



AS 8001—2008
Fraud and Corruption Control



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 Zealand
 - 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Standards may also be withdrawn.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.

COPYRIGHT

© Standards Australia

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

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

	<i>Page</i>
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

	<i>Page</i>
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 research¹ 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 year³ 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 countries¹¹ 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

S E C T I O N 1 S C O P E A N D G E N E R A L

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 categories¹³—

- (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)*.



The remainder of this document
is available for purchase online at

➤ www.saiglobal.com/shop ◀

SAI Global also carries a wide range of publications from a wide variety of Standards Publishers:



Click on the logos to search the database online.