Draft Prudential Practice Guide

SPG 223 – Fraud Risk Management

October 2014

Disclaimer and copyright

This prudential practice guide is not legal advice and users are encouraged to obtain professional advice about the application of any legislation or prudential standard relevant to their particular circumstances and to exercise their own skill and care in relation to any material contained in this guide.

APRA disclaims any liability for any loss or damage arising out of any use of this prudential practice guide.

About this guide

Prudential practice guides (PPGs) provide guidance on APRA's view of sound practice in particular areas. PPGs frequently discuss legal requirements from legislation, regulations or APRA's prudential standards, but do not themselves create enforceable requirements.

This PPG is to be read with APRA's prudential standards and PPGs relevant to fraud risk management – in particular, *Prudential Standard SPS 220 Risk Management* (SPS 220) and *Prudential Practice Guide SPG 220 Risk Management* (SPG 220).

SPS 220 sets out APRA's requirements for a registrable superannuation entity (RSE) licensee to have systems for identifying, assessing, managing, mitigating and monitoring material risks that may affect its ability to meet its obligations to beneficiaries. This PPG aims to assist an RSE licensee in complying with those requirements and, more generally, to outline prudent practices in relation to the management of fraud risk.

For the purposes of this guide, and consistent with the application of SPS 220, 'RSE' and 'RSE licensee' have the meanings given in the *Superannuation Industry (Supervision) Act 1993* (SIS Act).

Subject to the requirements of SPS 220, an RSE licensee has the flexibility to structure its business operations in the way most suited to achieving its business objectives. Not all of the practices outlined in this PPG will be relevant for every RSE licensee and some aspects may vary depending upon the size, business mix and complexity of the RSE licensee's business operations.

Table of contents

Chapter 1 — Introduction

1. Under SPS 220, an RSE licensee is responsible for ensuring that its risk management framework covers all material risks to its business operations, both financial and non-financial. An effective risk management framework therefore includes appropriate consideration of fraud risk, which is a subset of operational risk.[1]
2. Fraud risk refers to the risk of loss from internal fraud or external fraud. These can be defined as:
   a) internal fraud - losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy (excluding diversity / discrimination events) which involves at least one internal party; and
   b) external fraud - losses due to acts of a third party that are of a type intended to defraud, misappropriate property or circumvent the law.[2]
3. This PPG provides guidance on APRA's expectations of the treatment of fraud risk in an RSE licensee's risk management framework. The PPG outlines sound practices in relation to the management of fraud risk throughout an RSE licensee's business operations.[3]
4. APRA expects that appropriate consideration of fraud risk by an RSE licensee would also include consideration of the risks posed to the RSE licensee's business operations due to corruption and bribery.[4]

[1] Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events and is a material risk of the business operations of an RSE licensee. Refer to SPG 220 for guidance on categories of material risks.

[2] Refer to Attachment A of SPG 220.

[3] The definition of an RSE licensee's business operations in SPS 220 is sufficiently broad to include risks arising not only from RSEs within those business operations, but also other, non-superannuation activities of the RSE licensee, such as the operation of a managed investment scheme, to the extent that those activities may pose a material risk to the activities of the RSE licensee.

[4] *Australian Standard AS8001-2008 - Fraud and Corruption Control* (AS8001-2008) defines corruption as "dishonest activity in which a director, executive, manager, employee or contractor of an entity acts contrary to the interests of the entity and abuses his/her position of trust in order to achieve some personal gain or advantage for him or herself, or for another person or entity" and a bribe as "the act of paying a secret commission to another individual. It is also used to describe the secret commission itself".

Chapter 2 — Fraud risk management framework

5. Under SPS 220, the Board[5] of an RSE licensee is ultimately responsible for the risk management framework. It is APRA's view that a core element of an effective risk management framework is a strong risk culture that exhibits organisational attributes and behaviours which reflect an intolerance of fraud.

6. SPS 220 provides the minimum criteria that must be included in an RSE licensee's risk management framework to appropriately manage different types of material risks. APRA expects that an RSE licensee's risk management framework would include a framework for the management of fraud risk. This framework would be expected to address the risks arising from both internal fraud and external fraud in a manner that is commensurate with the RSE licensee's broader risk management framework and which reflects the size, business mix and complexity of the RSE licensee's business operations.

7. Under SPS 220, an RSE licensee must maintain an up-to-date risk appetite statement. APRA expects that an RSE licensee's risk appetite statement would cover the fraud risks of its business operations and would articulate its intolerance for those risks, albeit recognising that elimination of fraud risk is unlikely to be possible in practice. Paragraph 15 below sets out approaches a prudent RSE licensee would consider in managing fraud risk.

8. APRA also expects that a prudent RSE licensee would consider how its risk management strategy would effectively communicate, both internally and externally, its approach to managing fraud risk. This may include, for example, relevant policies by reference, such as an employee code of conduct, fitness and propriety policy or whistleblowing policy.

9. APRA considers that an effective fraud risk management framework would enable an RSE licensee to form a clear understanding of its fraud risk profile, taking into consideration fraud risk scenarios, organisational change and incident and action management.

10. For the purposes of the Operational Risk Financial Requirement (ORFR) under *Prudential Standard SPS 114 Operational Risk Financial Requirement*, an RSE licensee must determine the financial resources necessary to address operational risks that it has identified in its risk management framework, taking into account its risk appetite and appropriate risk mitigations and controls (the ORFR target amount). This amount must reflect any uncertainty in the scale of losses. APRA expects that there will be alignment between the fraud risks considered by an RSE licensee when developing its fraud risk management framework and those identified for the purposes of determining the ORFR target amount.

11. A prudent RSE licensee would supplement the guidance outlined in this PPG with external sources of information relating to the development and implementation of a fraud risk management framework.[6]

12. SPS 220 requires that an RSE licensee have a designated risk management function. APRA considers that an effective risk management function is an integral part of an RSE licensee's risk management framework. It is therefore APRA's expectation that the role of the risk management function would include oversight of fraud risks.

[5] For the purposes of this PPG, a reference to 'the Board' is a reference to the Board of directors or group of individual trustees of an RSE licensee and 'group of individual trustees' has the meaning given in s. 10(1) of the SIS Act.

[6] For example, see AS8001-2008 and ASFA Best Practice Paper No. 20 – *"Managing the risk of fraud and corruption in superannuation funds"*.

13. Under SPS 220, an RSE licensee must maintain financial, human and technical resources at a level adequate to enable the RSE licensee to support its risk management framework. An RSE licensee must also be able to demonstrate to APRA that it has a process to determine the level of resources that are adequate based on an assessment of the business plan, risk management framework and the size, business mix and complexity of the RSE licensee's business operations. APRA expects that an RSE licensee would consider the adequacy of resources to support its fraudrisk management framework as part of this process.

14. An RSE licensee is responsible for ensuring its risk management framework is comprehensively reviewed in accordance with SPS 220. APRA expects that the scope of this comprehensive review would include the fraud risk management framework.

Chapter 3 — Development and implementation of the fraud risk management framework

15. Prudent practice suggests that an RSE licensee would consider a number of different approaches to managing fraud, depending on the source of potential risk. These may include, but not be limited to, the approaches outlined in this PPG. In APRA's view, a prudent RSE licensee would include the development of a suite of fraud risk controls that are designed to prevent fraud from occurring, to detect fraud when it occurs and to respond to fraud as it is detected.

Planning and resourcing

16. APRA considers that an effective risk management strategy includes a fraud control plan to reflect the application of a structured risk management approach to fraud risks.

17. In developing the fraud risk management framework, APRA expects an RSE licensee to consider previously identified fraud risks and existing policies and procedures pertaining to the management of these risks, such as a code of conduct or statement of ethics.

18. APRA is of the view that the senior management of the RSE licensee is responsible for the planning, execution and ongoing maintenance of the fraud risk management framework. Senior management ordinarily has close engagement with the business operations of the RSE licensee and is thus best placed to understand and manage the risks affecting those business operations. A key role of senior management is to consider whether the fraud control plan is meeting its objectives and that the measures implemented are addressing the identified risks across the entirety of the RSE licensee's business operations.

19. The risk management function would ordinarily be responsible for the design and development of the fraud risk management framework. This process may include the provision of specialist advice and training, and review and challenge to support consistent implementation of the framework.

20. The internal audit function would ordinarily be responsible for the provision of independent assurance on the fraud risk management framework. External fraud management experts may be used to support the internal audit function in providing assurance, including through consultation during the planning and resourcing phase.

Fraud prevention

21. APRA considers that an RSE licensee's fraud prevention approach is the primary and most cost effective defence against fraud risk. An effective approach to fraud risk prevention includes the establishment of an appropriate risk culture that promotes ethical behaviour across all levels of the staff of the RSE licensee and implements fraud risk controls to prevent and detect incidents of fraud. A prudent RSE licensee would inform third parties, such as contractors and suppliers, of its risk appetite in respect of fraud to strengthen the overall risk culture of the RSE licensee.[7]

22. Measures that an RSE licensee may consider adopting in the establishment of a strong risk culture include, but are not limited to:

    a) establishing an ethical culture supported and modelled by the Board and senior management who are seen to follow policies and procedures, and provide suitable role models for both employees and organisations with whom an RSE licensee may engage;

    b) creating or updating policies that communicate an RSE licensee's attitude and behavioural expectations in relation to fraud risk, such as a code of conduct or statement of ethics. These policies may include guidance on identifying, investigating and reporting fraud, values held by an RSE licensee, expected

[7] Refer to *Prudential Standard SPS 231 Outsourcing* for requirements relating to outsourcing.

behaviours, unacceptable conduct and consequences. These policies may have regard to the fraud control plan or other risk management related policies such as employee screening, data management, information technology usage and security and compliance with Anti-Money Laundering and Counter-Terrorism Financing Rules[8];

c) incentives and performance management policies for directors, senior management and staff that promote a strong risk culture;

d) communicating ethical behaviour responsibility through training on the code of conduct, statement of ethics and specific fraud risk management policies; and

e) internal declarations confirming compliance with all relevant policies. As part of a broader suite of measures, declarations can contribute to individual adherence to a positive risk culture.

23. APRA considers that identifying and implementing fraud risk controls that ensure adequate resources be maintained to manage significant fraud risks is integral to an RSE licensee's prevention approach. In identifying and implementing these fraud risk controls, APRA expects that an RSE licensee would consider both fraud risks and other types of risks concurrently to ensure that all risk controls integrate appropriately.

24. Preventative fraud risk controls may include, but are not limited to:

a) conducting regular fraud risk assessments that reflect an RSE licensee's policies and processes governing initial and ongoing assessment of fraud risks. Fraud risk assessments are central in assisting an RSE licensee to understand and assess its current and emerging fraud risk environment and its existing fraud risk controls. APRA considers that an effective fraud risk assessment process would be conducted across all of an RSE licensee's business units. A prudent RSE licensee may consider use of external fraud management experts in respect of fraud risks in specialised areas, for example the risks posed by information technology systems;

b) consideration of past fraud incidents, both internal and external, including how the RSE licensee managed and resolved the incidents. In considering past fraud incidents, a prudent RSE licensee would consider external sources of information that provide insight into broader market instances of fraud, in order to more fully understand the fraud risk environment. Past fraud incidents may inform an RSE licensee about how to improve management of fraud risk by providing insight into why fraud risk controls failed;

c) performance management policies, which can contribute to an effective fraud risk management framework through incentives to directors, senior management and staff to act in accordance with the fraud risk management framework;

d) communication such as:

i) fraud awareness training, which can contribute to a strong fraud risk management framework by setting out how to identify and correctly report fraud risk concerns;

ii) internal communication that is complementary to training, for example when incidents occur or when a new fraud risk emerges. Communication of investigation outcomes may also act as a deterrent to future improper conduct or heighten awareness of internal and external fraud risk indicators; and

iii) external communication to third parties about an RSE licensee's attitude and behavioural expectations in relation to fraud risk via the RSE licensee's website or through more direct communication such as providing third parties with policies that communicate the RSE licensee's

[8] Refer to *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*.

attitude and behavioural expectations; and

e) a fraud control plan, that documents:

i) fraud risks;

ii) person(s) responsible for fraud risk controls;

iii) key fraud indicators that fraud risk controls are designed to detect[9];

iv) processes to follow when reporting a fraud related concern, including how a subsequent investigation would be conducted; and

v) fraud risk management training to be provided.

25. Attachment B provides a non-exhaustive list of examples of preventative controls that an RSE licensee might consider implementing to mitigate fraud risk.

Fraud detection

26. APRA considers that a prudent RSE licensee would develop fraud risk controls aimed at detecting fraudulent activities, thereby limiting any potential impact and permitting timely recovery of losses.

27. Prudent practice suggests that an RSE licensee's detection approach would be developed and reviewed during the fraud risk assessment process.

28. APRA expects that an RSE licensee would employ a combination of both proactive and reactive detection controls:

a) proactive controls are periodic measures designed to actively seek out evidence of fraudulent activity and allow objective assessment of the effectiveness of the fraud risk controls in place. Proactive controls detect and address fraud, but also, in instances where no fraud is detected, provide assurance that fraud is being effectively controlled; and

b) reactive controls are tools or systems designed to identify indicators of fraud, to detect fraud when it has occurred, and are typically structured as part of an RSE licensee's business as usual processes.

29. Proactive controls may include, but are not limited to:

a) monitoring and review of financial and operational data for indications of fraud, which may take the form of transactional analysis or compliance assessment;

b) data analysis of electronic records, including databases, to identify unusual trends or suspicious activity indicative of fraud. Such analysis may identify improper financial practices or weak controls; and

c) the involvement of professionals with sufficient expertise to identify, evaluate and report on fraud risks. For example, internal auditors and/or external auditors may test the effectiveness of fraud risk controls, identify weaknesses in the overall fraud risk management framework and provide advice on how to address the weaknesses for planning and resourcing purposes and for the detection of fraud.

30. Reactive controls may include, but are not limited to:

a) assessment of discrepancies identified during regular key reconciliations of financial and accounting data to independent data, for indications of fraud. Where feasible, it would be prudent practice to conduct such reconciliations with regard to the frequency at which members are permitted to transact, i.e. redeem, switch or make additional contributions;

b) assurance that assets are properly recorded, properly valued and their existence verified;

c) transactional review and monitoring of business operations that includes measures to detect unauthorised transactions and inaccurate records;

[9] Refer to Attachment A for a non-exhaustive list of examples of potential fraud that an RSE licensee may refer to when determining key fraud indicators.

d) whistleblowing policies, an integral component of a fraud detection approach, that facilitate reports from both within an RSE licensee and from third parties; and

e) specific training and communication, to staff responsible for fraud risk controls in their daily role, on how to ensure fraud risk controls work effectively.

31. Attachment B provides a non-exhaustive list of specific examples of proactive and reactive detection controls that an RSE licensee might consider implementing to mitigate fraud risk.

Fraud response

32. APRA considers that timely investigation and response to detected incidents of actual or potential fraud is a key component of an effective fraud risk management framework. An effective response to fraud minimises losses and maximises potential recoveries. In addition, an effective response assists in ensuring that an RSE licensee adheres to its legislative obligations.

33. APRA expects that an RSE licensee would investigate all instances of actual or potential fraud that are detected. A robust fraud investigation seeks to determine facts and to identify risk issues and control weaknesses.

34. A prudent RSE licensee would have in place procedures to govern the investigation of suspected fraud. APRA's expectation is that these procedures would designate the person(s) responsible for overseeing and carrying out the investigation and establish rules relevant to the conduct of the investigation, such as rules governing the conduct of interviews, evidence handling, treatment of persons involved and reporting of outcomes.

35. It is APRA's view that sound fraud investigations would be conducted by appropriately skilled and experienced personnel, independent of the business unit in which the alleged fraudulent conduct has occurred. Appropriate personnel for the investigation may be a director, senior manager or an external consultant. Alternatively, the investigation may be carried out by cooperation with an external law enforcement agency.

36. APRA expects that an RSE licensee would capture all incidents of fraud and maintain a process that manages incidents of fraud as part of its fraud risk management framework, with appropriate linkage to its ORFR strategy. An effective process that manages incidents of fraud would report all such incidents to senior management and as appropriate to relevant Board Risk Committees and the Board.

37. APRA considers that it would be prudent for an RSE licensee to undertake a formal process to determine whether the matter should be reported to a law enforcement agency for investigation. In the case of material fraud events, a prudent RSE licensee would also consider making a report to APRA and would determine whether a Significant Event Notice is required.[10]

38. A prudent RSE licensee would typically be expected to operate a register to capture all incidents of detected fraud, to be analysed to further improve the RSE licensee's fraud risk management framework.

39. Following a fraud event, APRA expects that an RSE licensee would reassess the adequacy of the internal control environment and consider whether improvements are required to the fraud risk management framework.

[10] Refer to s. 106(1) of the SIS Act.

40. APRA considers that a sound communication strategy can contribute to a strong fraud response approach, as a proactive measure in the event of a fraud incident. A sound communication strategy typically addresses internal and external communication needs, including interaction with law enforcement agencies and regulators, and outlines procedures for responding to external enquiries that arise after fraud is detected.

41. A prudent RSE licensee would document its response measures within its fraud control plan.

Monitoring and review

42. APRA is of the view that an effective fraud risk management framework would incorporate regular monitoring and review of fraud risk controls to assess whether they remain suitable and current. An RSE licensee's business operations evolve over time, as does the risk landscape in which it operates. Therefore, a prudent RSE licensee would be vigilant in monitoring and reviewing its fraud risk controls. Such a review would ensure that fraud risk controls continue to address identified fraud risks and address any emerging risks identified during the review.

43. APRA considers that effective monitoring and review of the fraud risk management framework would include, but not be limited to:

    a) testing and review of the implementation and functioning of the fraud control plan. Prudent practice suggests that testing and review would be conducted by each of the RSE licensee's business units and the risk management function, through risk based testing of controls that are considered to be most critical for the prevention of fraud or that may have previously failed to prevent or detect an incidence of fraud; and

    b) independent evaluation of fraud risk controls by internal audit, to identify any control weaknesses and ensure corrective actions in response to past control weaknesses are effective.

Chapter 4 — Superannuation-specific fraud risk

44. In APRA's experience, common types of fraud perpetrated in relation to the business operations of RSE licensees include the diversion of funds, misappropriation of assets and the improper registration and use of an RSE's assets. Attachment A provides a non-exhaustive list of examples of fraud that are relevant to RSE licensees.

45. When developing its fraud risk management framework, a prudent RSE licensee would consider, in particular, investment risks and risks posed by the engagement of an outsourced service provider that arise from activities within its business operations.

Investment risks

46. APRA expects that an RSE licensee would undertake appropriate due diligence prior to any investment being made to mitigate the risk of investment related fraud occurring within its business operations. The RSE licensee's due diligence process would assist in gaining an adequate understanding of the investment and investment manager under consideration. A prudent RSE licensee would consider the level of fraud risk in a potential investment and conduct investment reviews proactively to minimise the potential for fraud to occur. In conducting such reviews, a prudent RSE licensee would give consideration to the fraud risks associated with any underlying investments made by the investment manager. Where a chain of investments is made, an RSE licensee would ensure they understand the ultimate investment and assess the fraud risk that investment poses.[11]

47. Unmitigated conflicts of interest can contribute to the risk of fraud events occurring. Consequently, an investment review may include the identification of undisclosed conflicts of interest and the provision of advice regarding the commercial rationale of investments to ensure investment decisions remain and are made in the best interest of beneficiaries.[12]

48. APRA's view is that where internal resources lack sufficient experience or independence to make an objective assessment, an RSE licensee would consider engaging an independent advisor with sufficient expertise to conduct due diligence and provide assurance on the level of fraud risk in a potential investment.

49. It is APRA's view that a sound investment governance process would include measures to prevent individuals from dominating the investment decision-making process. Without appropriate controls supported by an effective risk management function, concentration of investment expertise and decision-making within an RSE licensee to one or two key individuals may increase its exposure to fraud risk, as investment decisions may be inadequately scrutinised.

[11] Refer to *Prudential Practice Guide SPG 530 Investment Governance* for further guidance on the due diligence and review of investments.

[12] Refer to *Prudential Practice Guide SPG 521 Conflicts of Interest* for further guidance on conflicts of duty and interest.

Outsourcing risks

50. APRA is of the view that engagement of outsourced service providers may increase an RSE licensee's exposure to fraud risk. As part of the fraud risk management framework, a prudent RSE licensee would address fraud risk where a material activity is outsourced and consider undertaking monitoring and review of the risk management systems of outsourced service providers.[13] This process would generally be provided for in the outsourcing arrangement.

51. APRA's view is that assurance about outsourced service providers may be achieved through a number of different approaches. These approaches may include, but not be limited to:

    a) a due diligence process prior to engagement of the service provider;

    b) consideration of whether the service provider has a current insurance policy that covers losses caused by fraud;

    c) being satisfied that senior management of the service provider is committed to the control of fraud risks and gain assurance that fraud risks are being properly managed;

    d) obtaining an independent review of the service provider during engagement; and

    e) tests of the systems and processes of the service provider.

[13] Refer to *Prudential Practice Guide SPG 231 Outsourcing* for further guidance on outsourced service providers.

Attachment A

1. Examples of potential fraud may include:
    a) fraud during the unit pricing process;
    b) member identity fraud to unlawfully access benefits;
    c) fraudulent benefit payments;
    d) accounts payable fraud;
    e) investment fraud, including the use of opaque structures to conceal the ultimate destination of investment funds;
    f) improper use of confidential or commercially sensitive information to provide a benefit to a member or employee of the RSE licensee or outsourced service provider;
    g) fraud during an RSE's wind up; and
    h) unauthorised access to information systems leading to theft of data and/or fraud.
2. Examples of corruption and bribery within an RSE licensee may include:
    a) corruption of procurement processes, for example bribes paid to an employee of the RSE licensee or an outsourced service provider or decisions made by an employee to benefit themselves or an associate or other third party;
    b) payment of bribes to foreign officials by a RSE Licensee or by an agent or outsourced service provider acting on behalf of a RSE Licensee; and
    c) investment decisions made with the intention of benefiting parties other than the RSE's members.
3. Characteristics of an investment that may create potential for fraud may include that the investment is:
    a) involving a related party of a responsible person of the RSE licensee, of the parent of the RSE licensee or the investment manager of the RSE licensee;
    b) specifically set up for the RSE licensee and not promoted to external investors;
    c) new, untested or promoted by an investment manager with no track record;
    d) located offshore in a poorly regulated jurisdiction;
    e) an unlisted investment;
    f) an investment that is opaque;
    g) superficially rated or recommended by research agencies without adequate analysis;
    h) subject to limited review, for example because it is part of an asset allocation mix and so is not considered as a standalone investment; and
    i) not subject to adequate external assurance.

Attachment B

Examples of fraud prevention controls

1. Control of RSE assets;
    a) Controls to safeguard transactions relating to RSE assets may include establishing:
        i) documented authorisation procedures for the release of fund assets;
        ii) physical security procedures for fund assets through the use of safes or an independent custodian;
        iii) whether there are any conflicts of interest before authorising new investments;
        iv) written agreements with custodians outlining duties, responsibilities and indemnities; and
        v) procedures to ensure all assets are registered in the name of the fund upon acquisition.
    b) Controls to ensure proper authorisation in the management of RSE assets may include:
        i) establishing procedures in accordance with the Trust Deed;
        ii) establishing and implementing an investment strategy;
        iii) considering fraud risk when authorising the appointment of investment managers, administrators and auditors;
        iv) passing resolutions on benefit payments, crediting rates and contribution rates; and
        v) delegating day-to-day responsibilities to staff and authorisation responsibilities to senior management.
    c) Controls to safeguard day-to-day activities may include procedures which:
        i) authorise the payment of fund expenses;
        ii) authorise the payment of benefits, including insurance proceeds;
        iii) obtain banking contribution receipts;
        iv) ensure contributions are allocated to the correct member account; and
        v) authorise the investment of the RSE's cash flow.

    APRA expects that an RSE licensee would have regard to *Prudential Practice Guide SPG 270 Contribution and Benefit Accrual Standards* and *Prudential Practice Guide SPG 280 Payment Standards* when considering authorisation procedures relating to contributions and benefit payments, respectively.
2. Due diligence on the staff of an RSE licensee represents a key fraud risk control. Where appropriate, employment screening may be conducted:
    a) prior to the commencement of employment;
    b) when an employee becomes a responsible person of the RSE licensee;
    c) when an employee is moved into a position that has a significant exposure to fraud risk; and
    d) as part of a periodic review of responsible persons and employees in significant risk positions to ensure they do not pose a risk to the RSE licensee.
3. Controls to manage risks relating to outsourced service providers may include:
    a) due diligence on new suppliers, to assess the potential for fraud risk;
    b) due diligence on ongoing suppliers, periodically, to assess any change in their risk profile and the need to adjust the RSE licensee's fraud risk management framework; and
    c) assessment of the procurement process by which suppliers are engaged, to obtain assurance that the process is not corrupt, either internally or externally.

4. Controls to manage risks relating to new fund members may include:

   a) due diligence on new members to determine any fraud risks, including verifying application details; and

   b) assessment of the due diligence carried out to satisfy Anti-Money Laundering and Counter-Terrorism Financing Rules.

5. Procedures to verify that data collected by an RSE licensee in the normal course of business is correct, complete and substantiated may include:

   a) establishing and documenting procedures for recording information;

   b) linking the control procedures for transaction authorisations to those of data recording so that only properly authorised transactions are recorded; and

   c) recording transactions on a timely basis to ensure that all unauthorised transactions are immediately identified.[14]

6. To manage the fraud risks posed by RSE licensees' information systems, such as theft, unauthorised access, modification or destruction, APRA expects an RSE licensee would consider employee training to highlight fraud risks associated with using information systems.[15]

7. Controls to manage corruption risks may include:

   a) creating a strong anti-bribery and corruption policy that is publically available;

   b) creating gifts and entertainment policies and procedures;

   c) rotation of personnel working in positions that the RSE licensee considers to be exposed to a high risk of bribery or corruption, to prevent the development of inappropriate relationships;

   d) controls to mitigate the risk of third parties acting on behalf of an RSE licensee engaging in bribery and/or corruption, including investment managers, custodians and agents or promoters used by an RSE licensee to generate new business;

   e) regular audits of suppliers who are deemed to present a higher risk of fraud or corruption; and

   f) providing a means for members, suppliers and other third parties to report concerns relating to bribery and corruption.

8. Controls to mitigate investment related fraud risk may include:

   a) a framework for appropriate investment limits and trading restrictions to ensure investment decisions are carried out as per the investment strategy and relevant policy;

   b) segregation of duties between the dealing, settling and reporting functions;

   c) regular reconciliations between investment manager and custodian reports and accounting records of the RSE;

   d) investment management agreements that contain a comprehensive description of duties, dealing authorities and investment restrictions;

   e) appointment of a reputable custodian; and

   f) obtaining and reviewing indemnity policies from investment related outsourced service providers.

Examples of fraud detection controls

9. Examples of proactive controls used to detect incidents of fraud within an RSE licensee may include:

   a) review and monitoring controls - transactional analysis of high risk areas or compliance review to assess effectiveness of fraud risk controls; periodic review of third parties such as contractors and outsourced service providers for

[14] Refer to *Prudential Practice Guide CPG 235 Managing Data Risk* for further guidance on reviewing data management policies.

[15] Refer to *Prudential Practice Guide CPG 234 Management of Security Risk in Information and Information Technology* for further guidance on managing information systems.

compliance with the fund's policies; periodic review of high risk accounts for duplicated information, recreated member accounts or unallocated monies; and

b) data controls - evidence of relationships between employees and members or outsourced service providers, unusual payment amounts or patterns, or manipulation of accounting records.

10. Examples of reactive controls used to detect incidents of fraud within an RSE licensee may include:

a) reconciliation controls - reconciliation between bank statements and a cashbook, between accounting records and members' statements, between investment manager statements and investments recorded in the accounting system and of withdrawals and member account movements;

b) asset verification controls - regular reconciliations between the investments recorded in the accounting system to custodian or investment manager records and with bank statements to verify there are no unauthorised transactions;

c) review and monitoring controls - material variances and/or unusual transaction patterns in accounts such as member benefit accounts, expense claims, reserves, and investment holdings should be investigated further; and

d) whistleblowing - an RSE licensee may require staff, contractors and service providers to report any known or suspected instances of fraud.

Telephone
1300 55 88 49

Email
info@apra.gov.au

Website
www.apra.gov.au

Mail
GPO Box 9836
in all capital cities
(except Hobart and Darwin)