Fraud Control Policy

NOVEMBER 2016

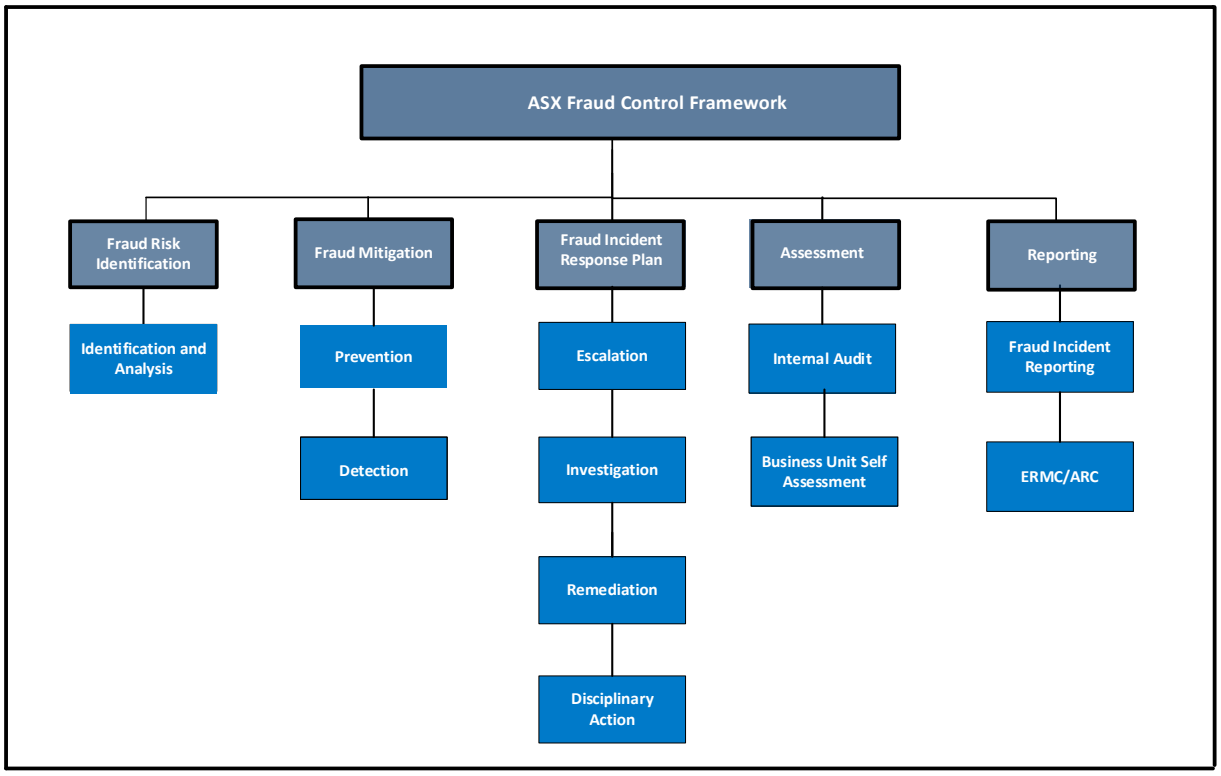
ASX

CONTENTS

1. Overview

The ASX Fraud Control Policy outlines the principles and framework implemented to ensure ASX is able to minimise the risk of fraud occurring across the organisation. As a markets operator and provider of clearing and settlement facilities ASX is subject to the risk of fraud occurring - either internally by staff, externally by third parties upon ASX or externally by third parties targeting customers using ASX's name or infrastructure - and requires strong fraud prevention and detection procedures. Additionally, given the unique nature of fraud risk and the extensive impacts a fraudulent event can have, comprehensive response procedures are in place to limit any negative organisational impacts.

The ASX Fraud Control Framework has been developed to enable executive management and business units to implement appropriate fraud prevention, detection and response processes. The framework was designed with reference to AS 8001-2008: Fraud and Corruption Control and comprises several elements as summarised in the diagram below.



The ASX Fraud Control Framework consists of the following elements:

Fraud Risk Identification	The identification and assessment of specific fraud risks applicable to ASX.
Fraud Mitigation	Implementation of both preventative and detective fraud control measures to reduce the risk of fraud occurrence and to allow for prompt identification of incidents if they occur. Fraud awareness training is provided to ASX staff focussing on task diligence and concern

	escalation with references to the ASX Code of Conduct and ASX Whistleblower Protection Policy.
Fraud Incident Response	Includes investigation responsibilities, remedies and reporting requirements for fraud incidents that do occur. Initial investigations into alleged or potential frauds are to be conducted by a Fraud Response Team comprising Internal Audit, Office of General Counsel and Human Resources.
Fraud Assessment	An annual fraud risk assessment is conducted by Internal Audit to identify and document key fraud risks and associated mitigations. In addition, fraud is considered in the majority of the audits performed by Internal Audit and also by the external auditors. Business units self-assess their fraud risks as part of their risk profiling activities.
Reporting	Regular reporting of fraud risks and any fraud incidents is undertaken to both the Enterprise Risk Management Committee (ERMC) and, if significant, the Audit and Risk Committee (ARC).

Overall, the ASX Fraud Control Framework is a combination of embedded fraud controls and general staff awareness supported by regular business unit and independent fraud risk assessment. On-going execution of this framework is expected to minimise the occurrence and impacts of fraud across the ASX.

2. Introduction

Fraud involves dishonestly obtaining an advantage through the intentional misrepresentation, deception, or concealment of information. General examples of fraud potentially manifesting at ASX, whether from within the organisation itself or from an external source, include:

- financial theft or misappropriation of cash or securities
- improper or unauthorised expenditure
- unauthorised or inappropriate access to or release of information
- forgery and alteration of documents
- inappropriate use of insider knowledge
- misappropriation or misallocation of organisational resources, such as computer or telecoms equipment
- inappropriate or favourable treatment of associated parties for personal benefit
- falsification of records and data, such as payment or payroll records, and
- fraudulent financial reporting.

Factors identified that can increase the risk of fraud at ASX include:

- busy schedule of business and system change activities, including changes to processes and internal control
- processing of high value, high volume financial market transactions
- intelligent, sophisticated employees and customers
- complex systems and products
- remote/dual site team operations and frequent organisation restructures
- on-going business expansion and increasing number of initiatives new to ASX

- adoption of sales based reward programs
- competition across wider span of ASX's businesses
- certain key procedures and controls are performed manually
- concentrated business and system knowledge, and
- potential for collusion on the part of employees, customers or suppliers.

Conversely, key factors identified that can reduce the risk of fraud include:

Centralised operations	– there is a limited geographical spread of activities with key operations centralised in Sydney
Cost control focus	– there is a strong culture of sustainable cost control within the organisation encouraging close review of resource usage
Daily automated transaction processing	– a significant component of ASX's processing and workflow is IT based and is matched, settled and reconciled automatically on a daily basis
Transparent range of business activities	– the markets and facilities operated by ASX are transparent in nature, subject to on-going analysis and monitoring by a range of internal and external parties.

3. Objectives and Principles

3.1. Objectives

The objectives of the ASX Fraud Control Framework are to:

1. identify and assess potential risks and sources of fraud within the organisation
2. design effective mitigating controls to reduce the opportunity to commit fraud and detect its occurrence should the preventative controls not be designed or operating effectively
3. enable effective responses and investigations into fraud incidents to reduce their impact and potential loss amounts
4. provide a mechanism and environment for staff to report suspected fraud incidents, and
5. facilitate reporting of the fraud control environment and timely reporting of fraud incidents.

3.2. Principles

The key principles governing the ASX Fraud Control Framework and application are:

1. ASX has zero tolerance for fraudulent or dishonest activity within the organisation
2. Responses to fraud incidents need to be objective, timely and comprehensive
3. Business units take responsibility for fraud risk and are required to understand and mitigate their fraud risks; and

4. Staff are required to contribute to the minimisation of fraud occurrence and impacts.

4. Scope

The ASX Fraud Control Framework applies to any activities potentially subject to fraud, or suspected fraud, involving employees, consultants, vendors or contractors and/ or any other parties with a corporate relationship with ASX in any of its locations. This includes fraud associated with cyber security risks such as phishing and malware (ransomware) intrusion.

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and other personal details (e.g. bank account or credit card details) by masquerading as a trustworthy entity in an electronic communication (e.g. in an email or on a website). Phishing is a form of fraud and is covered in general by the principles of this policy. However, given the unique nature and technology focus associated with phishing, more specific consideration is contained within the ASX Technology Security framework.

Fraud may also be perpetrated at other organisations connected to ASX infrastructure. For example, a customer's trading account at a participant could be compromised and used to perform unauthorised share transactions on the ASX market. This type of fraud is not covered by this policy. ASX works with ASIC to communicate the risks of this type of fraud and encourages participants to implement comprehensive cyber security controls.

External payment frauds occur occasionally whereby requests are made to customers purportedly from ASX (e.g. an investor receives an ASX-styled letter advising a share transfer will be completed upon pre-payment of funds). Such frauds do not impact ASX directly and are not covered by this policy. A standardised response procedure is being developed for these types of incidents to rapidly re-direct customers to the police. An anti-phishing notice is also being drafted.

5. Roles and Responsibilities

Chief Risk Officer

The Chief Risk Officer (CRO) is responsible for managing, monitoring, and implementing the ASX Fraud Control Policy.

Audit and Risk Committee

The ARC notes the ASX's Fraud Control Policy and considers fraud control reports.

Enterprise Risk Management Committee

The ERMC is responsible for approving and overseeing implementation of the Fraud Control Policy, including reviewing incidents and fraud control reports.

Business Risk Committee

The BRC is responsible for contributing to this policy and follow up of fraud incident learnings.

Fraud Response Team

Refer to Section 6.2.

Internal Audit

Internal Audit is responsible for considering ASX's fraud control arrangements as part of its audit coverage and individual assignment scopes. Specifically, Internal Audit is responsible for conducting an annual ASX-wide fraud risk control assessment and participating in the Fraud Response Team as required.

Enterprise Risk

The facilitation and ongoing maintenance of ASX's Fraud Control Policy is the responsibility of Enterprise Risk. Specific responsibilities include:

- developing and maintaining the ASX Fraud Control Policy and procedures
- reviewing fraud risks in the business unit risk profiles; and
- coordinating the awareness steps of the Fraud Control Policy.

Group General Counsel and Group Executive, Human Resources

Group General Counsel and GE, Human Resources, together with General Manager Internal Audit, are to form a Fraud Response Team in the event a significant fraud is suspected or an investigation initiated.

Business Unit Group Executives and General Managers

Business Unit Group Executives and General Managers are responsible for:

- identification of fraud risks in their business unit and including them in their risk profile
- the design and operation of fraud controls in their business unit; and
- escalating potential or actual fraud incidents to CRO, Internal Audit, Office of General Counsel and/or Human Resources.

ASX Staff

ASX staff are required to:

- perform their roles and tasks ethically and diligently
- be vigilant and report any instances of suspected fraud promptly; and
- actively participate in ASX fraud awareness training as required.

6. Policy Statements

6.1. Identification and analysis

Fraud risks can arise from a number of areas within the ASX as noted above.

Reference	Policy Statement
FR01	Business unit managers are to assess existing and new business activities for fraud risks. As with other risk categories, identified fraud risks are to be assessed in terms of likelihood of occurrence and impact to the organisation.

6.2. Mitigating fraud controls

Control procedures to mitigate the risk of fraud can either be preventative or detective, or both, in nature. Examples of each include:

Preventative

- workplace policies and culture promoting and encouraging ethical behaviour
- new employees and contractors acknowledgement of policies upon commencement
- regular policy updates and communication to staff
- online fraud awareness training
- high risk employees subject to annual acknowledgement of some policies
- Authorisation and dual check controls within key processes
- segregation of duties (including some enforced by systems and automated workflow)
- periodic review of fraud risks and scenarios
- pre-employment screening and background checks
- system access controls
- centralised operations
- automated daily transaction processing
- physical security controls.

Detective

- escalation and provision of whistleblowing through letter, internal mail or anonymous mail
- reviews of exception reports and reconciliations and other management reporting
- exception reporting for some systems
- periods of consecutive staff leave without office/telecommunication contact
- assurance and compliance functions

These controls are either purposely implemented to prevent fraud or by their nature indirectly reduce the risk of fraud.

1. Primary Fraud Controls

   These are controls which are specifically designed to reduce the risk of fraud occurring and usually operate 'nearby' to physical assets. Segregation of duties between specific functions, the requirement for dual transaction authorising signatories and input/checker transaction approval procedures are examples of primary fraud controls.

2. Secondary Fraud Controls

   These are controls which have primary objectives of accuracy, validity and completeness, but their presence acts to deter or detect fraud. Examples include bank and system reconciliations, and supervisory reviews.

3. Risk culture

   Risk culture manifests itself in the risk attitudes ethics, integrity and competence of the people within an organisation. It is influenced by management's operating style and philosophy, the way management assigns responsibility and authority, the way the organisation structures and develops

its people and the attention and direction provided by the Board. The key elements of ASX's risk culture contributing to an effective fraud control environment include:

- management-defined policies and procedures eg policies on ethics and conduct policies (including code of conduct, whistleblower policy, dealing rules for employees and directors, employee assistance, diversity and equal opportunity, WHS, leave and working conditions);
- a culture of recognition and compliance with the organisational responsibilities in regard to regulatory, environmental and social issues;
- performance, remuneration and reward strategies and commitment to promote competence, compliance and development of staff;
- an independent board and requisite oversight committees;
- an organisational structure that promotes independent internal audit, risk management and compliance functions; and
- management focus on operational issues and willingness to discuss and address potential control weaknesses.

4. Fraud Awareness

   A common way in which internal fraud is detected is by observation and reporting by workplace colleagues of the perpetrator(s). Similarly, a likely way for externally instigated fraud to be detected is by an employee of the victim organisation. It is therefore important that ASX staff have a general awareness of fraud and the appropriate response to be adopted if this type of activity is detected or suspected. Accordingly, ASX staff are provided general fraud awareness training.

Complementary to this, ASX senior management play an important role in demonstrating the organisation's commitment to fraud control, including supporting a culture of fraud awareness and vigilance amongst staff.

Fraud controls are required to be effectively designed and implemented; however, it should be noted that any system of fraud risk management and internal control is designed to provide reasonable assurance that fraud will not eventuate. Although clearly desired, it does not guarantee that fraud will not occur; rather, its objective is to reduce the risk of fraud to an acceptable low level.

Reference	Policy Statement
FR02	Executive Management, as part of organisational risk culture settings, is required to set an appropriate fraud control "tone from the top" in terms of ethics, integrity, operating style, assignment of responsibility and authority, policies and procedures.
FR03	Business unit managers are required to implement appropriate preventative and detective fraud controls and are to support a fraud control culture.
FR04	General Manager, Enterprise Risk in conjunction with Regulatory Assurance is to coordinate organisation-wide fraud control training on an approximate two yearly basis.

6.3. Fraud incident response

Detection and Escalation

A key aim of the fraud control framework is the early detection and escalation of fraud incidents within the organisation. A culture of fraud awareness and openness in relation to fraud reporting should be encouraged with escalation to Internal Audit, Office of General Counsel or Human Resources as required. Clear channels of escalation through senior management are defined and, if applicable, the staff member(s) reporting the incident will be afforded protection as outlined in the ASX Whistleblower Policy.

Investigation

Upon notification of a fraud event, Internal Audit, Office of General Counsel and HR will form a Fraud Response Team (FRT). Actions of the FRT are to:

- identify and assess required team members;
- determine requirements to notify law enforcement or regulatory agencies of events;
- determine whether to seek to recover any misappropriated monies or assets;
- make recommendations regarding sanctions on the employees involved, up to and including terminations;
- notify insurers of fraud as required;
- implement appropriate stakeholder interaction procedures, covering media, investors, regulators, etc.
- define and conduct investigation procedures ;engage external specialists as required, and
- assess investigation results and propose recommended actions.

Refer **Appendix 1** for the Fraud Response Checklist template.

Remediation

Agreed actions to address the impacts of the fraud should be tracked and monitored by Internal Audit.

Disciplinary Action

Committing a fraudulent act and breach of internal policy is viewed seriously by ASX and staff found to be involved will be subject to disciplinary action.

Reference	Policy Statement
FR05	Staff are required to escalate any indications or occurrences of fraud. Staff reporting an incident will, as appropriate, be afforded protection as outlined in the ASX Whistleblower Protection Policy.
FR06	Upon notification of a fraud event, Internal Audit, Office of General Counsel and Human Resources will form a Fraud Response Team and activate appropriate actions, analysis and assessment.
FR07	Agreed actions to address the impacts of a fraud are to be tracked and monitored by Internal Audit.

Reference	Policy Statement
FR08	The commitment of a fraudulent act and breach of internal policy is viewed seriously by ASX and involved staff will be subject to disciplinary action.

6.4. Fraud assessment

Internal Audit

Internal Audit conducts two types of fraud review and assessment activities:

- high level, annual assessment of fraud risks across ASX and
- detailed assessment of fraud risks as part of each audit review conducted.

Reference	Policy Statement
FR09	Internal Audit is to include fraud risk in their audit scopes and undertake an annual fraud risk assessment.

Business Unit Self Assessment

Reference	Policy Statement
FR11	Fraud risks are to be considered by GEs and GMs as part of their 6 monthly risk profiling, requiring identification of mitigating controls and assessment of residual risks.

7. Reporting

Fraud Incident Reporting

Noting legal and other considerations, fraud related incidents and outcomes of fraud investigations are to be reported to the ERMC, ARC and external parties as appropriate.

Related internal policy breaches (if any) should follow the ASX Procedure for Addressing Breaches in Internal Policy.

ERMC /ARC Reporting

In addition to any incident reporting, both ERMC and ARC receive and review the annual ASX Fraud Risk Assessment from Internal Audit. Industry developments and fraud occurrences amongst peer organisations are also considered in this report.

External Audit are required to perform certain fraud procedures and report to the ARC if they have observed any indications of fraud during their audit enquiries and procedures.

8. Relationship to other documents

This policy should be considered with reference to the following underlying policies and guides:

- ASX Code of Conduct
- ASX Whistleblower Protection Policy

Appendix 1 – Fraud Response Checklist

The following table includes guidance for the Fraud Response Team on areas to be considered in the event of a suspected fraud event.

Area	Action	Considerations	Responsibility	Status
Fraud Response Team Composition	Agree composition of Fraud Response Team.	• Chair • Independence/Objectivity/ Conflicts of interest • Size and nature of fraud • Required skills sets • Establishment of specific investigation team	GM, Internal Audit Group General Counsel GE, Human Resources	
Police Notification	Determine requirements to notify law enforcement agencies of events.	• State Police Fraud Squad	Group General Counsel	
Asset Recovery	Make recommendations to seek to recover a missing monies or assets.	• Speedy recovery response action more likely to be successful	FRT	
Staff	Make recommendations regarding appropriate remediation / disciplinary actions.	• Employment laws • Suspensions	GE, Human Resources	
Confidentiality	Remind and enforce confidentiality requirements around FRT activities.	• Confidential treatment of response actions is important in the management of potential negative impacts of fraud. • Internal and external parties	FRT	
Evidence	Implement arrangements to secure evidence.	Potential to seek legal remedy influenced by sufficiency of evidence • Interviews • Telephone records • Data recovery • External parties	Group General Counsel	
Insurance	Notify insurers of fraud as required.	• Bond, Electronic & Computer Crime Policy • Fidelity policy	Group General Counsel Chief Financial Officer	
Stakeholders	Implement appropriate stakeholder interaction procedures, covering media, investors, regulators, etc.	• Media • Investors • Regulators • Staff	FRT / GEs / EGMs	
Investigation	Define and conduct investigation procedures.	• Scope • Procedures • Event facts • Accountabilities • Root causes	GM, Internal Audit	
Recommendations	Assess investigation results and propose recommended actions.	• Present results to ERMC/ARC	GM, Internal Audit	