

Chapter 14

Risk management and associated systems and controls for insurers



14.1 Application

14.1.1 **R** This section applies to an *insurer* unless it a *non-directive friendly society*.

14.1.2 **R** This section applies to a *Swiss general insurer* only in respect of the activities of the *firm* carried on from a *branch* in the *United Kingdom*.

14.1.2A **R** This section does not apply to:

- (1) an *incoming ECA provider* acting as such; or
- (2) a *firm* in relation to *benchmark activities*.

14.1.2AA **R** This section applies to a *UK ISPV*.

Internal controls: introduction

14.1.27 **R** A *firm* must take reasonable steps to establish and maintain adequate *internal controls*.

14.1.28 **G** The precise role and organisation of *internal controls* can vary from *firm* to *firm*. However, a *firm's internal controls* should normally be concerned with assisting its *governing body* and relevant *senior managers* to participate in ensuring that it meets the following objectives:

- (1) safeguarding both the assets of the *firm* and its *customers*, as well as identifying and managing liabilities;
- (2) maintaining the efficiency and effectiveness of its operations;
- (3) ensuring the reliability and completeness of all accounting, financial and management information; and
- (4) ensuring compliance with its internal policies and procedures as well as all applicable laws and regulations.

- 14.1.29A** **G** When determining the adequacy of its *internal controls*, a *firm* should consider both the potential risks that might hinder the achievement of the objectives listed in **■ SYSC 14.1.28 G**, and the extent to which it needs to control these risks. More specifically, this should normally include consideration of:
- (1) the appropriateness of its reporting and communication lines (see **■ SYSC 3.2.2 G**);
 - (2) how the delegation or contracting of functions or activities to *employees, appointed representatives* or, where applicable, its *tied agents* or other third parties (for example *outsourcing*) is to be monitored and controlled (see **■ SYSC 3.2.3 G** to **■ SYSC 3.2.4 G** and the additional guidance on the management of *outsourcing* arrangements is also provided in **■ SYSC 13.9**);
 - (3) the risk that a *firm's employees* or contractors might accidentally or deliberately breach a *firm's* policies and procedures (see **■ SYSC 13.6.3 G**);
 - (4) the need for adequate segregation of duties (see **■ SYSC 3.2.5 G**);
 - (5) the establishment and control of risk management committees;
 - (6) the need for risk assessment and the establishment of a risk assessment function (see **■ SYSC 3.2.10 G**);
 - (7) the need for internal audit and the establishment of an internal audit function and audit committee (see **■ SYSC 3.2.15 G** to **■ SYSC 3.2.16 G**).
- 14.1.29B** **G**
- (1) **■ SYSC 14.1.29G(6)** does not apply to a *Solvency II firm*.
 - (2) **■ SYSC 14.1.29G(7)** does not apply to a *Solvency II firm*, but only in relation to references to the internal audit function. It does apply to a *Solvency II firm* in relation to references to the internal audit committee.
 - (3) For *Solvency II firms*, the *PRA* has made rules implementing the governance provisions of the *Solvency II Directive* relating to internal controls (article 46), see *PRA Rulebook: Solvency II firms: Conditions Governing Business*.
 - (4) The *Solvency II Regulation* (EU) 2015/35 of 10 October 2014 also imposes specific requirements (see articles 266, 267 and 270).
 - (5) The *FCA* will take the rules and requirements in (3) and (4) into account when considering a *Solvency II firm's* internal controls.

