Chapter 13

Operational risk: systems and controls for insurers

13.1 Application

13.1.1 G SYSC 13 applies to an *insurer* unless it is a *non-directive friendly society*.

13.1.2 G SYSC 13 applies a *Swiss general insurer* only in respect of the activities of the *firm* carried on from a *branch* in the *United Kingdom*.

only in respect of the activities of the *firm* carried on from a *branch* in the *United Kingdom*.

13.1.3 G SYSC 13 applies to a *UK ISPV*.

13.1.4 G SYSC 13 does not apply to an *incoming ECA provider* acting as such.

13.2 Purpose

13.2.1 G ■ SYSC 13 provides *guidance* on how to interpret ■ SYSC 3.1.1 R and ■ SYSC 3.2.6 R, which deal with the establishment and maintenance of systems and controls, in relation to the management of operational risk. Operational risk has been described by the Basel Committee on Banking Supervision as "the risk of loss, resulting from inadequate or failed internal processes, people and systems, or from external events". This chapter covers systems and controls for managing risks concerning any of a *firm*'s operations, such as its IT systems and *outsourcing* arrangements. It does not cover systems and controls for managing credit, market, liquidity and insurance risk.

13.2.2 G Operational risk is a concept that can have a different application for different *firms*. A *firm* should assess the appropriateness of the *guidance* in this chapter in the light of the scale, nature and complexity of its activities as well as its obligations as set out in *Principle* 3, to organise and control its affairs responsibly and effectively.

13.2.3 G A *firm* should take steps to understand the types of operational risk that are relevant to its particular circumstances, and the operational losses to which they expose the *firm*. This should include considering the potential sources of operational risk addressed in this chapter: people; processes and systems; external events.

13.2.4 G [deleted]

13.2.4A G Operational risk can, amongst other things, lead to unfair treatment of consumers or lead to financial crime. A *firm* should consider all operational risk events that may affect these matters in establishing and maintaining its systems and controls.

13.2.4B G

13.3 Other related Handbook sections

13.3.1 G [deleted]

13.3.1A G The following is a non-exhaustive list of *rules* and *guidance* in the *Handbook* that are relevant to a *firm's* management of operational risk:

(1) *COBS* contains *rules* and *guidance* that can relate to the management of operational risk; for example, COBS 2 (Conduct of business obligations), COBS 4 (Communicating with clients, including financial promotions), COBS 6 (Information about the firm, its services and remuneration), COBS 7 (Insurance distribution), COBS 9 (Suitability (including basic advice)(other than MiFID and insurance-based investment products)), COBS 9A (Suitability (MiFID and insurance-based investment products provisions), COBS 10A (Appropriateness (for non-advised services) (MiFID and insurance-based investment products provisions), COBS 11 (Dealing and managing), COBS 12 (Investment research), COBS 14 (Providing product information to clients) and COBS 19 (Pensions: supplementary provisions).

13.3.1B G

13.4 Requirements to notify the appropriate regulator

13.4.1 G Under *Principle* 11 and SUP 15.3.1 R, a *firm* must notify the *FCA* immediately of any operational risk matter of which the *FCA* would reasonably expect notice. SUP 15.3.8 G provides *guidance* on the occurrences that this requirement covers, which include a significant failure in systems and controls and a significant operational loss.

13.4.2 G Regarding operational risk, matters of which the *FCA* would expect notice under *Principle* 11 include:

(1) any significant operational exposures that a *firm* has identified;

(2) the *firm*'s invocation of a business continuity plan; and

(3) any other significant change to a *firm*'s organisation, infrastructure or business operating environment.

13.5 Risk management terms

13.5.1 G In this chapter, the following interpretations of risk management terms apply:

(1) a *firm*'s risk culture encompasses the general awareness, attitude and behaviour of its *employees* and *appointed representatives* or, where applicable, its *tied agents*,to risk and the management of risk within the organisation;

(2) operational exposure means the degree of operational risk faced by a *firm* and is usually expressed in terms of the likelihood and impact of a particular type of operational loss occurring (for example, fraud, damage to physical assets);

(3) a *firm*'s operational risk profile describes the types of operational risks that it faces, including those operational risks within a *firm* that may have an adverse impact upon the quality of service afforded to its *clients*, and its exposure to these risks.

13.6 People

13.6.1 G A *firm* should consult SYSC 3.2.2 G to SYSC 3.2.5 G for *guidance* on reporting lines and delegation of functions within a *firm* and SYSC 3.2.13 G to SYSC 3.2.14 G for *guidance* on the suitability of *employees* and *appointed representatives* or, where applicable, its *tied agents*. This section provides additional *guidance* on management of *employees* and other human resources in the context of operational risk.

13.6.2 G A *firm* should establish and maintain appropriate systems and controls for the management of operational risks that can arise from *employees*. In doing so, a *firm* should have regard to:

(1) its operational risk culture, and any variations in this or its human resource management practices, across its operations (including, for example, the extent to which the compliance culture is extended to in-house IT staff);

(2) whether the way *employees* are remunerated exposes the *firm* to the risk that it will not be able to meet its regulatory obligations (see SYSC 3.2.18 G). For example, a *firm* should consider how well remuneration and performance indicators reflect the *firm*'s tolerance for operational risk, and the adequacy of these indicators for measuring performance;

(3) whether inadequate or inappropriate training of *client*-facing services exposes *clients* to risk of loss or unfair treatment including by not enabling effective communication with the *firm*;

(4) the extent of its compliance with applicable regulatory and other requirements that relate to the welfare and conduct of *employees*;

(5) its arrangements for the continuity of operations in the event of *employee* unavailability or loss;

(6) the relationship between indicators of 'people risk' (such as overtime, sickness, and *employee* turnover levels) and exposure to operational losses; and

(7) the relevance of all the above to *employees* of a third party supplier who are involved in performing an *outsourcing* arrangement. As necessary, a *firm* should review and consider the adequacy of the staffing arrangements and policies of a service provider.

13

Employee responsibilities

13.6.3 G A *firm* should ensure that all *employees* are capable of performing, and aware of, their operational risk management responsibilities, including by establishing and maintaining:

(1) appropriate segregation of *employees*' duties and appropriate supervision of *employees* in the performance of their responsibilities (see SYSC 3.2.5 G);

(2) appropriate recruitment and subsequent processes to review the fitness and propriety of *employees* (see SYSC 3.2.13 G and SYSC 3.2.14 G);

(3) clear policy statements and appropriate systems and procedures manuals that are effectively communicated to *employees* and available for *employees* to refer to as required. These should cover, for example, compliance, IT security and health and safety issues;

(4) training processes that enable *employees* to attain and maintain appropriate competence; and

(5) appropriate and properly enforced disciplinary and employment termination policies and procedures.

13.6.4 G A *firm* should have regard to SYSC 13.6.3 G in relation to *approved persons*, people occupying positions of high personal trust (for example, security administration, payment and settlement functions); and people occupying positions requiring significant technical competence (for example, *derivatives* trading and technical security administration). A *firm* should also consider the *rules* and *guidance* for *approved persons* in other parts of the *Handbook* (including *APER*, *COCON* and *SUP*) and the *rules* and *guidance* on *senior manager* responsibilities in SYSC 2.1 (Apportionment of Responsibilities).

13.7 Processes and systems

13.7.1 G A *firm* should establish and maintain appropriate systems and controls for managing operational risks that can arise from inadequacies or failures in its processes and systems (and, as appropriate, the systems and processes of third party suppliers, agents and others). In doing so a *firm* should have regard to:

(1) the importance and complexity of processes and systems used in the end-to-end operating cycle for products and activities (for example, the level of integration of systems);

(2) controls that will help it to prevent system and process failures or identify them to permit prompt rectification (including pre-approval or reconciliation processes);

(3) whether the design and use of its processes and systems allow it to comply adequately with regulatory and other requirements;

(4) its arrangements for the continuity of operations in the event that a significant process or system becomes unavailable or is destroyed; and

(5) the importance of monitoring indicators of process or system risk (including reconciliation exceptions, compensation payments for *client* losses and documentation errors) and experience of operational losses and exposures.

Internal documentation

13.7.2 G Internal documentation may enhance understanding and aid continuity of operations, so a *firm* should ensure the adequacy of its internal documentation of processes and systems (including how documentation is developed, maintained and distributed) in managing operational risk.

External documentation

13.7.3 G A *firm* may use external documentation (including contracts, transaction statements or advertising brochures) to define or clarify terms and conditions for its products or activities, its business strategy (for example, including through press statements), or its brand. Inappropriate or inaccurate information in external documents can lead to significant operational exposure.

13.7.4 G A *firm* should ensure the adequacy of its processes and systems to review external documentation prior to issue (including review by its compliance, legal and marketing departments or by appropriately qualified external advisers). In doing so, a *firm* should have regard to:

(1) compliance with applicable regulatory and other requirements;

(2) the extent to which its documentation uses standard terms (that are widely recognised, and have been tested in the courts) or non-standard terms (whose meaning may not yet be settled or whose effectiveness may be uncertain);

(3) the manner in which its documentation is issued; and

(4) the extent to which confirmation of acceptance is required (including by *customer* signature or counterparty confirmation).

IT systems

13.7.5 G IT systems include the computer systems and infrastructure required for the automation of processes, such as application and operating system software; network infrastructure; and desktop, server, and mainframe hardware. Automation may reduce a *firm's* exposure to some 'people risks' (including by reducing human errors or controlling access rights to enable segregation of duties), but will increase its dependency on the reliability of its IT systems.

13.7.6 G A *firm* should establish and maintain appropriate systems and controls for the management of its IT system risks, having regard to:

(1) its organisation and reporting structure for technology operations (including the adequacy of senior management oversight);

(2) the extent to which technology requirements are addressed in its business strategy;

(3) the appropriateness of its systems acquisition, development and maintenance activities (including the allocation of responsibilities between IT development and operational areas, processes for embedding security requirements into systems); and

(4) the appropriateness of its activities supporting the operation of IT systems (including the allocation of responsibilities between business and technology areas).

Information security

13.7.7 G Failures in processing information (whether physical, electronic or known by *employees* but not recorded) or of the security of the systems that maintain it can lead to significant operational losses. A *firm* should establish and maintain appropriate systems and controls to manage its information security risks. In doing so, a *firm* should have regard to:

(1) confidentiality: information should be accessible only to *persons* or systems with appropriate authority, which may require firewalls within a system, as well as entry restrictions;

(2) integrity: safeguarding the accuracy and completeness of information and its processing;

(3) availability and authentication: ensuring that appropriately authorised *persons* or systems have access to the information when required and that their identity is verified;

(4) non-repudiation and accountability: ensuring that the *person* or system that processed the information cannot deny their actions.

13.7.8 G A *firm* should ensure the adequacy of the systems and controls used to protect the processing and security of its information, and should have regard to established security standards such as ISO17799 (Information Security Management).

Geographic location

13.7.9 G Operating processes and systems at separate geographic locations may alter a *firm*'s operational risk profile (including by allowing alternative sites for the continuity of operations). A *firm* should understand the effect of any differences in processes and systems at each of its locations, particularly if they are in different countries, having regard to:

(1) the business operating environment of each country (for example, the likelihood and impact of political disruptions or cultural differences on the provision of services);

(2) relevant local regulatory and other requirements regarding data protection and transfer;

(3) the extent to which local regulatory and other requirements may restrict its ability to meet regulatory obligations in the *United Kingdom* (for example, access to information by the *FCA* and local restrictions on internal or external audit); and

(4) the timeliness of information flows to and from its headquarters and whether the level of delegated authority and the risk management structures of the overseas operation are compatible with the *firm*'s head office arrangements.

13.8 External events and other changes

13.8.1 G The exposure of a *firm* to operational risk may increase during times of significant change to its organisation, infrastructure and business operating environment (for example, following a corporate restructure or changes in regulatory requirements). Before, during, and after expected changes, a *firm* should assess and monitor their effect on its risk profile, including with regard to:

(1) untrained or de-motivated *employees* or a significant loss of *employees* during the period of change, or subsequently;

(2) inadequate human resources or inexperienced *employees* carrying out routine business activities owing to the prioritisation of resources to the programme or project;

(3) process or system instability and poor management information due to failures in integration or increased demand; and

(4) inadequate or inappropriate processes following business re-engineering.

13.8.2 G A *firm* should establish and maintain appropriate systems and controls for the management of the risks involved in expected changes, such as by ensuring:

(1) the adequacy of its organisation and reporting structure for managing the change (including the adequacy of senior management oversight);

(2) the adequacy of the management processes and systems for managing the change (including planning, approval, implementation and review processes); and

(3) the adequacy of its strategy for communicating changes in systems and controls to its *employees*.

Unexpected changes and business continuity management

13.8.3 G SYSC 3.2.19 G provides high level *guidance* on business continuity. This section provides additional *guidance* on managing business continuity in the context of operational risk.

13.8.4 G The high level requirement for appropriate systems and controls at SYSC 3.1.1 R applies at all times, including when a business continuity plan is invoked. However, the *FCA* recognises that, in an emergency, a *firm* may be unable to comply with a particular *rule* and the conditions for relief are outlined in GEN 1.3 (Emergency).

13.8.5 G A *firm* should consider the likelihood and impact of a disruption to the continuity of its operations from unexpected events. This should include assessing the disruptions to which it is particularly susceptible (and the likely timescale of those disruptions) including through:

(1) loss or failure of internal and external resources (such as people, systems and other assets);

(2) the loss or corruption of its information; and

(3) external events (such as vandalism, war and "acts of God").

13.8.6 G A *firm* should implement appropriate arrangements to maintain the continuity of its operations. A *firm* should act to reduce both the likelihood of a disruption (including by succession planning, systems resilience and dual processing); and the impact of a disruption (including by contingency arrangements and insurance).

13.8.7 G A *firm* should document its strategy for maintaining continuity of its operations, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy. A *firm* should establish:

(1) formal business continuity plans that outline arrangements to reduce the impact of a short, medium or long-term disruption, including:

(a) resource requirements such as people, systems and other assets, and arrangements for obtaining these resources;

(b) the recovery priorities for the *firm*'s operations; and

(c) communication arrangements for internal and external concerned parties (including the *FCA*, *clients* and the press);

(2) escalation and invocation plans that outline the processes for implementing the business continuity plans, together with relevant contact information;

(3) processes to validate the integrity of information affected by the disruption; and

(4) processes to review and update (1) to (3) following changes to the *firm*'s operations or risk profile (including changes identified through testing).

13.8.8 G The use of an alternative site for recovery of operations is common practice in business continuity management. A *firm* that uses an alternative site should assess the appropriateness of the site, particularly for location, speed of recovery and adequacy of resources. Where a site is shared, a *firm* should

13

evaluate the risk of multiple calls on shared resources and adjust its plans accordingly.

13.9 Outsourcing

13.9.1 G As SYSC 3.2.4 G explains, a *firm* cannot contract out its regulatory obligations and should take reasonable care to supervise the discharge of outsourced functions. This section provides additional *guidance* on managing *outsourcing* arrangements (and will be relevant, to some extent, to other forms of third party dependency) in relation to operational risk. *Outsourcing* may affect a *firm's* exposure to operational risk through significant changes to, and reduced control over, people, processes and systems used in outsourced activities.

13.9.2 G *Firms* should take particular care to manage *material outsourcing* arrangements and, as SUP 15.3.8 G (1)(e) explains, a *firm* should notify the *FCA* when it intends to enter into a *material outsourcing* arrangement.

13.9.3 G A *firm* should not assume that because a service provider is either a regulated *firm* or an intra-group entity an *outsourcing* arrangement with that provider will, in itself, necessarily imply a reduction in operational risk.

13.9.4 G Before entering into, or significantly changing, an *outsourcing* arrangement, a *firm* should:

(1) analyse how the arrangement will fit with its organisation and reporting structure; business strategy; overall risk profile; and ability to meet its regulatory obligations;

(2) consider whether the agreements establishing the arrangement will allow it to monitor and control its operational risk exposure relating to the *outsourcing*;

(3) conduct appropriate due diligence of the service provider's financial stability and expertise;

(4) consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed *outsourcing* arrangement (including what will happen on the termination of the contract); and

(5) consider any concentration risk implications such as the business continuity implications that may arise if a single service provider is used by several *firms*.

13.9.5 G In negotiating its contract with a service provider, a *firm* should have regard to:

(1) reporting or notification requirements it may wish to impose on the service provider;

(2) whether sufficient access will be available to its internal auditors, external auditors or *actuaries* (see section 341 of the *Act*) and to the *FCA* (see SUP 2.3.5 R (Access to premises) and SUP 2.3.7 R (Suppliers under material outsourcing arrangements);

(3) information ownership rights, confidentiality agreements and *Chinese walls* to protect *client* and other information (including arrangements at the termination of the contract);

(4) the adequacy of any guarantees and indemnities;

(5) the extent to which the service provider must comply with the *firm*'s policies and procedures (covering, for example, information security);

(6) the extent to which a service provider will provide business continuity for outsourced operations, and whether exclusive access to its resources is agreed;

(7) the need for continued availability of software following difficulty at a third party supplier;

(8) the processes for making changes to the *outsourcing* arrangement (for example, changes in processing volumes, activities and other contractual terms) and the conditions under which the *firm* or service provider can choose to change or terminate the *outsourcing* arrangement, such as where there is:

(a) a change of ownership or *control* (including insolvency or receivership) of the service provider or *firm*; or

(b) significant change in the business operations (including sub-contracting) of the service provider or *firm*; or

(c) inadequate provision of services that may lead to the *firm* being unable to meet its regulatory obligations.

13.9.6 G In implementing a relationship management framework, and drafting the service level agreement with the service provider, a *firm* should have regard to:

(1) the identification of qualitative and quantitative performance targets to assess the adequacy of service provision, to both the *firm* and its *clients*, where appropriate;

(2) the evaluation of performance through service delivery reports and periodic self certification or independent review by internal or external auditors; and

(3) remedial action and escalation processes for dealing with inadequate performance.

13.9.7 G In some circumstances, a *firm* may find it beneficial to use externally validated reports commissioned by the service provider, to seek comfort as to the adequacy and effectiveness of its systems and controls. The use of such reports does not absolve the *firm* of responsibility to maintain other oversight. In addition, the *firm* should not normally have to forfeit its right to access, for itself or its agents, to the service provider's premises.

13.9.8 G A *firm* should ensure that it has appropriate contingency arrangements to allow business continuity in the event of a significant loss of services from the service provider. Particular issues to consider include a significant loss of resources at, or financial failure of, the service provider, and unexpected termination of the *outsourcing* arrangement.

13.9.9 G

(1) Parts of the *guidance* in SYSC 13.9 do not apply to a *Solvency II firm*. They are SYSC 13.9.3G, SYSC 13.9.4G(1), (2), (4) and (5) and SYSC 13.9.5G(6).

(2) A *Solvency II firm* is subject to the outsourcing requirements in PRA Rulebook: Solvency II firms: Conditions Governing Business 7.

(3) The *Solvency II Regulation* (EU) 2015/35 of 10 October 2014 (article 274) also imposes specific requirements on *firms* which outsource, or propose to outsource, functions or insurance activities.

(4) *EIOPA* guidelines on systems of governance dated 28 January 2015 (EIOPA-BoS-14/253 EN) include guidelines on, or relating to, outsourcing.

(5) The *FCA* will take the requirements and guidelines in (2) to (4) into account when considering a *firm's* outsourcing arrangements.

13.10 Insurance

13.10.1 G Whilst a *firm* may take out insurance with the aim of reducing the monetary impact of operational risk events, non-monetary impacts may remain (including impact on the *firm*'s reputation). A *firm* should not assume that insurance alone can replace robust systems and controls.

13.10.2 G When considering utilising insurance, a *firm* should consider:

(1) the time taken for the *insurer* to pay claims (including the potential time taken in disputing cover) and the *firm*'s funding of operations whilst awaiting payment of claims;

(2) the financial strength of the *insurer*, which may determine its ability to pay claims, particularly where large or numerous small claims are made at the same time; and

(3) the effect of any limiting conditions and exclusion clauses that may restrict cover to a small number of specific operational losses and may exclude larger or hard to quantify indirect losses (such as lost business or reputational costs).