

AS 8001:2021



Fraud and corruption control



AS 8001:2021

This Australian Standard® was prepared by QR-017, Organizational Governance. It was approved on behalf of the Council of Standards Australia on 26 May 2021.

This Standard was published on 11 June 2021.

The following are represented on Committee QR-017:

- Australian Information Industry Association
- Australian Institute of Company Directors
- Australian Institute of Professional Investigators
- Australian Organisation for Quality
- Consumers Federation of Australia
- GRC Institute
- Griffith University
- Institute of Internal Auditors — Australia
- Institute of Management Consultants
- Joint Accreditation System of Australia & New Zealand
- Law Society of New South Wales
- Office of the NSW Ombudsman

This Standard was issued in draft form for comment as DR AS 8001:2020.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

ISBN 978 1 76113 367 1

Fraud and corruption control

Originated as AS 8001—2003.
Second edition 2008.
Third edition 2021.

© Standards Australia Limited 2021

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, unless otherwise permitted under the Copyright Act 1968 (Cth).

Preface

This Standard was prepared by Standards Australia Committee QR-017, Organizational Governance, to supersede AS 8001:2008, *Fraud and corruption control*.

The objective of this Standard is to provide minimum requirements and additional guidance for organizations wishing to develop, implement and maintain an effective fraud and corruption control system (FCCS) through initiatives aimed at —

- (a) preventing fraud and corruption;
- (b) detecting fraud and corruption; and
- (c) responding to fraud and corruption events that have already occurred.

This Standard sets out an approach to controlling fraud and corruption through —

- (i) establishing the organization's fraud and corruption control objectives and values;
- (ii) developing, implementing, communicating and maintaining an integrity framework;
- (iii) developing and implementing a fraud and corruption control system;
- (iv) raising awareness of fraud and corruption control issues;
- (v) establishing clear accountability structures in terms of response and escalation of an investigation of fraud and corruption events;
- (vi) setting guidelines for the recovery of the proceeds of fraud or corruption.

The major changes in this edition are as follows:

- (A) Inclusion of minimum requirements.
- (B) Updated references to relevant standards and other resources, particularly AS ISO 37001 and AS ISO 31000.
- (C) Updated definitions of fraud and corruption to include dishonest conduct that is not necessarily a breach of the law.
- (D) Updated requirements and guidance on information system security and controlling the risks of external attack.
- (E) Updated requirements and guidance on the application of information and communication technologies (ICT) in relation to fraud and corruption prevention, detection and response.

The terms “normative” and “informative” are used in Standards to define the application of the appendices to which they apply. A “normative” appendix is an integral part of a Standard, whereas an “informative” appendix is only for information and guidance.

Contents

Preface	ii
Introduction	vi
Section 1 Scope and general	1
1.1 Scope	1
1.2 Application	1
1.3 Normative references	2
1.4 Terms and definitions	2
Section 2 Foundations for fraud and corruption control	8
2.1 General	8
2.2 Governing body	8
2.3 Top management	
2.4 Specialist fraud and corruption control resourcing	9
2.4.1 Specialist fraud and corruption control function	9
2.4.2 Appointment of an ISMS professional	10
2.4.3 Collaboration with other risk management resources	10
2.4.4 Leveraging organizational fraud and corruption control resources	10
2.5 Line management	11
2.6 Business unit accountability for fraud and corruption control	11
2.7 Awareness raising of fraud and corruption risk	11
2.7.1 General	11
2.7.2 Matters to be covered in a fraud and corruption awareness raising program	12
2.8 Fraud and corruption risk management	12
2.9 External environment scan	13
2.10 Developing and implementing a fraud and corruption control system (FCCS)	14
2.10.1 General	14
2.10.2 Developing a fraud and corruption control system	15
2.10.3 Documenting the fraud and corruption control system (FCCS)	15
2.10.4 Promoting the fraud and corruption control system	17
2.10.5 Monitoring and maintaining a fraud and corruption control system	17
2.10.6 Factors to be considered in reviewing a fraud and corruption control system	18
2.11 Leveraging the internal audit function in fraud and corruption control	18
2.11.1 General	18
2.11.2 The role of the internal audit function in assessing fraud and corruption risk	18
2.12 Leveraging the external audit function in fraud and corruption control	19
2.13 Information Security Management system (ISMS)	19
2.14 Record keeping and confidentiality of information	19
Section 3 Preventing fraud and corruption	21
3.1 General	21
3.2 Promoting a sound integrity framework	21
3.2.1 Structure and policy elements of an integrity framework	21
3.2.2 Actions to support an integrity framework	22
3.3 Managing conflicts of interest	23
3.4 Managing risks connected to gifts, hospitality, donations and similar benefits	24
3.5 Internal controls and the internal control environment	24
3.5.1 The role of internal controls in fraud and corruption prevention	24
3.5.2 Implementing and maintaining an internal control system that will be effective in preventing fraud and corruption	24
3.5.3 Pressure testing the internal control system	25
3.6 Managing performance-based targets	26
3.7 Workforce screening	26
3.7.1 Implementing a robust workforce screening program	26
3.7.2 Developing a workforce screening policy	26
3.8 Screening and ongoing management of business associates	27

3.8.1	General	27
3.8.2	Verification of business associates	
3.8.3	Enquiries to be undertaken regarding the integrity of business associates	27
3.8.4	Managing the risk of fraud and corruption by business associates	28
3.9	Preventing technology-enabled fraud	28
3.10	Physical security and asset management	29
Section 4	Detecting fraud and corruption	30
4.1	General	30
4.2	Post-transactional review	30
4.3	Analysis of management accounting reports	30
4.4	Identification of early warning signs	31
4.5	Data analytics	31
4.6	Fraud and corruption reporting channels	32
4.7	Whistleblower management system	33
4.8	Leveraging relationships with business associates and other external parties	34
4.9	Complaint management	34
4.10	Exit interviews	34
Section 5	Responding to fraud and corruption events	36
5.1	General	36
5.2	Immediate action on discovery of a fraud or corruption event	36
5.2.1	Immediate actions in response to discovery of fraud or corruption	36
5.2.2	Digital evidence first response	37
5.3	Investigation of a detected fraud or corruption event	37
5.3.1	General	37
5.3.2	The role of the investigator	38
5.3.3	Expertise of the investigator	38
5.3.4	Safety of investigators	39
5.3.5	Investigation principles	39
5.3.6	Capturing, analysing and managing digital evidence	39
5.3.7	Handling evidence other than digital evidence	39
5.3.8	Investigation planning	40
5.3.9	Record keeping	40
5.3.10	Consideration of grievances	41
5.4	Disciplinary procedures	41
5.4.1	General	41
5.4.2	Implementing a disciplinary procedures policy	41
5.4.3	Separation of investigation and determination processes	41
5.5	Crisis management following discovery of a fraud or corruption event	42
5.6	Internal reporting and escalation	42
5.6.1	Collating information in relation to fraud and corruption events	42
5.6.2	Fraud and corruption event register	42
5.6.3	Analysis and reporting of fraud and corruption events	42
5.7	External reporting	43
5.7.1	General	43
5.7.2	Cooperation with law enforcement agencies	43
5.7.3	Format for reports to law enforcement agencies	44
5.8	Recovery of stolen funds or property	44
5.9	Responding to fraud and corruption events involving business associates	44
5.10	Insuring against fraud events	44
5.11	Assessing internal controls, systems and processes post-detection of a fraud or corruption event	45
5.12	Third parties	45
5.12.1	Impact of fraud on third parties	45
5.12.2	Notification of third parties	46
5.13	Disruption of fraud and corruption	46
Appendix A	(informative) The prevalence and impact of fraud and corruption in the Australian economy	48

Appendix B (informative) Examples of fraud and corruption risks impacting Australian entities	50
Appendix C (informative) Examples of fraud and corruption Key Risk Indicators (KRI)	53
Bibliography	54

Introduction

Fraud and corruption are significant issues for the Australian business, government and not-for-profit sectors. Fraud and corruption frequently impact the financial position of the target organization and often have flow-on financial consequences for the Australian economy. Fraud can also result in severe and enduring psychological or emotional harm for the people involved. Corruption can result in sub-optimal outcomes for business decisions and reputational damage to all parties. See [Appendix A](#) for an overview of the prevalence and impact of fraud and corruption in the Australian economy. See [Appendix B](#) for a summary of the types of fraud common in Australian organizations.

So far as fraud is concerned (as distinct from the concept of corruption), previous editions of this Standard were primarily concerned with internal occupational fraud i.e. fraud events where the perpetrator is an employee or otherwise closely connected to the target organization. The pervasiveness and increasing sophistication of information technology, the rapid take-up of internet-based payment systems by the general population and an increasingly globalized economy have led to an increased incidence of external fraudulent attack on Australian organizations across all sectors. In response to these fundamental changes in the way business operates, this edition of the Standard includes minimum requirements and updated guidance on controlling external, often technologically-driven, attacks on Australian organizations.

Managing business risk is a core governance issue. By logical extension, controlling the risk of fraud and corruption is also a core governance issue which should be given due attention by the governing bodies and top management of all Australian organizations. Governance generally and, in the context of this Standard, fraud and corruption control specifically, are ultimately the responsibility of an organization's governing body.

Conformance to this document cannot provide assurance that no fraud or corruption has occurred or will occur as it is not possible to completely eliminate the exposure to these risks. However, comprehensive application of this document including adequately resourcing the organization's fraud and corruption control system will help organizations to mitigate fraud and corruption risks and to respond appropriately to fraud and corruption events as they occur.

Australian Standard®

Fraud and corruption control

Section 1 Scope and general

1.1 Scope

This Standard provides minimum requirements and additional guidance for organizations wishing to develop, implement and maintain an effective fraud and corruption control system (FCCS) incorporating —

- (a) prevention of internal and external fraud and corruption including fraud and corruption against and by the organization;
- (b) early detection of fraud and corruption in the event that preventative strategies fail; and
- (c) effective response to fraud and corruption events in ways that achieve optimal outcomes for the organization including the recovery of the organization's property or the award of compensation to an equivalent value.

The aim of such a system is to control the risks of fraud and corruption against the organization (i.e. where the organization is the target or intended target) as well as fraud and corruption committed by or in the name of the organization (i.e. where fraud or corruption is committed by an organization or by a person or persons purporting to act on the organization's behalf or in the organization's economic interest).

This Standard addresses both internal and external fraud and corruption.

This Standard does not address fraud against the individual, including consumer fraud.

NOTE This standard makes no distinction between technology-enabled fraud and corruption and fraud and corruption that are less reliant on technology, as the majority of frauds and many forms of corruption will involve technology to a greater or lesser degree. However, the distinction between internal and external fraud and corruption remains useful.

1.2 Application

This Standard is intended to apply to all organizations operating in Australia. This includes publicly listed corporations, proprietary corporations, incorporated associations, unincorporated organizations and all government departments and agencies. It is intended to apply to not-for-profit as well as for-profit organizations.

Conformance to this Standard requires an appropriate level of forward planning and application of a structured risk management approach. The application of contemporary risk management principles outlined in AS ISO 31000 is fundamental to the prevention of fraud and corruption against or by Australian organizations.

Corruption control is within the intended scope of this Standard. Relevant to this is AS ISO 37001, which provides requirements and guidance for organizations wishing to control bribery. Both AS ISO 37001 and AS 8001 consider —

- (a) bribery to be a subset of corruption; and
- (b) that all instances of bribery will constitute corruption; but
- (c) that not all instances of corruption will constitute bribery.

Due to this distinction between the definitions of corruption and bribery, corrupt behaviours that do not constitute bribery are within the scope of this Standard but are not within the scope of AS ISO 37001.

1.3 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document.

NOTE Documents for informative purposes are listed in the Bibliography.

AS 4811, *Employment screening*

AS ISO 31000, *Risk management — Guidelines*

AS ISO 37001, *Anti-bribery management systems — Requirements with guidance for use*

AS ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

ISO/IEC 27041, *Information technology — Security techniques – Guidance on assuring suitability and adequacy of event investigative method*

ISO/IEC 27042, *Information technology — Security techniques – Guidelines for the analysis and interpretation of digital evidence*

ISO/IEC 27043, *Information technology — Security techniques - Incident investigation principles and processes*

ASA 240 *The Auditor's Responsibilities Relating to Fraud in an Audit of a Financial Report issued by the Auditing and Assurance Standards Board*

NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide*

1.4 Terms and definitions

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

1.4.1

attack

attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

[SOURCE: ISO/IEC 27000:2018(en), 3.2]

1.4.2

bona fide

bona fides

person or organization whose business practices appear to be straightforward and of integrity

1.4.3

bribe

bribery

offering, promising, giving, accepting or soliciting of an undue advantage of any value (which could be financial or non-financial), directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the performance of that person's duties

Note 1 to entry: The above is a generic definition. The meaning of the term "bribery" is as defined by the anti-bribery law applicable to the organization and by the anti-bribery management system designed by the organization

[SOURCE: ISO 37001:2016(en), 3.1, modified — headword has been adjusted]

1.4.4

business associate

external party with whom the organization has, or plans to establish, some form of business relationship

Note 1 to entry: A business associate includes but is not limited to clients, customers, joint ventures, joint venture partners, consortium partners, outsourcing providers, contractors, consultants, sub-contractors, suppliers, vendors, advisors, agents, distributors, representatives, intermediaries and investors. This definition is deliberately broad and should be interpreted in line with the bribery risk profile of the organization to apply to business associates which can reasonably expose the organization to bribery risks.

Note 2 to entry: Different types of business associate pose different types and degrees of bribery risk, and an organization will have differing degrees of ability to influence different types of business associate. Different types of business associate can be treated differently by the organization's bribery risk assessment and bribery risk management procedures.

Note 3 to entry: Reference to "business" in this document can be interpreted broadly to mean those activities that are relevant to the purposes of the organization's existence.

[SOURCE: ISO 37001:2016(en), 3.26]

1.4.5

code of behaviour

code of conduct

code of ethics

document broadly communicated within the organization setting out expected standards of behaviour

1.4.6

conflict of interest

situation where business, financial, family, political or personal interests could interfere with the judgement of persons in carrying out their duties for the organization

[SOURCE: ISO 37001:2016(en), 3.29]

1.4.7

control

measure that is modifying risk

Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO Guide 73:2009(en), 3.8.1.1]

1.4.8

corruption

dishonest activity in which a person associated with an organization (e.g. director, executive, manager, employee or contractor) acts contrary to the interests of the organization and abuses their position of trust in order to achieve personal advantage or advantage for another person or organization. This can also involve corrupt conduct by the organization, or a person purporting to act on behalf of and in the interests of the organization, in order to secure some form of improper advantage for the organization either directly or indirectly

Note 1 to entry: the concept of corruption in this Standard is broader than the concept of bribe or bribery in AS ISO 37001. All acts of bribery would constitute corruption under AS 8001 but not all acts of corruption would constitute bribery under AS ISO 37001.

Note 2 to entry: While conduct must be dishonest for it to meet the definition of corruption, the conduct does not necessarily represent a breach of the law.

1.4.9**cybercrime**

criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime

[SOURCE: ISO/IEC 27032:2012(en), 4.18]

1.4.10**digital evidence**

information or data, stored or transmitted in binary form that may be relied on as evidence

[SOURCE: ISO/IEC 27037:2012(en), 3.5]

1.4.11**digital evidence first responder****DEFR**

individual who is authorized, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence

Note 1 to entry: Authority, training and qualification are the expected requirements necessary to produce reliable digital evidence, but individual circumstances may result in an individual not adhering to all three requirements. In this case, the local law, organizational policy and individual circumstances should be considered.

[SOURCE: ISO/IEC 27037:2012(en), 3.7]

1.4.12**external fraud****externally instigated fraud**

fraudulent activity where no perpetrator is employed by or has a close association with the target organization

1.4.13**fraud**

dishonest activity causing actual or potential gain or loss to any person or organization including theft of moneys or other property by persons internal and/or external to the organization and/or where deception is used at the time, immediately before or immediately following the activity

Note 1 to entry: Property in this context also includes intellectual property and other intangibles such as information.

Note 2 to entry: Fraud 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.

Note 3 to entry: While conduct must be dishonest for it to meet the definition of “fraud” the conduct need not necessarily represent a breach of the criminal law.

Note 4 to entry: The concept of fraud within the meaning of this Standard can involve fraudulent conduct by internal and/or external parties targeting the organization or fraudulent or corrupt conduct by the organization itself targeting external parties.

1.4.14**fraud and corruption control system****FCCS**

framework for controlling the risks of fraud and corruption against or by an organization

Note 1 to entry: This is also referred to as a fraud and corruption control framework (FCCF).

1.4.15**fraud and corruption event**

instance of fraudulent or corrupt activity against or by an organization

1.4.16**fraud and corruption risk assessment**

application of risk management principles and techniques to the assessment of the risk of fraud and corruption within an organization in accordance with AS ISO 31000

1.4.17**governing body**

group or body that has the ultimate responsibility and authority for an organization's activities, governance and policies and to which top management reports and by which top management is held accountable

Note 1 to entry: Not all organizations, particularly small organizations, will have a governing body separate from top management.

Note 2 to entry: A governing body can include, but is not limited to, board of directors, committees of the board, supervisory board, trustees or overseers.

[SOURCE: ISO 37001:2016(en), 3.7]

1.4.18**information security**

preservation of confidentiality, integrity and availability of information

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

[SOURCE: ISO 27000:2018(en), 3.28]

1.4.19**information security management system****ISMS**

part of the overall management system, based on a business risk approach, that establishes, implements, operates, monitors, reviews, maintains and improves information security

Note 1 to entry: Note to entry: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

[SOURCE: ISO/IEC 18598:2016(en), 3.1.23]

1.4.20**information security management system (ISMS) professional**

person who establishes, implements, maintains and continuously improves one or more information security management system processes

[SOURCE: ISO/IEC 27000:2018(en), 3.33]

1.4.21**interested party****stakeholder**

person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

[SOURCE: ISO 37001:2019, 3.3]

1.4.22**internal fraud****internally instigated fraud**

fraudulent activity where at least one perpetrator is employed by or has a close association with the target organization and has detailed internal knowledge of the organization's operations, systems and procedures

1.4.23**investigation**

search for evidence connecting or tending to connect a person (either a natural person or a body corporate) with conduct defined by this Standard as fraud or corruption

1.4.24**management system**

set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning and operation.

Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

[SOURCE: ISO/IEC 27000:2018(en), 3.41]

1.4.25**monitoring**

determining the status of a system, a process or an activity

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

[SOURCE: ISO/IEC 27000:2018(en), 3.46]

1.4.26**organization**

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: For organizations with more than one operating unit, one or more of the operating units can be defined as an organization.

[SOURCE: ISO 37001:2016(en), 3.2]

1.4.27**policy**

intentions and direction of an organization, as formally expressed by its top management

[SOURCE: ISO/IEC 27000:2018(en), 3.53]

1.4.28**preservation**

process to maintain and safeguard the integrity and/or original condition of the potential digital evidence

[SOURCE: ISO/IEC 27037:2012, 3.15]

1.4.29**risk**

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

[SOURCE: ISO 31000:2018(en), 3.1]

1.4.30

risk assessment

overall process of risk identification, risk analysis and risk evaluation

[SOURCE: ISO Guide 73:2009(en), 3.4.1]

1.4.31

serious risk

likely to have an impact on the organization, 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

1.4.32

target organization

organization that is the object of a fraud or corruption event whether initiated by persons internal to the organization or external to it

1.4.33

technology-enabled fraud

fraud against or by an organization which relies heavily on information technologies and which would not be possible without information technologies

Note 1 to entry: The concept of technology-enabled fraud types follows the binary classification of cyber-enabled and cyber-dependent crimes in which the former include frauds made possible through the use of technologies, while the latter are so-called "pure" cybercrimes that require the presence of technologies for their commission — such as access and disruption offences.

1.4.34

threat

potential cause of an unwanted incident, which can result in harm to a system or organization

[SOURCE: ISO/IEC 27000:2018(en), 3.74]

1.4.35

top management

person or group of people who directs and controls an organization at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

[SOURCE: ISO 37001:2016(en), 3.6, modified — note 2 to entry and note 3 to entry deleted]

1.4.36

whistleblower

person who reports wrongdoing

Note 1 to entry: Applicable whistleblower protection legislation may apply.

[SOURCE: ISO/FDIS 37002]

Section 2 Foundations for fraud and corruption control

2.1 General

An important factor contributing to the incidence of fraud and corruption in Australian organizations across all sectors is a failure of some organizations to view fraud and corruption as a serious threat and a consequent failure to allocate adequate resources to managing the exposures.

Fraud and corruption control resourcing is a critical element of any fraud and corruption control system (FCCS). An effective FCCS requires commitment by the organization's governing body and top management and a clear statement of the organization's commitment to fraud and corruption control.

Organizations shall have a FCCS which clearly defines the roles and accountabilities for controlling the organization's fraud and corruption exposures covering —

- (a) the governing body;
- (b) top management;
- (c) specialist fraud and corruption control resources including information security;
- (d) line management; and
- (e) other organizational personnel.

2.2 Governing body

Managing risk is an important governance issue and, by logical extension, managing fraud and corruption risk is an important governance issue. Consistent with its responsibilities for organization-wide governance, the governing body has overall accountability for ensuring that the organization has in place adequate anti-fraud and anti-corruption measures.

Organizations shall implement a strategy aimed at ensuring that their governing body —

- (a) acknowledges and accepts overall accountability for controlling the organization's fraud and corruption risks;
- (b) acknowledges fraud and corruption as a serious risk;
- (c) has an awareness of the organization's fraud and corruption exposures; and
- (d) demonstrates a high level of commitment to controlling the risks of fraud and corruption both against the organization and by the organization.

See [Clause 2.6](#) for matters to be covered when raising awareness of fraud and corruption.

2.3 Top management

Separately to ensuring fraud and corruption control governance responsibilities are addressed by their governing body, organizations shall ensure that top management has:

- (a) an adequate understanding of their role in the control of the organization's fraud and corruption exposures; and
- (b) an awareness of the organization's fraud and corruption exposures.

See [Clause 2.6](#) for matters to be covered when raising awareness of fraud and corruption.

Organizations should consider the appropriateness of linking top management remuneration to their performance in complying with the organization's integrity framework and fraud and corruption control. This would involve (as and where appropriate to their organizational role) —

- (a) including accountability for fraud and corruption control in the position description of each top manager;
- (b) setting achievable performance targets for fraud and corruption control; and
- (c) linking performance-based remuneration to achieving fraud and corruption control targets.

2.4 Specialist fraud and corruption control resourcing

2.4.1 Specialist fraud and corruption control function

Organizations shall implement an appropriate level of fraud and corruption control resourcing based on the organization's assessed fraud and corruption exposures.

This should include the appointment of specialized fraud and corruption control personnel, as appropriate to the organization and its assessed exposures, whose role includes —

- (a) developing, implementing and maintaining the organization's FCCS;
- (b) coordinating periodic assessment of the organization's fraud and corruption risks;
- (c) recording fraud and corruption events;
- (d) escalating and monitoring fraud and corruption events including coordinating internal and external reporting; and
- (e) conducting, coordinating or monitoring investigations into allegations of fraud and corruption.

Fraud and corruption control resourcing may involve recruitment of specialist resources (internal or external to the organization) with the requisite skills and experience or, alternatively, training existing personnel in this role.

Ideally the fraud and corruption control function should be no more than two levels removed from the Chief Executive Officer (CEO) or equivalent function or, alternatively, with a direct line of reporting to the CEO or equivalent on fraud and corruption control issues.

The person(s) appointed to such a position should have the capacity to understand and apply current better practice in fraud and corruption control and an ability to deliver or coordinate delivery of awareness raising on relevant fraud and corruption control procedures to —

- (i) the governing body;
- (ii) top management;
- (iii) line management; and
- (iv) the organization's workforce generally.

An organization with a person delivering a specialist fraud and corruption control function shall ensure that this resource remains up-to-date with current best practice through —

- (A) formal training on fraud and corruption control issues;
- (B) attendance at relevant seminars, conferences and workshops with a defined time commitment each year;
- (C) maintaining a library of reference materials; and

- (D) networking with other fraud and corruption control specialists as part of a “community of practice”.

2.4.2 Appointment of an ISMS professional

An important consideration in the management of technology-enabled fraud is the deployment of appropriately qualified information security resources.

An ISMS professional, where appointed, shall have the following attributes —

- (a) formal qualifications appropriate to the role of an ISMS professional;
- (b) a sound understanding of the organization’s fraud and corruption exposures;
- (c) a program for continuing professional development in technology-enabled fraud and corruption;
- (d) a sound understanding of how an ISMS can effectively mitigate the risks of fraud and corruption; and
- (e) a sound understanding of cybercrime and the methods for managing the risk of cybercrime as set out in ISO/IEC 27032.

An ISMS Professional, where appointed, shall apply principles in accordance with AS ISO/IEC 27001 in the development, implementation and maintenance of an ISMS.

NOTE See [Clause 2.13](#) for requirement for the implementation of an ISMS.

2.4.3 Collaboration with other risk management resources

Organizations shall ensure that fraud and corruption control initiatives are coordinated with the organization’s broader risk management approach. This requires that the organization’s specialist fraud and corruption control resources, including ISMS professionals, collaborate closely with the organization’s other risk management resources in order to ensure that fraud and corruption risks are incorporated into the organization’s overall risk management system.

See [Clause 2.8](#) for further requirements and guidance on the application of risk management principles to fraud and corruption exposures.

2.4.4 Leveraging organizational fraud and corruption control resources

There is often a range of other internal functions within organizations that can be beneficial in the control of fraud and corruption. These internal functions will vary from organization to organization but generally will include such roles as —

- (a) human resources, industrial relations, payroll and learning and development;
- (b) occupational health and safety personnel;
- (c) compliance professionals;
- (d) corporate counsel;
- (e) quality assurance;
- (f) records management;
- (g) insurance manager;
- (h) regulatory affairs managers;
- (i) environmental impact managers;

- (j) physical security and asset management;
- (k) procurement and accounts payable;
- (l) finance and treasury staff;
- (m) policy and program design; and
- (n) internal audit.

Organizations shall coordinate these resources in order to control the organization's fraud and corruption exposures.

2.5 Line management

Organizations shall communicate to all line managers a mandatory accountability for promptly reporting fraud and corruption matters that come to their attention.

Organizations shall ensure that line management personnel are fully aware that managing fraud and corruption is as much part of their responsibility as managing other types of enterprise risk (see [Clause 2.6](#) for matters to be covered when raising awareness of fraud and corruption within an organization).

In order to reinforce this, it is important that a system be developed and implemented with the following elements:

- (a) Fraud and corruption control are incorporated into the performance management system.
- (b) Preventing and detecting fraud and corruption shall be specified in the position description of line managers where appropriate.

2.6 Business unit accountability for fraud and corruption control

Fraud and corruption control is sometimes seen as a high-level corporate issue in affected organizations i.e. the responsibility for fraud and corruption control sits with top management rather than as a responsibility for local or line management within business units that make up the organization.

Fraud or corruption events often occur in business operations geographically remote from the organization's central management because the local business operation may not be subject to adequate corporate level scrutiny and local management do not perceive a need for fraud and corruption control measures.

Organizations shall communicate to management personnel of discrete business units, particularly business units that are geographically remote to the organization's core business functions, that they are accountable for fraud and corruption control within their business unit.

2.7 Awareness raising of fraud and corruption risk

2.7.1 General

Organizations shall implement a program aimed at ensuring that the governing body, top management, specialist fraud and corruption control resources, line management and all other personnel are aware of the organization's fraud and corruption exposures and how they should respond if they detect or suspect a fraud or corruption event.

Overall responsibility for ensuring that this program is implemented rests with the governing body and top management, but the day-to-day aspects shall be delegated to the specialist fraud and corruption control function or other appropriately qualified resource.

2.7.2 Matters to be covered in a fraud and corruption awareness raising program

A fraud and corruption awareness raising program shall be delivered regularly, appropriate to the organization's exposure to fraud and corruption risk and so that it is relevant and useful to the position and role of each person in the organization.

Such a program should include the following elements:

- (a) A clear statement of the organization's definition of behaviours that constitute fraud or corruption.
- (b) An unequivocal statement that fraudulent and corrupt practices within the organization will not be tolerated.
- (c) The incidence of fraud and corruption generally.

NOTE: In the current age this should include a consideration of fraud and corruption trends globally particularly if the organization operates outside of Australia.
- (d) Fraud and corruption exposures in the industry sectors and in jurisdictions in which the organization operates.
- (e) The assessed fraud and corruption exposures of the organization itself.
- (f) Types of fraud and corruption that have been detected in the organization in the previous five years and how those matters were dealt with in terms of disciplinary action and internal control enhancements.
- (g) A clear statement about what is expected of management and staff if fraud or corruption is detected or suspected.
- (h) A statement as to how management and staff can report allegations or concerns regarding fraud or unethical conduct including the organization's policy for the protection of whistleblowers.
- (i) An overview of the organization's FCCS.
- (j) An overview of resources allocated to fraud and corruption control.
- (k) An overview of fraud and corruption red flag behaviours.

Additionally, fraud and corruption awareness and standards of conduct should be promoted through regular meetings within each business unit, staff newsletters and other internal methods of communication.

2.8 Fraud and corruption risk management

Fraud and corruption are business risks and will have a similar impact on affected organizations as other types of enterprise risk including —

- (a) financial loss;
- (b) loss of information;
- (b) penalties imposed on the organization by courts and regulators;
- (c) reputational impact;
- (d) diversion of management energy;
- (e) organizational morale;
- (f) organizational disruption;