AS 8001:2021

Australian STANDARD®

STANDARDS Australia

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.

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

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.