditure against industry benchmarks and reports highlighting unusual trends in bad or doubtful debts.

4.3 ROLE OF THE EXTERNAL AUDITOR IN THE DETECTION OF FRAUD

4.3.1 Working with the external auditor in the detection of fraud

Entities whose financial statements are audited, should be familiar with the role and responsibilities of the auditor in detecting fraud. Senior management and/or audit committees of audited entities should undertake a discussion with the auditor in terms of the audit procedures that will be carried out during the audit that are aimed at detecting material misstatements in the entity's financial statements due to fraud or error.

4.3.2 Recent changes to the auditor's accountability for detecting fraud

Recent changes to international and Australian auditing standards have raised the auditor's accountability for the detection of fraud as part of the audit. These standards have amended auditing procedures so that the audit will be more likely to detect a material misstatement in the subject entity's financial statements due to fraud (or error).

4.3.3 Leveraging from the external auditor fraud detection program

Audited entities should take a proactive position in relation to the audit fraud detection program. This would include—

(a) stressing to the auditor the entity's fraud and corruption detection philosophy and the importance the entity places on fraud detection as part of the audit;

(b) offering such assistance as the auditor may require to enable a more comprehensive examination of this issue; and

(c) an internal consideration of the fraud risk factors set out in the auditing standard[60].

4.4 AVENUES FOR REPORTING SUSPECTED INCIDENTS

4.4.1 Implementation of a program for alternative reporting channels

Entities should ensure that adequate means for reporting suspicious or known illegal or unethical conduct are available to all personnel.

In this context also, the entity should consider a policy of mandatory reporting of known or suspected fraud or corruption through one or more of these alternative reporting lines.

4.4.2 The need for a formalized system of reporting

It is important that all instances of fraud and corruption detected within, against or by the entity are reported to senior management.

It is important also that all personnel associated with an entity, have alternative means by which to report matters of concern involving allegations of unethical or illegal behaviour. This will involve avenues through which employees and others with concerns or allegations may report their suspicions to senior management.

Reports of behaviour involving possible fraud or corruption should be capable of being communicated to senior management through—

(a) an appropriate system for reporting concerns through the entity's usual organizational structure (i.e. to senior management via the staff member's immediate manager or supervisor);

(b) internal alternative reporting channels; and

(c) external alternative reporting channels.[61]

[60] Auditing Standard ASA 240, *The Auditors Responsibility to Consider Fraud in an Audit of a Financial Department*.

4.4.3 Alternative avenues for reporting

The objective of the alternative reporting mechanisms is to ensure that—

(a) all actual or potential fraud and corruption control system failures are rectified in an appropriate way; and

(b) systemic and recurring problems of non-compliance are reported to those with sufficient authority to correct them.

A fraud and corruption control program should have both internal and external reporting arrangements. Both internal and externally operated alternative reporting lines should allow anonymous reporting. Anonymous information often proves to be correct but it must be treated with the utmost scepticism until its veracity is confirmed by independent investigation.

Anonymous information in many cases will justify a preliminary examination and investigation of the available evidence but a more complete investigation should only proceed if the information received from anonymous sources is appropriately supported by evidence.

4.5 WHISTLEBLOWER PROTECTION PROGRAM

4.5.1 Implementing a whistleblower protection policy

Entities should implement a policy for the active protection of whistleblowers and should ensure that the policy is well communicated and understood by all personnel.

4.5.2 Further guidance on implementing a whistleblower protection program

In order to encourage the prompt reporting of concerns and suspicions, entities should adopt a policy of encouraging staff who have knowledge of fraudulent or corrupt conduct to come forward. Staff should feel able to report a fraud or corruption concern directly to their manager or supervisor and should have alternative means of raising concerns and suspicions outside the usual channels (refer to Clause 4.4).

Refer to AS 8004—2003 for further guidance on the implementation of an effective whistleblower protection policy.

[61] Refer also to Clause 4.5.

SECTION 5 RESPONSE

5.1 APPLICATION

The response elements set out below represent a number of action items that can be implemented to improve the entity's response to fraud and corruption incidents actually detected.

Compliance with this Standard requires an entity to implement each of the 'minimum acceptable compliance' response initiatives in a way that is appropriate to the entity having regard to its size, diversity, geographic spread, risk profile and the industry sector in which it operates.

5.2 POLICIES AND PROCEDURES

Entities should install appropriate policies and procedures for dealing with suspected fraud or corruption detected through its detection systems or otherwise coming to their notice.

This will include the development and implementation of—

(a) appropriate measures for the comprehensive investigation of such matters based on the principles of independence, objectivity and the rules of natural justice;

(b) systems for internal reporting of all detected incidents;

(c) protocols for reporting the matters of suspected fraud or corruption to the appropriate law enforcement agency; and

(d) policies for the recovery of stolen funds or property.

5.3 INVESTIGATION[62]

5.3.1 The need for qualified investigation resources

An investigation into apparent or suspected fraud and corruption should be conducted by appropriately skilled and experienced personnel who are independent of the business unit in which the alleged fraudulent or corrupt conduct occurred.

This independent party should be an external law enforcement agency, a manager or other senior person within the entity itself or an external consultant operating under the direction of an independent senior person within the entity.

5.3.2 External investigation resources

If an external party is engaged to assist with the conduct of the investigation, all persons engaged should be appropriately qualified, by reason of formal qualifications and relevant experience, to deliver the work contemplated. It is important also that any investigation accords with acceptable practices within respective jurisdictions and any person conducting such an investigation is an acceptable person within the jurisdiction(s) in which the investigation is being conducted.

An acceptable practice refers to affording fairness and propriety to possible suspects so that their rights are not impinged upon. That also means that any evidence obtained during the course of an investigation from whatever source complies with jurisdictional requirements in order to guarantee the sufficiency of evidence should charges result.

[62] Federal Government agencies should refer to the *Commonwealth Fraud Control Guidelines* (Guideline 4) and the *Australian Government Investigations Standard.*

Investigations should be conducted in accordance with the following principles:

(a) External parties engaged to assist in investigations on an entity's behalf should be required to enter into a binding agreement in relation to the release of confidential information coming into their possession during the course of the investigation. External consultants need to have appropriate expertise when conducting investigations. They may also need to have access to other resources to deal with technical queries or legal issues as they arise.

(b) Any investigation and resulting disciplinary proceedings should be conducted in an atmosphere of transparency at all times ensuring that the rules of natural justice are observed.

(c) The overall guiding principles of any investigation into alleged improper conduct are independence and objectivity.

(d) An investigation should comply with all relevant legislation in the jurisdiction in which action will or could be initiated.

(e) Adequate records to be made and kept of all investigations. These records should be kept in accordance with legal, best practice or privacy management guidelines.

(f) An entity conducting an investigation into allegations for misconduct should ensure that information arising from, or relevant to, the investigation is not disseminated to any person not required by their position description to receive the information.

(g) An investigation will potentially involve the following investigative activities:

    (i) Interviewing of relevant witnesses including obtaining statements, where appropriate including witnesses internal and external to the entity.

    (ii) Reviewing and collating documentary evidence.

    (iii) Forensic examination of computer systems.

    (iv) Examination of telephone records.

    (v) Enquiries with banks and other financial institutions (subject to being able to obtain appropriate Court orders).

    (vi) Enquiries with other third parties.

    (vii) Data search and seizure.

    (viii) Expert witness and specialist testimony.

    (ix) Tracing funds/assets/goods.

    (x) Preparing briefs of evidence.

    (xi) Liaison with the police or other law enforcement or regulator agencies.

    (xii) Interviewing persons suspected of involvement in fraud and corruption.

    (xiii) Report preparation.

(h) Any investigation into improper conduct within an entity should be subject to an appropriate level of supervision by a responsible committee within the entity having regard to the seriousness of the matter under investigation. In serious cases, it is contemplated that the relevant committee will be the audit committee, the ethics committee or the board of Directors.

5.4 INTERNAL REPORTING AND ESCALATION

5.4.1 Collating information in relation to fraud and corruption incidents

Entities should develop and implement a program for the capturing, reporting, analysis and escalation of all detected fraud and corruption incidents. This program would be aimed at ensuring that fraud and corruption incidents that occur with or without the knowledge of senior management are reported. An entity should establish a fraud and corruption register and ensure that all incidents occurring (subject to minimum reporting thresholds) are entered therein.

5.4.2 Fraud and corruption incident register

The fraud and corruption incident register should be maintained by the Fraud Control Officer and will typically include the following information in relation to every reportable fraud and corruption incident:

- Date and time of report.
- Date and time that incident was detected.
- How the incident came to the attention of management (e.g. anonymous report, normal report, supplier report.
- The nature of the incident.
- Value of loss (if any) to the entity.
- The action taken following discovery of the incident.

5.4.3 Analysis and reporting program of fraud and corruption incidents

An entity should undertake a regular analysis of incidents reported and periodically report trends to an appropriate body of review (e.g. the audit committee, ethics committee, the board). Annual reports should indicate what action has been taken to reduce the level of fraud overall.

5.5 DISCIPLINARY PROCEDURES

5.5.1 Disciplinary procedures

An entity should ensure that its own Human Resources Manual (or other relevant guidelines) includes particulars on how disciplinary proceedings should be conducted.

5.5.2 Implementing a disciplinary procedures policy

The ultimate outcome of disciplinary proceedings may involve the admonition, termination, demotion, fining or reduction in seniority of an employee or other internal person. An important element of the policy will be the application of the rules of natural justice and fairness.

5.5.3 Separation of investigation and determination processes

It is important to separate the investigation and determination processes in relation to fraud or corruption incidents. The results of the investigation should be put to those with responsibility for making the decision as to what disciplinary action is taken. This responsibility could rest with a senior person or a small committee who can make a decision on the basis of the evidence and after applying the entity's disciplinary procedures policy.

5.6 EXTERNAL REPORTING

5.6.1 Implementing a policy dealing with external reporting of fraud and corruption

Entities should ensure that they have a policy on whether and how allegations of fraud and corrupt conduct should be reported to the police, other appropriate law enforcement agency[63], or other government body (for example, as identified in legislation).

On reaching a finding that there is evidence of fraud or corruption in respect of an allegation or series of allegations, the entity should undertake a formal process to form a view as to whether the matter is one that ought to be reported to the relevant law enforcement agency for investigation and therefore, potentially, prosecution. The entity's external reporting policy should be consistently applied so that there can be no suggestion of selective application.

5.6.2 Format for reports to law enforcement agencies

As a minimum, the entity should provide the following items to the law enforcement agency (the entity should elicit from the law enforcement agency particulars as to how this material should be presented to ensure minimal duplication of effort)[64]:

- A summary of the allegations.
- A list of witnesses and potential witnesses.
- A list of suspects and potential suspects.
- Copies of all statements, depositions or affidavits obtained to that point including and in particular, any written statement made by the subject of the investigation.
- A copy of the transcript of any interview conducted with a person suspected of involvement in the matters alleged.
- A copy of any electronic media on which such interviews have been recorded.
- Copies of all documentary evidence obtained to that point (ultimately the law enforcement agency will probably require the original documents, in which case copies should be retained by the entity).
- Any charts or diagrammatical summaries of the allegations and evidence that the entity may have produced.

5.6.3 Commitment to assist law enforcement

In the event that a decision is made to refer the matter to the appropriate law enforcement agency, the entity should give an undertaking to the law enforcement agency that it will do all that is reasonable in assisting the law enforcement agency to conduct a full and proper investigation. This may involve the entity committing financial and other resources to an investigation either for or independently of the law enforcement agency.

5.7 CIVIL ACTION FOR RECOVERY OF LOSSES—POLICY FOR RECOVERY ACTION

Entities should ensure that they have a policy requiring that recovery action be undertaken where there is clear evidence of fraud or corruption and where the likely benefits of such recovery will exceed the funds and resources invested in the recovery action.

[63] The legal obligation to report serious crime to the police varies from jurisdiction to jurisdiction in Australia—in some jurisdictions, reporting is mandatory and in others it is optional.

[64] Derived from the *Commonwealth Fraud Control Guidelines.*

5.8 REVIEW OF INTERNAL CONTROLS

5.8.1 Internal control review following detection of a fraud or corruption incident

In each instance where fraud is detected, the Fraud Control Officer (if appointed—refer to the guidelines for the development of a Fraud Control Plan in Clause 2.2 which provides guidelines for the appointment of a Fraud Control Officer) and line management should reassess the adequacy of the internal control environment (particularly those controls directly impacting on the fraud incident and potentially allowing it to occur) and consider whether improvements are required.

Where improvements are required, these should be implemented as soon as practicable.

5.8.2 Accountability for undertaking internal control review

The responsibility for ensuring that the internal control environment is re-assessed and for ensuring that the recommendations arising out of this assessment are implemented should be allocated in advance. A summary of recommendations or requirements for the modification of the internal control environment should be provided to the manager of the department concerned.

5.9 INSURANCE—CONSIDERATION OF THE NEED FOR FIDELITY GUARANTEE INSURANCE

Entities should consider maintaining a fidelity guarantee insurance policy (subject to an ongoing analysis of cost/benefit of holding such a policy) that insures the entity against the risk of loss arising from internal fraudulent conduct.

Insurance for externally instigated fraud and corruption should also be maintained as appropriate including insurance against the theft of the entity's property.

Insurances dealing with the risk of fraud, corruption and theft of an entity's property should be undertaken as part of the entity's overall insurance program and include a consideration of the level of cover, inclusions/exclusions and deductibles.

APPENDIX A

SUGGESTED FRAMEWORK FOR A FRAUD AND CORRUPTION CONTROL PLAN

(Informative)

1 Executive summary

1.1 Introduction

1.2 Definition of fraud

1.3 Definition of corruption

1.4 Statement of entity’s attitude to fraud and corruption

1.5 Code of conduct

1.6 Relationship with the entity’s other plans

1.7 Roles and accountabilities for fraud control

2 Planning and resourcing

2.1 Program for fraud control planning and review

2.2 Appointment of a Fraud Control Officer and other dedicated fraud control resources

2.3 External assistance to the Fraud Control Officer

2.4 Fraud control responsibilities

2.5 Internal audit activity in fraud and corruption control

3 Fraud and corruption prevention

3.1 Implementing and maintaining an integrity framework

3.2 Ensuring senior management commitment to controlling the risk of fraud and corruption

3.3 Line management accountability for controlling fraud and corruption within their business unit

3.4 Maintaining a strong internal control system and internal control culture

3.5 Fraud and corruption risk assessment

3.6 Communication and awareness of fraud and corruption

3.7 Employment screening (pre-employment and on internal promotion or transfer)

3.8 Policy dealing with taking annual leave and job rotation

3.9 Supplier and customer vetting

3.10 Specific initiatives aimed at controlling the risk of corruption

4 Fraud and corruption detection

4.1 Fraud and corruption detection program

4.2 Defining the external auditor’s role in the detection of fraud

4.3 Mechanisms for reporting suspected fraud and corruption incidents

4.4 Implementing a whistleblower protection program

5 Responding to detected fraud and corruption incidents

5.1 Procedures for the investigation of detected or suspected incidents

5.2 Internal reporting and escalation

5.3 Disciplinary procedures

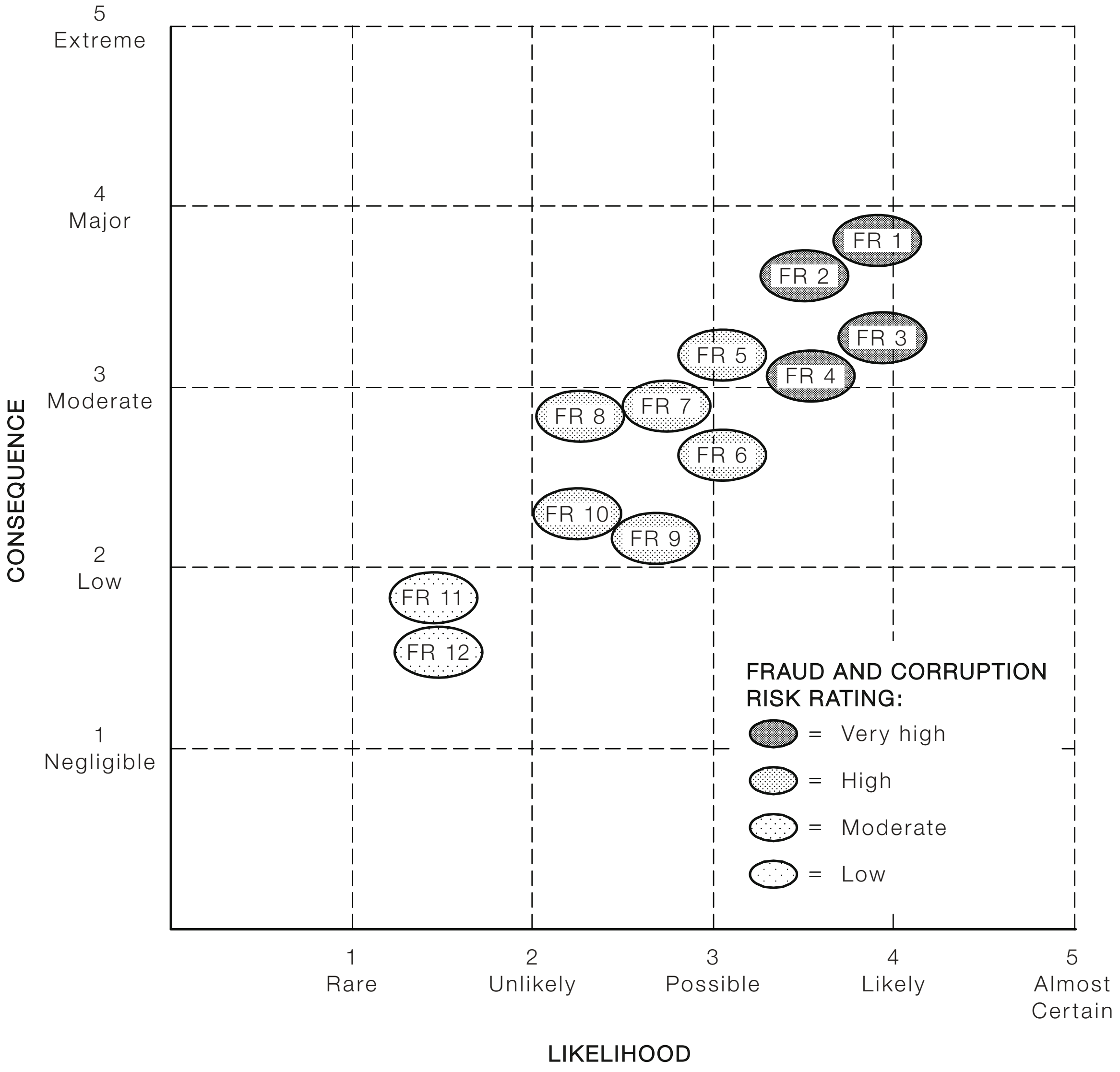
5.4 External reporting (Police, ASIC)

5.5 Policy for civil proceedings to recover the proceeds of fraud or corruption

5.6 Internal control review following discovery of fraud

5.7 Maintaining and monitoring adequacy of Fidelity Guarantee insurance and other insurance relative policies dealing with fraudulent or improper conduct

APPENDIX B
FRAUD RISK SUMMARY
(Informative)



FR 1	Brief description of risk No. 1
FR 2	Brief description of risk No. 2
FR 3	Brief description of risk No. 3
FR 4	Brief description of risk No. 4
FR 5	Brief description of risk No. 5
FR 6	Brief description of risk No. 6
FR 7	Brief description of risk No. 7
FR 8	Brief description of risk No. 8
FR 9	Brief description of risk No. 9
FR 10	Brief description of risk No. 10
FR 11	Brief description of risk No. 11
FR 12	Brief description of risk No. 12

NOTES

NOTES

Standards Australia

Standards Australia develops Australian Standards® and other documents of public benefit and national interest. These Standards are developed through an open process of consultation and consensus, in which all interested parties are invited to participate. Through a Memorandum of Understanding with the Commonwealth Government, Standards Australia is recognized as Australia's peak non-government national standards body. Standards Australia also supports excellence in design and innovation through the Australian Design Awards.

For further information visit **www.standards.org.au**

Australian Standards®

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

International Involvement

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

Sales and Distribution

Australian Standards®, Handbooks and other documents developed by Standards Australia are printed and distributed under license by SAI Global Limited.

ISBN 0 - 7337 - 8552 - 0

Standards Development
Standards Australia
GPO Box 476
Sydney NSW 2001
Phone: 02 9237 6000
Fax: 02 9237 6010
Email: mail@standards.org.au
Internet: www.standards.org.au

Sales and Distribution
SAI Global
Phone: 13 12 42
Fax: 1300 65 49 49
Email: sales@sai-global.com