Prudential Practice Guide

LPG 230 – Operational Risk

March 2007

www.apra.gov.au

Australian Prudential Regulation Authority

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 Standard LPS 220 Risk Management (LPS 220) sets out APRA's requirements for life companies in relation to risk management. This prudential practice guide aims to assist life companies in complying with requirements in relation to operational risk and, more generally, to outline prudent practices in relation to operational risk management.

Subject to the requirements of LPS 220, life companies have the flexibility to configure their operational risk management framework in the way most suited to achieving their business objectives.

Not all of the practices outlined in this prudential practice guide will be relevant for every life company and some aspects may vary depending upon the size, complexity and risk profile of the life company.

Operational risk

1. Operational risk is defined as the risk of loss (including to policy owners) resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk. A life company would typically apply this definition as appropriate to the size, business mix and complexity of the life company's activities and operating environment. APRA envisages that the definition and application of operational risk would be clearly understood throughout the life company in order for the life company to effectively identify and manage this risk.

2. The management of operational risk would include consideration of a broad range of risks for current and legacy operations, such as those associated with:

   (a) information technology;

   (b) human resources;

   (c) internal and external fraud;

   (d) project management;

   (e) information systems;

   (f) outsourcing;[1]

   (g) business continuity;[2]

   (h) product administration (including processing, transactions, production of documentation, underwriting and claims);

   (i) unit pricing;[3]

   (j) business processes including non-outsourced third party arrangements; and

   (k) introducing new products.

Information technology

3. Information technology (IT) risk is the risk of failure or malfunction of the IT applications and infrastructure used to support the life company. Generally, a life company's risk management framework would consider risks associated with IT infrastructure (hardware and software), security and application development and maintenance.

4. Some of the elements of IT infrastructure that may be relevant include:

   (a) network and user management;

   (b) configuration management;

   (c) system performance and capacity;

   (d) IT service request, service level management and helpdesk management;

   (e) the change request process; and

   (f) IT asset management.

5. When assessing the management of risk related to IT security, a life company may consider the relevant:

   (a) policies and standards;

   (b) prevention measures (such as preventing unauthorised access);

   (c) monitoring; and

   (d) testing of controls.

6. When considering risks associated with application development, a life company would consider whether the following are in place:

   (a) a formal methodology for application development;

   (b) governance and monitoring arrangements;

   (c) development and testing protocols;

   (d) a strategy for version control of source code;

   (e) maintenance of application documentation; and

   (f) post implementation reviews.

[1] Requirements in relation to outsourcing are set out in *Prudential Standard LPS 231 Outsourcing.*

[2] Requirements in relation to business continuity management are set out in *Prudential Standard LPS 232 Business Continuity Management*.

[3] Refer *APRA and ASIC Unit Pricing – Guide to good practice*.

Human resources

7. Aspects of a life company's human resources can lead to operational risks. In considering those risks the following may be relevant:

   (a) risk identification and assessment of the life company's human resource needs, including key persons;

   (b) background verification of employees and contractors;[4]

   (c) segregation of duties;

   (d) succession planning; and

   (e) monitoring and supervision of staff.

Fraud

8. APRA envisages that the risk management framework would address fraud risk. Fraud risk relates to the risk associated with intentional acts, undertaken with the objective of personal benefit, to tamper with or manipulate the financial or operational aspects of the business.

9. Fraudulent activity can arise from internal sources (e.g. product administration) or external sources (e.g. fictitious claims and cheque fraud) and exposes the life company to risk of financial loss if not managed appropriately.

10. In relation to fraud, the risk management framework would typically include consideration of the following elements:

    (a) segregation of duties at both an operational level and in relation to functional reporting lines;

    (b) delegation and authority limits;

    (c) financial accounting controls; and

    (d) staff training and awareness of fraud risk and policies (including a code of conduct).

Project management

11. A life company could consider addressing project management risk in its risk management framework. Project management risk is the risk that projects will not achieve the desired objectives or will have a negative impact on resource levels of the life company.

12. In relation to project management, the risk management framework could consider the management of a range of risks, including the appropriateness of the following elements:

    (a) a formal project methodology for the promulgation of project initiatives including:

        (i) setting a business case for the project;

        (ii) cost/benefit analysis;

        (iii) risk identification and assessment; and

        (iv) stakeholder sign-offs;

    (b) clearly defined and appropriate levels of delegations of authority;

    (c) ongoing monitoring of project objectives and timeframes;

    (d) centralised oversight of compliance with project management protocols; and

    (e) post-implementation review.

Information systems

13. APRA envisages that controls would be in place for ensuring that data in the risk management framework's information and reporting systems is timely, accurate and complete. Internal information and reporting systems would be secure and supported by adequate business continuity arrangements.

14. A properly functioning information and reporting system would typically:

    (a) produce detailed financial, operational and compliance data;

    (b) be able to incorporate external market information relating to events and conditions that are relevant to decision-making;

    (c) enable relevant, accurate and timely information to be reported;

[4] Requirements in relation to fitness and propriety are set out in *Prudential Standard LPS 520 Fit and Proper.*

(d) allow the life company to identify, quantify, assess and monitor business activities, exposure to risk, financial position and performance;

(e) allow the life company to monitor the effectiveness of, and compliance with, its internal control system, and report any exceptions that arise; and

(f) be reviewed regularly to assess the timeliness and relevance of information generated, and the adequacy, quality and accuracy of the system's performance over time.

Telephone
1300 13 10 60

Email
contactapra@apra.gov.au

Web site
www.apra.gov.au

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