Adam Simms

Adam Simms is a forensic services partner at BDO Australia and provides investigation, risk management and advisory services. Adam has over 25 years' investigation and financial crime risk management experience. This includes as a financial crime lawyer, working within law enforcement, Australia's competition regulator, Big 4 banking, one of Australia's largest insurance providers and private consulting.

AS8001: Fraud and Corruption Control

Is your business ready for the changes?

Adam Simms

A new [that is, revised version of] Australian Standard AS8001:2008 *Fraud and Corruption Control* was released by Standards Australia on 11 June 2021 and is now ready for implementation [as AS8001:2021].

This standard is considered the benchmark when it comes to how organisations can mitigate fraud and corruption risks. It is of particular importance to boards, principally in how they assess their cyber risks.

The history of AS8001—fraud and corruption control and why it is changing

The AS8001 standard was created to provide guidance on corporate governance around fraud and corruption issues due to some large global corporate collapses at the time. AS8001 was one of five standards released to guide boards and senior management in minimising fraud and corruption risks.

Standards Australia ensures standards are revised within 10 years or withdrawn. As a result, all of the five standards (excluding AS8001) were withdrawn. In 2008, AS8001 was revised but has not been revisited until now, undergoing a much-needed refresh. BDO participated in the revision process.

As a priority, the revision brings the 2008 standard up-to-date, especially when it comes to the impact of technology in modern business operations. In today's world of integrated technology and greater interconnectivity, businesses and organisations are at a much greater risk of external attacks such as cyber attacks. As the 2008 version and its predecessors were heavily focused on internal activities, the revised standard recognises the significant rise of external threats.

Since the COVID-19 pandemic, there has been a marked change in the profile of fraud and corruption across all sectors, with the rationalisation to commit financial crime reaching alarming levels. The release of the revised standard is timely in a COVID-19 world and will offer some useful insight and, in some cases a reminder, about fraud and corruption risk across organisations.

What are some of the more significant changes in the new AS8001?

Aside from the proven traditional approaches to fraud and corruption control that remain in AS8001, there are some important changes for organisations.

In particular, the new standard moves away from 'should' statements and now states organisations 'shall' consider the 12 points covered in the following discussion.

1. The concept of 'fraud control plans' is replaced with the 'fraud and corruption control systems'
Fraud control plans have evolved into a more robust documented system. The idea of a system, as opposed to a plan, is that it brings together the strategies adopted by the organisation to combat fraud and corruption as required, as opposed to a plan that may end up as another governance document gathering dust. This is because historically, we have seen that organisations develop a plan and then 'shelve' it—not implementing it well, or indeed at all.

2. Updated definitions for 'fraud' and 'corruption'
New definitions encompass the full scope of fraud and corruption to provide more holistic approaches to combatting it. The idea of updating these definitions is that if organisations were to only focus on a breach of the criminal law, they may miss an opportunity to stamp out other behaviours that are harmful.

3. Distinguish and harmonise AS8001 with ISO 37001-2019 *Anti-Bribery Management Systems*
The International Standard ISO 37001 became an Australian Standard in 2019, so it does apply in Australia. While the concept of bribery is not that far from that of corruption, the concept of corruption is far broader than bribery, and AS8001:2021 addresses this distinction.

4. There is a requirement for organisations to now plan for preventing, detecting and responding to external attacks—particularly 'cyber-born' attacks
This recognises organisational reliance on technology and the associated risks being more prevalent now than in 2008.

5. A new concept referred to as 'normative references' will mean other fraud and corruption-related standards will also need consideration to afford compliance with AS8001:2021
There are nine of these normative references, but two important examples are as follows:

- Information security management is required conforming with ISO/IEC 27001 *Information technology – Security techniques – Information Security Management Systems – Requirements*. This standard reflects the impact of cyber-attacks on businesses in recent times. Businesses will need to work towards an International Security Management System, which is a set of policies and procedures that control an organisation's sensitive data.
- Risk management is required conforming with ISO 31000:2018 *Risk Management – Guidelines*. Businesses are faced with varying risks. These guidelines assist businesses to apply common approaches to risk management to meet the individual needs of their business.

6. Scrutiny of boards
There is broader scrutiny on the tone from the top, with the standard referencing the 'governing body' role as distinct from 'top management'. The new standard AS8001:2021 defines the various lines of management and brings in the board as the governing body responsible for managing governance and risk, together with senior management.

Further, senior management should have an understanding of their role in combatting fraud and corruption risk and ensure that they are in a position to understand the organisation's risks so they can inform the board but also manage that risk.

7. Third-party notification
There is new guidance that considers the impact of a fraud and corruption event on third parties such as customers/clients, government services and the relevant industry more broadly and whether to inform these parties. This includes guidance around the right time to share information to prevent further or ongoing fraud.

For example, if an organisation is subjected to an external attack and what has happened to them may be happening to other organisations within the same industry or sector, there are considerations to be made.

8. 'Pressure testing' of internal controls
The standard introduces the concept of pressure testing of internal controls, just as there is penetration testing in cybersecurity, where a 'white-hat' hacker attacks an organisation's technology system. Pressure testing draws on this concept, but is used to test internal fraud and corruption mitigation controls.

An example given in the standard is a test of the controls around false invoicing. This is a common type of fraud associated with poor controls over entering new vendors and updating vendor information in the system. A specific test might include an email communication to change client details in the vendor management system and observing how the internal controls respond. How organisations do this will be up to them, but it must form part of the program.

9. Due diligence requirements for business associates
This involves the screening and management of business associates which includes external parties with whom the organisation has a business relationship. Risks around business associates has been heightened during the COVID-19 pandemic and is something that has not been well managed in the past. The standard suggests searches that can be undertaken to verify business associates.

10. Reference and guidance to whistleblower protection and misconduct reporting channels
Whistleblowing remains a key detection mechanism in all organisations, and a whistleblowing platform should be considered as a misconduct barometer on the business and a safeguard to the business and interested parties. There is a new standard in production, ISO 37002

The quote

The revision of AS8001 brings the 2008 standard up-to-date, especially when it comes to the impact of technology in modern business operations.

Whistleblowing Management Systems, expected in Q3, 2021, however, some items from the draft ISO 37002 have been included in AS8001:2021.

11. Immediate actions in fraud and corruption response

There is a range of new guidance within the standard relating to the immediate actions in response to the discovery of fraud or corruption. More specifically, the standard requires the capture of digital evidence at that point.

A number of fraud and corruption events fail to be investigated correctly in the first instance because the evidence is not being captured immediately or appropriately, and it is not secured to protect it from deletion, or safeguarded against contamination. The same exists for physical evidence. The guidance also covers investigations, the investigator as well as the safety of that person, investigations planning and record-keeping. These guides are geared towards ensuring organisations are well placed to respond to incidents and prosecute where necessary.

12. New guidance around the disruption of fraud and corruption.

In many cases, an investigation may not uncover enough evidence for legal proceedings or police referral, so there is guidance around the disruption of fraud and corruption being an adequate response in these circumstances by ensuring the activity does not continue. The standard refers to actions like:

- increased audit activity
- increased monitoring of specific transactions
- internal control augmentation
- delivery channel re-evaluation
- augmented identity checking.

Assessing compliance with standards

Many of these changes are already considered and recommended in the effective mitigation of the impact of fraud and corruption on businesses and organisations. Inclusion in the revised standard will make them a 'must'. As such, organisations will need to begin reviewing their fraud control program and implement critical changes to create a fraud and corruption control system and to ensure they are complying with the revised 2021 standard.

Are standards mandatory?

One of the key questions that many businesses and organisations have is whether these standards are mandatory—it is a bit of a 'yes' and 'no'.

While standards are a good reference point for businesses, they are not legally binding unless they are incorporated into legislation—such as the standards for child car seats, for example. In this case, the law imposes a duty to use the Australian standard to ensure compliance with the legal obligations.

Where standards are not incorporated into law, they do serve as an excellent source of reference.

When the courts or tribunals are looking at a determination as to whether the company did all things reasonably possible to manage the risk, they will often look at whether the company was compliant with Australian standards.

Organisations should be aware of what Australian standards are and how they apply to their business operations. Complying with the standards now could save a company some serious problems (and money) at a later time.

What about instances where there are international Standards (ISOs)?

International standards, for example, ISO 37001-2019 *Anti-Bribery Management Systems*, can also be considered in conjunction with the equivalent Australian standard. This means that an international standard may be useful, particularly where its use achieves the same or better overall level of risk mitigation to its Australian standard equivalent. **FS**